Morphisms of Drinfeld Modules and their Algorithms

Antoine Leudière

Thèse de doctorat en
Informatique

de
l'Université de Lorraine

au
Laboratoire Lorrain de Recherche en Informatique et ses Applications

soutenue publiquement le
lundi 16 septembre 2024

devant un jury composé de

Xavier Goaoc Université de Lorraine, Professeur	Président du jury
Alain Couvreur INRIA, Directeur de recherche	Rapporteur
Éric Schost University of Waterloo, Professor	Rapporteur
Cécile Armana Université de Franche-Comté, Maîtresse de conférences	Examinatrice
Elena Berardini CNRS, Chaire de Professeur Junior	Examinatrice
Pierre-Jean Spaenlehauer INRIA, Chargé de recherche	Encadrant
Emmanuel Thomé INRIA, Directeur de recherche	Encadrant

et grâce au précieux soutien de l'école doctorale
iaem

Université de Lorraine

Contents

Remerciements

Mes premiers remerciements vont à Pierre-Jean Spaenlehauer et Emmanuel Thomé, artisans fondateurs de cette thèse. Ils m'ont offert ce sujet, dans sa pertinence et sa beauté, et leur inlassable patience, leur infaillible savoir et la permanente disponibilité de leur expérience. Je dois à Xavier Caruso certaines des plus belles idées du manuscrit — je suis aussi émerveillé que reconnaissant. Ce document fut évalué par des gens que j'admire : Alain Couvreur et Éric Schost comme rapporteurs ; Cécile Armana, Elena Berardini et Xavier Goaoc comme examinatrices et examinateurs. Je les remercie pour leur exigence, mêlée de bienveillance. Enfin, je pense à David Ayotte et Joseph Musleh, pour leur aide logicielle, et pour avoir formé avec moi un trio de doctorants travaillant sur l'algorithmique des modules de Drinfeld. Pour l'enseignement, Xavier Goaoc et Pierre-Étienne Moreau furent des guides. Et je remercie Simon Perdrix, pour son suivi.

During my thesis, I was privileged to visit Renate Scheidler at the university of Calgary. Our work arrived too late to make its way into this manuscript, but I look forward to collaborating with her again soon, as a post-doctoral researcher. Laurent Imbert initiated this exchange; I cannot thank him enough. Gaetan Bisson, too, helped in many ways. Finally, I think of Gregory Knapp, Hunter Yaworski, and Joshuah Lockett-Harris. And of course: Karina, te extraño*; Keira, I miss you.*

Je pense avec émotion à mes amis du Loria. Initialement : Haetham Al Aswad et Margarita Cordero. Puis : Medhi Kermaoui, Julien Soumier, Marie Bolzer, Alexandre Benoist, Amaury Saint-Jore et Sélène Corbineau. Il y eut aussi *les vieux* — toutes et tous — et puis les autres, d'égale importance : Emmanuelle Deschamps & Cécilia Olivier, Anne Chrétien, Claire Bacheter, et évidemment, Isabelle Legrand.

Et il y a *les miens*, que j'aime infiniment : Topnu, Patience et Goldie, puis Meige, Pourpreneige, Cotirel, Cécile & Ludo, CamCam, Julou, Stéphane, Jé, Pauliphonie, Emma & Marthe, Ludo et Aurore. Léo-Louis, pour des raisons évidentes. Quant à Quentin Dupré, Abel Laval & Adrien Deloro, Frédéric Le Roux et Emmanuel Ferrand, ils m'accompagnent depuis la licence ; cette thèse est un peu la leur.

De manière plus abstraite, mais peut-être plus profonde, je rends hommage à l'esprit universitaire, éther des chemins et des échanges. C'est à lui que je m'adonne, et par lui que brillent : Evrim Evci, mon professeur de terminale ; tous mes amis de la double-licence de sciences et musicologie ; Boris Doval, responsable de l'époque ; Hélène Dumontet qui, avec le soutien de Laurent Koelblen, m'a permis d'étudier les mathématiques ; Frédéric Le Roux, Emmanuel Ferrand et Adrien Deloro, que j'ai déjà mentionnés ; Alain Kraus, pédagogue ; Antonin Guilloux, que j'ai cru ; Fabrice Rouillier, l'algèbre effective ; et Anne Canteaut, qui m'a reçu, puis guidé vers Caramba et Lfant. Vint ensuite le début de ma thèse ; eurent comme place particulière : les précédents, Jade Nardi, Benjamin Wesolowski et Paola de Pertuis.

Je remercie Anna Cadoret pour m'avoir redonné goût aux mathématiques, et Ktorphée.

Je dois à ma mère de ne pas être complètement imbécile. Je dois à ma sœur d'avoir appris à l'aimer. Je dois à Bob et Julie le bonheur de l'enfance, et d'être ce que je suis.

Cette thèse est évidemment dédiée à Hélène Dumontet.

How strange is it to be anything at all?

—Jeff Mangum

Introduction

The goal of this thesis is to develop the algorithmic toolbox of Drinfeld modules. We target applications ranging from computer algebra to cryptography. Most of our problems are inspired from the arithmetic of elliptic curves, and we build upon a series of works started in the last decade which establishes the algorithmics of Drinfeld modules as a topic on its own [Car18; DNS21; MS19; CGS20; MS23; Ayo23; Mus23].

New approaches. We suggest that the main new algorithmic approaches of this thesis are:

(i) Using Anderson motives to solve computational problems on Drinfeld modules.

(ii) Using a certain central simple algebra to solve computational problems on Drinfeld modules over a finite field.

(iii) Using the fact that in some cases, the characteristic polynomial of the Frobenius endomorphism of a Drinfeld module over a finite field, defines an imaginary hyperelliptic curve.

Contributions. These helped us working on the following problems:

(i) In Chapters 4, 5 and 6, we compute characteristic polynomials of Drinfeld module endomorphisms and norms of Drinfeld module isogenies. Our algorithms work over any base field, any function ring (not restricting to $\mathbb{F}_q[T]$), and any rank. But in the case of finite fields and Frobenius endomorphisms, we provide optimizations. In some cases, we reach asymptotic complexities that enhance the state of the art. Chapters 4 and 5 rely on a common framework based on Anderson motives, while Chapter 6 focuses on the sole Frobenius endomorphism, and computes it as a reduced norm in a central simple algebra. All these algorithms are implemented; their running times are analyzed both in theory and practice. This is a joint work with Xavier Caruso [CL23].

(ii) In Chapter 7, we compute a group action that was defined in the class field theory of function fields. An analogous group action is known in the context of elliptic curves as the main building block of the Couveignes-Rostovtsev-Stolbunov (CRS) cryptosystem [CL09; RS06], the first post-quantum cryptographic protocol based on elliptic curves, but the computational performances are not practical. Our algorithm is significantly faster than its characteristic zero counterpart, as it relies on the characterization of the acting group as the Picard group of an imaginary hyperelliptic curve, and on the representation of Drinfeld module isogenies as Ore polynomials. This is a joint work with Pierre-Jean Spaenlehauer [LS24].

(iii) In Chapter 3, we introduce a SageMath implementation of Drinfeld modules—the first Drinfeld module framework directly integrated to a major computer algebra system. This is a joint work with David Ayotte, Xavier Caruso and Joseph Musleh [Ayo+23].

Motivation

To some extent, Drinfeld modules are to function fields what elliptic curves are to number fields. The motivation for studying Drinfeld modules from a computational point of view mainly comes from their similarities with elliptic curves, and from the convenience of working with function fields. Elliptic curves are researched in both theory and applications, mainly thanks to their applications to cryptography, and to their role in algebraic geometry. On the other hand, function fields distinguish themselves from number fields by their geometrical structure. Indeed, while a function field can be defined as a finite extension of $\mathbb{F}_q(T)$, it can also be viewed as a space of functions from an algebraic curve to its base field. This point of view allows to study function fields with all the tools of algebraic geometry, as the arithmetic of a function field is dictated by the geometry of the curve it corresponds to; algebraic properties of a function field can be described using points, divisors, singularities, etc, which is not possible (or at least to the same extent) in number fields. As a consequence, function fields offer a wider range of algorithms, with better performances. For example, it is well known that the factorization of integers is a hard computational problem of significant importance, while factorizing univariate polynomials only requires a polynomial number of operations. A more technical example is the following. The CSIDH cryptosystem, which we review in § A.2.3.2, is based on the group action of the class group of an order in a quadratic imaginary number field. Knowing the order of this class group—a problem different as that of computing the group action—would pave the way to better key exchange protocols based on isogenies of elliptic curves [Feo+23; CLP24], a class of protocols which typically allows for very compact keys and signatures sizes. Unfortunately, computing this order is not currently attainable, except on very specific instances [BKV19]. On the opposite, we compute in Chapter 7 a group action whose acting group is also the class group of a quadratic imaginary field, but in function fields. The theory of algebraic geometry allows us to view this class group as the Picard group of an imaginary hyperelliptic curve, whose elements can be represented with Mumford coordinates. The order is computed in about fifty hours using an algorithm of Denef and Vercauteren [DV06a].

When it comes to computation, there is thus a significant disparity between characteristic zero and characteristic p. While many constructions fall under the same theoretical ideas (*e.g.* number fields are finite extensions of $\mathbb{Q}$, function fields are finite extensions of $\mathbb{F}_q(T)$), the asymmetry in computational efficiency owes to the fact that (1) polynomials are computationally easier than integers (for example, adding two polynomials does not require caries), and (2) function fields provide $\mathbb{F}_q$-linear objects, while number fields do not, for no field injects into $\mathbb{Z}$. Algebraic number theory and class field theory have now firmly established elliptic curves as one of the key tools for the study of number fields and Diophantine equations; for function fields, the role of elliptic curves is played by (rank two) Drinfeld modules. These objects, formally defined in 1977 [Dri77] but studied since the inter-war period [Car35], exist in much greater generality than elliptic curves. Besides, most computational problems that exist for elliptic curves find an analogue for Drinfeld modules, which is more often easier to solve. An important question is then to build computational bridges between characteristic zero and characteristic p; a fundamental open problem that, among others, could drastically change the course of cryptography.

State of the art

The first research works that were fully devoted to the algorithmics of Drinfeld modules were mirrors of techniques for elliptic curve. In that spirit, and in order to get the best analogies between Drinfeld modules

and elliptic curves, one has to restrict to rank two Drinfed $\mathbb{F}_q[T]$-modules. In [DNS21], Doliskani, Narayanan and Schost use them to factorize polynomials over a finite field, and their probabilistic method matches the state of the art. In her thesis [Car18], Caranay developed the Drinfeld module analogue of Kohel's thesis [Koh96], a major milestone in the computational theory of elliptic curves. Caranay was also interested in computing Drinfeld modular polynomials, which are related to Drinfeld modular forms and Drinfeld modular curves. Drinfeld modular forms and curves were studied in [Ayo23], and hold potential to be used in code-based cryptography, following the work of [BC24], which uses Ore polynomials. In [CGS20], Caranay, Greenberg and Scheidler are interested in the problem of computing isogenies between two Drinfeld modules over a finite field, a problem also reviewed in [LS22]. At the time, this problem was suspected to be hard, and Wesolowski found a simple yet efficient method to solve it [Wes22]. Musleh then built on Wesolowski's approach (as well as, to a lesser extent, on the approach Chapters 4 and 5 relying on Anderson motives) to compute endomorphism rings of Drinfeld modules in polynomial time [Mus23, § 7.3]. In contrast, the computation of endomorphism rings of elliptic curves is significantly harder, so much that it is actively studied as the computational problem underlying the security of new post-quantum cryptosystems [PW23]. The key for Wesoloski and Musleh was to build *ad hoc* methods and not to rely on analogies with elliptic curves. Their ideas exploit the fact that morphisms between two Drinfeld modules form an $\mathbb{F}_q$-vector space (they only form a $\mathbb{Z}$-module for elliptic curves), which not only allowed them to find an efficient solution, but also to make the solution much more general than the sole rank two case.

While rank two Drinfeld modules hold many similarities with elliptic curves, and rank one Drinfeld modules do so with cyclotomic number fields (see § 2.2.2.2), the theory of Drinfeld modules makes it relatively easy to work on a general rank. Isogenies (that is, nonzero morphisms) can only exist between Drinfeld module of equal rank, and computations tend to be more challenging in larger rank, but most theoretical results fall within the same framework. Computations related to rank one or rank two Drinfeld modules may even be enhanced by considering Drinfeld modules of general ranks and solving the general case. In that context, one cannot rely on elliptic curves, and has to take advantage of function field arithmetics. Following this philosophy, Musleh and Schost revisited their 2019 paper [MS19] in 2023, and came up with an original and explicit approach based on the crystalline cohomology of Drinfeld modules [MS23]. This massively enhanced the state of the art, as their methods work on any endomorphism, any base field, and any rank. The methods presented in Chapter 4, 5 and 6 were developed simultaneously, and solve the same problem: computing the characteristic polynomial of any endomorphism of Drinfeld modules. While the question is surely inspired from elliptic curves, the methods we mention are original, and general.

Contributions

We studied two algorithmic problems, and proposed an implementation of Drinfeld modules in SageMath. First, let us briefly present the mathematical context in which Drinfeld modules are defined. We begin by fixing a finite field $\mathbb{F}_q$. A smooth and geometrically connected curve C over $\mathbb{F}_q$ is then chosen, together with a point denoted ∞. We let A be the ring of functions in $\mathbb{F}_q(C)$ that are regular on all points but ∞. Then, an extension K of $\mathbb{F}_q$ is picked as the base field. We say that A is the *function ring*. Although it is not necessary in this section, we mention that K has to be equipped with a morphism of $\mathbb{F}_q$-algebras $\gamma : A \to K$. The simplest Drinfeld modules are those for which C is $\mathbb{P}^1(\mathbb{F}_q)$ and ∞ is the point at infinity; then, A is $\mathbb{F}_q[T]$, and we talk about *Drinfeld* $\mathbb{F}_q[T]$*-modules*. In the general case, *i.e.* when

no assumption on the function ring A is given, we talk about *Drinfeld A-modules*, or *general Drinfeld modules*. This subset of Drinfeld $\mathbb{F}_q[T]$-modules were originally the most studied, for its similarities with elliptic curves. However, many of our results work over any function ring, and we provide mathematical context for the consideration of general function rings in § *Mathematical history of Drinfeld modules*. We also mention that any Drinfeld modules has an invariant called the *rank*, which is an integer; the Drinfeld modules that are closest to elliptic curves are rank two Drinfeld $\mathbb{F}_q[T]$-modules.

Computing norms and characteristic polynomials

As often in algebra, morphisms of Drinfeld modules are as important as Drinfeld modules themselves. Nonzero morphisms of Drinfeld modules are called isogenies, and an isogeny exists from a Drinfeld module to another if and only if one exists in the other direction. Consequently, isogenous Drinfeld modules form an equivalence class, and on finite fields, these isogeny classes can be represented by a single invariant, the *characteristic polynomial of the Frobenius endomorphism*. For elliptic curves, the same is true, and two elliptic curves are isogenous if and only if they have the same number of rational points. This theorem can evidently not be formulated for Drinfeld modules, which do not have points. However, the number of rational points of an elliptic curve is related to its *characteristic polynomial of its Frobenius endomorphism*, a degree two polynomial with coefficients in $\mathbb{Z}$. For Drinfeld modules, this polynomial can also be defined: $\mathbb{Z}$ is replaced by $\mathbb{F}_q[T]$ or A, 2 is replaced by the rank r, and to any endomorphism can be attached a characteristic polynomial. Even assumptions on the base field K can be removed, and our goal is to efficiently compute these characteristic polynomials in the highest possible degree of generality.

As we mentioned, the first paper fully devoted to the computation of the characteristic polynomial of the Frobenius endomorphism was that of Musleh and Schost [MS19]. It was devoted to Drinfeld $\mathbb{F}_q[T]$-modules of rank two, and the follow-up paper [MS23] dealt with the general case, allowing the computation of characteristic polynomials of any endomorphism, for any rank and base field, the function ring being $\mathbb{F}_q[T]$. Their algorithms are very efficient, and rely on the crystalline cohomology of Drinfeld modules. Our joint-work with Xavier Caruso [CL23] achieves the same task, with a different approach, and getting rid of the assumption that A is $\mathbb{F}_q[T]$. While both methods express the characteristic polynomial of an endomorphism as that of a classical polynomial matrix, ours does so by using *Anderson motives*. Conceptually, Drinfeld modules and Anderson motives are related by a dual correspondence, which is presented in terms of a contravariant fully faithful functor. This allows to assimilate Drinfeld modules and their Anderson motives, as well as morphisms of both objects. The key is that contrary to Drinfeld modules, Anderson motives are modules in the classical sense. When A is $\mathbb{F}_q[T]$, the Anderson motive is a free $K[T]$-module with with rank r (r being the rank of the Drinfeld module). It has a so-called *canonical $K[T]$-basis*, which is given by a closed formula, which makes it possible to represent endomorphisms of Drinfeld modules by r-by-r polynomial matrices. We developed an algorithm to compute the said matrices, and subsequently obtain the characteristic polynomial of any Drinfeld module endomorphism. Here, the impact of the rank is very transparent: it only determines the size of the matrix, but does not change the algorithm. Our approach also extends to the computation of norms of isogenies, by computing a determinant rather than a characteristic polynomial. When A is larger than $\mathbb{F}_q[T]$, the Anderson motive is unfortunately not free, but only projective; yet, we manage to adapt our algorithms by reducing to the $\mathbb{F}_q[T]$ case.

It was already known that, for Drinfeld $\mathbb{F}_q[T]$-modules, the characteristic polynomial of an endomorphism was that of its action on the Anderson motive. However, we give a new theoretical proof of this statement, without any restriction on A. On the other hand, when A is the polynomial ring $\mathbb{F}_q[T]$,

several optimizations are presented, most notably for finite fields and the Frobenius endomorphism. Our algorithms are implemented, benchmarked, and accompanied by thorough asymptotic complexity analyses, which reveal that our methods are the most asymptotically efficient in many parameter ranges.

These motivic methods (Chapters 4 and 5) work best when the rank is low with respect to the extension degree of the ground field. In order to have competitive algorithms in the opposite situation, we derived an approach based on *central simple algebras* and *reduced norms* (Chapter 6). Reduced norms are norm maps defined on a central simple algebra, that have values in its center, and naturally give the notion of *reduced characteristic polynomial*—in our case, the central simple algebra is a ring $K\{\tau\}$ of Ore polynomials; the Frobenius endomorphism of a Drinfeld module embeds in this algebra and generates its center over $\mathbb{F}_q$. We thus compute the characteristic polynomial of the Frobenius endomorphism as the reduced norm of a well-chosen element in this central simple algebra. Once again, we have reduced the computation of the characteristic polynomial of a Drinfeld module endomorphism to the computation of the characteristic polynomial of a classical matrix. This second method works on all function rings A, but demonstrates its strengths when the rank is large with respect to the extension degree of the ground field.

Computing a group action from class field theory of function fields

Our other algorithmic task was the computation of a group action originating from class field theory of function fields. Drinfeld modules were introduced to make the class field theory of function fields more explicit, and this group action exactly does that: it describes the free and transitive action of the class group of a function ring A on a set of isomorphism classes of rank one Drinfeld modules over $\mathbb{C}_\infty$, the function field avatar of $\mathbb{C}$. In the case of elliptic curves, this correspondence between ideal classes and isomorphism classes of elliptic curves, is also known as the main building block of the foundational construction of *isogeny-based cryptography*, the branch of cryptography which uses isogenies of elliptic curves to build protocols immune against quantum computers. The group action (for elliptic curves) was first used in cryptography by Couveignes in [Cou06], and independently so by Rostovtsev and Stolbunov in [RS06]. The construction, named CRS, is very elegant: it replicates a Diffie-Hellman key exchange, but replaces finite fields or elliptic curves by isomorphism classes of ordinary and isogenous elliptic curves; this set is acted upon by the class group of an order in an imaginary quadratic number field. The security of the cryptosystem is based on the assumption that computing an isogeny between two distinct elliptic curves over a finite field is a hard problem. This problem has since been widely studied, and is now the cornerstone of many *isogeny-based* constructions, including the *SQIsign* signature protocol and its derivatives [De +20; Dar+24; Bas+24; NO24; DF24]. These are being considered by the *National Institute of Standards and Technology* (NIST) for standardization as a post-quantum (meaning safe against quantum computers) standardized cryptosystem.

Unfortunately, computing the group action behind the CRS cryptosystem is challenging. Despite recent optimizations [DKS18], performing a key exchange requires about ten minutes, which makes CRS unpractical. With Pierre-Jean Spaenlehauer, we thus investigated the practical computation of the group action, by switching to Drinfeld modules. For the efficiency, we managed to compute the group action in less than a second, on cryptographic sizes. We owe this performance to two phenomenon:

(i) In our case, the characteristic polynomial of the Frobenius endomorphism of the Drinfeld modules defines an imaginary hyperelliptic curve. This allows to represent the acting class group as a Picard

group, and to use Mumford coordinates for fast computations.

(ii) Isogenies of Drinfeld modules can be represented as Ore polynomials; the isogeny corresponding to the intersection of two kernels can be computed as the RGCD of two Ore polynomials.

Regarding the cryptographic applications, the work of Wesolowski [Wes22] makes the Drinfeld module version of the CRS cryptosystem insecure. This partially answers a longstanding questions regarding the use of Drinfeld modules in cryptography, that was first investigated in 2001 with the work of Scanlon [Sca01]. The complete state of the art is surveyed in Appendix A—all cryptographic proposals were broken using linear structures associated to Drinfeld modules, and most of the time, the secret key is recovered as the solution of a finite $\mathbb{F}_q$-linear system. If Drinfeld modules are to be used in cryptography, one must investigate about original hard computational problems. One downside of isogeny-based cryptography is that computations are slower than most alternatives—using Drinfeld modules may still lead to having the best of both worlds: secure cryptosystems and fast operations.

Implementing Drinfeld modules in SageMath

At the beginning of our research work, Drinfeld modules were implemented in no major computer algebra system, preventing this research topic to flourish. We thus decided to develop a fully-featured SageMath implementation of Drinfeld modules, and to implement our algorithms in it. SageMath is a free and open source computer algebra system which allows mathematicians of all levels to perform a wide range of computations. It is based on the widely-used *Python* programming language, making it a most valuable tool. Our implementation work started in April of 2022 (Github Issue `#33713`), and the first version was integrated into SageMath in March of 2023 (Github Pull Request `#35026`). We made our contribution as simple and general as possible, covering all our code with exhaustive documentation and testing. We also owe much to David Ayotte, Xavier Caruso and Joseph Musleh, who contributed to the design, code, and review [Ayo+23]. Algorithms of Chapters 4, 5 and 6 were all implemented and benchmarked. We refer to the instructions of Chapter 3 to try the code. We showcase our implementation in this thesis, both as computational and mathematical examples, by showing snippets of code that can directly be ran in the SageMath console.

```
sage: 57.is_prime()
False
sage: # Ok, this works!
```

Mathematical history of Drinfeld modules

The goal of this historical preliminary is to convince the reader that Drinfeld modules are natural analogues of elliptic curves in function fields, even though they exist in much greater generality. In particular, we explain the origins of the notion of *rank*, and motivate the definition of Drinfeld modules on general *function rings*, without restriction to $A = \mathbb{F}_q[T]$. The reader may safely skip this section and go to § *Organization of the thesis*.

Class field theory

The area studying the Galois abelian extensions of number fields is known as *class field theory*. Chevalley, in 1940, had this beautifully articulated expression (borrowed from [Mil20]):

> *L'objet de la théorie du corps de classes est de montrer comment les extensions abéliennes d'un corps de nombres algébriques L peuvent être déterminées par des éléments tirés de la connaissance de L lui-même ; ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possède en soi les éléments de son propre dépassement.*
>
> The purpose of class field theory is to show how abelian extensions of an algebraic number field L may be determined by elements drawn from the knowledge of L itself; or, should one wish to put things in dialectical terms, how a field contains in itself the elements of its own overcoming.

Attempts to solve this question, at least in its full generality, pan a wide area of mathematics. This should come as no surprise: number fields seem to be the simplest fields that are not $\mathbb{Q}$ or finite, and many try to study them by making objects act (such as elliptic curves) on them. However, some restricted instances of Chevalley's question can answered explicitly. The first of them is the *Kronecker-Weber theorem*: every abelian number field L lies within a cyclotomic number field. That is, there exists a primitive m-th root of unity ζ_m such that $L \subset \mathbb{Q}(\zeta_m)$; studying the algorithmic properties of roots of unity and cyclotomic polynomials would then mean studying L. Then, we have a slightly more technical result: every quadratic imaginary number field L lies within a field generated by invariants (in $\mathbb{C}$) that represent isomorphism classes of elliptic curves whose endomorphism ring is contained in L. This result is a special case of Kronecker's *Jugendtraum*; Kronecker had hoped that every abelian number field would lie in a special extension described in such manner, *i.e.* generated by some specific values of analytic functions. In the case of imaginary quadratic number fields, these analytic functions are obtained from modular forms on the coefficients of elliptic curves, which can be combined to form an analytic function encoding isomorphism classes of elliptic curves. The *theory of complex multiplication* originates from this result.

Replacing number fields by function fields

General statements in class field theory are significantly more abstract and the question of making them more explicit, for example using elliptic curves and modular forms, is central. The theory also generalizes to consider objects such as global and local fields. For example, the Kronecker-Weber theorem has a p-adic version, and mathematicians looked at replacing number fields by function fields. In their simplest description, function fields (of dimension one) are finite extensions of $\mathbb{F}_q(T)$, for some fixed finite field $\mathbb{F}_q$. This construction is symmetric with respect to number fields, but it does not immediately reveal the inner relations between function fields and geometrical objects. To do that, we have to turn to another framework: the dual equivalence between curves and function fields means that mathematicians can study function fields using the tools of algebraic geometry: points, valuations and norms, topology, schemes, and so on. For example, one key advantage of function fields is that the norms on $\mathbb{F}_q(T)$ are all nonarchimedean. While the Euclidean norm on $\mathbb{Q}$ is Archimedean and does not come from a p-adic valuation, all valuations on a function field correspond to a point of its corresponding curve, and *vice versa*. If K is the function field of a smooth curve, and v is a discrete valuation on K, one may consider the

ring A of functions in K that are regular on all points but the one corresponding to v. This construction does not require any other hypothesis than K being the function field of a fixed smooth curve, and any discrete valuation can be picked. Restricting v to a valuation at infinity (provided that one has been fixed) is not necessary, and while Archimedean and nonarchimedean valuations on $\mathbb{Q}$ lead to fundamentally different topologies and theories, the valuations on K are studied under the unified point of view of algebraic geometry. The ring $\mathbb{F}_q[T]$ corresponds to the coordinate ring of $\mathbb{P}^1(\mathbb{F}_q)$, which is also the ring of functions of $\mathbb{P}^1(\mathbb{F}_q)$ that are regular on the affine space and have a singularity at infinity. With the geometrical point of view, we realize that $\mathbb{F}_q[T]$ is only a familiar instance in a large framework. In number fields, objects are usually not described in terms of discrete valuations, while valuations play a leading role in the theory of Drinfeld modules.

Introducing Drinfeld modules

Drinfeld modules were introduced to produce *characteristic p* versions of class field theory and the theory of complex multiplication; they do so by replacing number fields by function fields, $\mathbb{Z}$ by $\mathbb{F}_q[T]$ and more generally, by A. If Drinfeld modules are to follow an analogy with elliptic curves as well as roots of unity, then it seems that a purely geometrical definition cannot be used. In fact, the theory elliptic curves defined over function fields does not lead to statements on which a function field analogue of the *Jugendtraum* could be built, and the same is true for roots of unity in an algebraic closure of $\mathbb{F}_q(T)$ to build cyclotomic function fields. Rather, one should observe that the common point between elliptic curves and roots of unity is the presence of $\mathbb{Z}$-modules: the points of an elliptic curve famously form an abelian group, while roots of unity are the torsion, in $\mathbb{C}^*$, of the $\mathbb{Z}$-module $\mathbb{Q}^*$. Drinfeld modules will thus have to be associated to an $\mathbb{F}_q[T]$-module, or even an A-module. The question is then to determine which set should be be the underlying set of this or A-module. For that, we turn to the definition of Drinfeld modules. First, we fix K, an extension of $\mathbb{F}_q$, accompanied by a morphism $\gamma : A \to K$. The purpose of this morphism is to indicate that in this new theory, integers shall be elements of A, and not of $\mathbb{Z}$. In number fields, fixing a morphism $\mathbb{Z} \to \mathbb{Q}$ is of course not necessary, while in our case, several morphisms exist, and one must be chosen.

Loosely speaking, a *Drinfeld A-module over K* is a map which to an element a of A associates an $\mathbb{F}_q$-linear endomorphism ϕ_a of $\overline{K}$, with the additional assumption that the operator $a \mapsto \phi_a$ defines a ring morphism for the composition. The associated A-module is simply $\overline{K}$, under the map $(a, z) \mapsto \phi_a(z)$. Under the hypothesis that A is $\mathbb{F}_q[T]$, *i.e.* when dealing with $\mathbb{F}_q[T]$-modules, Drinfeld $\mathbb{F}_q[T]$-modules can be defined without any reference to algebraic geometry, requiring only finite fields, commutative algebra, and linear algebra. Most definitions in this case are surprisingly elementary, which makes it even more striking that the theories of Drinfeld modules and elliptic curves yield so similar statements. For example, the definition of an isogeny of elliptic curves requires knowledge of both topological and geometrical structures of a curve; the definition of the function field using sheaves as well as appreciation for the notion of *genus* are also certainly helpful. On the other hand, an isogeny of Drinfeld modules is only a formal $\mathbb{F}_q$-linear combination of Frobenius endomorphisms; this compact representation makes computations very practical. Notice also that Drinfeld modules, defined as maps, have no underlying sets. Even though Drinfeld modules are associated to classical A-modules, the notion of *point* does not directly exist here. Despite these differences, the theory of complex multiplication of function fields, which is formulated with (rank two) Drinfeld modules closely follows its classical counterpart. As an example, we mention that the algebraic classification of the endomorphism ring of a (rank two) Drinfeld module over a finite field is very similar to that of elliptic curves over a finite field: (rank two) Drinfeld modules over

a finite field are either ordinary or supersingular, and their endomorphism ring is either an order in an imaginary quadratic function field, or a maximal order in a function field quaternion algebra.

Historical definitions of Drinfeld modules

However, while it is the so-called *algebraic* definition of Drinfeld A-modules that we choose to employ, *i.e.* the one in which a Drinfeld module is a morphism from A to a set of $\mathbb{F}_q$-linear endomorphisms of $\overline{K}$, it was not the first definition. Originally came Carlitz, whose goal was to derive a theory of complex analysis, and in particular, to define exponential entire and analytical functions in characteristic p. He achieved this, and his construction gave function fields their L, theta and zeta-functions, but also their versions of the Riemann Hypothesis (which in our context, is proved) and the Langlands program [Lafo1]. But as it turns out, when A equals $\mathbb{F}_q[T]$, the exponential functions defined by Carlitz, are in correspondence with rank one Drinfeld $\mathbb{F}_q[T]$-modules over $\mathbb{C}_\infty$—the function field version of $\mathbb{C}$, which we define later. Indeed, to a Carlitz exponential function e_C, one associates its kernel, which is a lattice of $\mathbb{C}_\infty$. (The same happens in the classical theory: the kernel of $\exp : \mathbb{C} \to \mathbb{C}^*$ is $2i\pi\mathbb{Z}$.) Then, to such a lattice, one associates a Drinfeld module, the same way that to a rank two lattice of $\mathbb{C}$, one associates an elliptic curve. The Carlitz exponential function e_C verifies a functional equation $e_C(a \cdot z) = C_a(e_C(z))$, $a \in \mathbb{F}_q[T]$, $z \in \mathbb{C}_\infty$, and the map $a \mapsto C_a$ in fact defines a Drinfeld module—the *Carlitz module*, by definition. The beauty of this construction, called *uniformization of Drinfeld modules*, is that not only does it create a Drinfeld module from an exponential function, it also creates compatible exponential functions from Drinfeld modules. One major difference here with the classical exponential on $\mathbb{C}$, is that lattices of $\mathbb{C}$ can only have rank one or two. In our function field setting, as $\mathbb{C}_\infty$ is in fact much larger than $\mathbb{F}_q(T)$ ($\mathbb{C}_\infty$ is defined as the completion of an algebraic closure of $\mathbb{F}_q((1/T))$, which itself is the completion of $\mathbb{F}_q(T)$ with respect to the point at infinity), sublattices exist in arbitrarily large rank. The *rank* of a Drinfeld module—one of its most crucial invariants—over $\mathbb{C}_\infty$ is the rank of the lattice it corresponds to; the Carlitz modules is a rank one Drinfeld module, and the most profound similarities between Drinfeld modules and elliptic curves occur when the rank is two. And while Drinfeld modules exist in any rank, they are not believed to correspond to any familiar objects in characteristic zero, outside of the ranks one and two.

The feat of Drinfeld was to notice that the construction of Carlitz can be tweaked to work over any base field K, any rank, and any function ring A. More humbly, he called these objects *elliptic modules*. Among many other things, we owe Drinfeld the common framework for all Drinfeld modules. This allows to consider Drinfeld modules over finite fields, and not just $\mathbb{C}_\infty$. The algebraic construction of Drinfeld, using $\mathbb{F}_q$-linear endomorphisms of $\overline{K}$, also highlights the linear properties of Drinfeld modules, which are absent in elliptic curves. In practice, many objects occurring in the theory are $\mathbb{F}_q$-vector spaces. Some even have finite dimension, which means that said objects can efficiently be computed using linear algebra techniques. It is with the works of Drinfeld and Hayes that the theory took off. Even though the Riemann hypothesis was already proved, and that Carlitz had already built function fields cyclotomic extensions, the work of Carlitz and Drinfeld lead to the explicit class field theory of function fields and theory of complex multiplication for function fields that we know today. Drinfeld modules have also been vastly generalized. To Anderson, we owe *Anderson motives*, which appear more explicitly described than the objects described by Grothendieck. The importance of Anderson motives goes far beyond the status of mathematical curiosity, as they embody a dual vision of Drinfeld modules: the category of Drinfeld modules is a subcategory of that of Anderson motives under a very explicit and well-understood contravariant fully faithful functor. We believe the use of Anderson motives to be one of the main

contributions of this thesis; we use them to bypass heavy computations on Drinfeld modules, by turning said computations into linear algebra problems.

Organization of the thesis

Part I exposes necessary background. Chapter 1 covers Ore polynomials (§ 1.1), necessary knowledge in algebraic geometry (§ 1.2) and our computational model (§ 1.3.1). We also review algorithmic primitives for finite fields (§ 1.3.2), polynomial matrices (§ 1.3.3), and Ore polynomials (§ 1.3.4). Chapter 2 covers Drinfeld modules: in § 2.1, we define all we need on Drinfeld $\mathbb{F}_q[T]$-modules; while these are sufficient for most our applications, we do need general Drinfeld A-modules, and define them in § 2.2.

Part II presents our contributions, which are organized in four chapters. Chapter 3 introduces and demonstrates the SageMath implementation of Drinfeld modules; we also discuss some of our design decisions. The two next chapters (Chapters 4 and 5) cover norms and characteristic polynomials computations using Anderson motives; Chapter 6 focuses on the Frobenius endomorphism, and computes its characteristic polynomial using central simple algebras. Finally, Chapter 7 covers the computation of a group action from the class field theory of function fields.

We propose in Appendix A to review past attempts to use Drinfeld modules in cryptography.

Statement of contributions

All contributions presented here are joint-work:

- The SageMath implementation of Drinfeld modules was made with David Ayotte, Xavier Caruso and Joseph Musleh. A *software presentation* was accepted at the 2023 *International Symposium on Symbolic and Algebraic Computation* (ISSAC). See [Ayo+23].
- All work regarding the computation of characteristic polynomials of endomorphisms and norms of isogenies was done with Xavier Caruso. Chapters 4, 5 and 6 are freely taken from [CL23].
- Chapter 7, a joint work with Pierre-Jean Spaenlehauer, is essentially [LS24].

Part I
Background

Chapter 1
General vocabulary

In this chapter, we review the following topics:

(i) In § 1.1, we define *Ore polynomials*, a class of noncommutative polynomials. Ore polynomials intervene in the definition of Drinfeld modules and their morphisms, and are used all along this thesis. In § 1.1.2, we present a more general framework for Ore polynomials and discuss its relation with central simple algebras, as required by Chapter 6.

(ii) In § 1.2, we focus on defining curves and their function fields. This serves multiple purposes. First of all, the definition of general Drinfeld modules (§ 2.2) involves the ring of functions A on a curve C that are regular on all but one fixed point. Second, in Chapter 7 we use imaginary hyperelliptic curves and their Picard groups (§ 1.2.4) to compute a group action from the class field theory of function fields.

(iii) Finally, in § 1.3, we present our computation model, and review relevant algorithmic primitives for finite fields, polynomial matrices, and Ore polynomials.

1.1 Ore polynomials

We let K be an extension of $\mathbb{F}_q$ and define two classes of Ore polynomials. In § 1.1.1, we define the $\mathbb{F}_q$-algebra $K\{\tau\}$, which is used in the definition of Drinfeld modules and their morphisms. As such used in all this thesis. Ore polynomials of $K\{\tau\}$ can also be referred to as *skew polynomials*. In § 1.1.2, we give a new definition for $K\{\tau\}$, which allows to to study more general algebras of Ore polynomials. This is necessary to prove the theoretical results of Chapter 6. For references on Ore polynomials, we refer to classical textbooks on Drinfeld modules [Pap23; Ros02; Gos96] (the last one having the most extensive study of them all). Ore polynomials are named after Oystein Ore, whose article [Ore33] can also be a valuable starting point. Finally, [Car17] (in French), is also a valuable resource.

1.1.1 Skew polynomials

Let $\mathbb{F}_q$ be a finite field with q elements, and K be an extension of $\mathbb{F}_q$. We let $\overline{K}$ denote a fixed algebraic closure of K.

1.1.1.1 Definition

Recall that K is a field over $\mathbb{F}_q$, and that the Frobenius map

$$\begin{array}{ccc} K & \to & K \\ x & \mapsto & x^q \end{array}$$

is $\mathbb{F}_q$-linear. Polynomials of $K[X]$ of the form $P(X) = \sum_{i=0}^{n} P_i X^{q^i}$ are called *q-polynomials*. For each such q-polynomial P, the map $x \mapsto P(x)$ is $\mathbb{F}_q$-linear. Crucially, the set of q-polynomials is closed under addition and composition, and forms an algebra over $\mathbb{F}_q$ with these compatible operations. We call this algebra the algebra of *Ore polynomials*. Any of its elements can be uniquely written as

$$a_0 + \cdots + a_n \tau^n, \quad a_0, \ldots, a_n \in K, \quad a_n \neq 0,$$

where

$$\tau^i = X^{q^i}, \quad \forall i \in \mathbb{Z}_{\geqslant 0}.$$

We let $K\{\tau\}$ denote the algebra of Ore polynomials. We say that $f = a_0 + \cdots + a_n \tau^n$ is called *monic* when $a_n = 1$; the coefficient a_0 is the *constant coefficient*, whereas a_n is the *leading coefficient*. Being defined as a composition, the multiplication in $K\{\tau\}$ is noncommutative as soon as K is strictly larger than $\mathbb{F}_q$. Indeed, for any $a \in K$, one has

$$a^q \tau = \tau a.$$

Elements in $K\{\tau\}$ are assigned a degree, called the τ-degree: the *τ-degree of f*, denoted $\deg_\tau(f)$, is n. As a regular polynomial in X, f would have degree $q^{\deg_\tau(f)}$.

Ore Polynomials were implemented in SageMath by Caruso, which played an instrumental role in the SageMath implementation of Drinfeld modules described in Chapter 3.

```
sage: K.<z> = GF(4)
sage: frob = K.frobenius_endomorphism()
sage: Ktau.<t> = OrePolynomialRing(K, frob)
sage: Ktau
Ore Polynomial Ring in t over Finite Field in z of size 2^2 twisted by z |--> z^2
sage: z * t
z*t
sage: t * z
(z + 1)*t
```

Furthermore, for z in $\overline{K}$ and f as before, we define

$$f(z) = \sum_{i=0}^{n} f_i z^{q^i}.$$

```
sage: f = 1 + z*t + (z+1)*t^2
sage: f(z)
z
sage: f(1)
0
```

1.1.1.2 Euclidean division of Ore polynomials

The noncommutativity of $K\{\tau\}$ is not an obstacle to efficient computations, as one can rely on the following property: $K\{\tau\}$ is left-Euclidean with respect to the τ-degree. More precisely, for any two Ore polynomials f and g in $K\{\tau\}$, there exist unique Ore polynomials α and β of $K\{\tau\}$ satisfying

$$\begin{cases} f = \alpha g + \beta, \\ \deg_\tau(\alpha) < \deg_\tau(\beta). \end{cases}$$

Therefore, left-ideals of $K\{\tau\}$ are all principal; they possess a unique monic generator called the *right-greatest common divisor*, abbreviated RGCD. More generally, we define the RGCD of any nonempty subset S of $K\{\tau\}$ as the RGCD of the left-ideal generated by S. The RGCD of two polynomials is easily computed. For starter, one can use a variant of Euclid's algorithm (see Algorithms 1 and 2). We also present techniques based on faster Ore polynomial multiplication in § 1.3.4 [CL17a; CL17b].

```
sage: f = t + t^2
sage: g = 1 + t
sage: h = t^2
sage: (alpha, beta) = f.right_quo_rem(g)
sage: (alpha, beta)
(t, 0)
sage: f == alpha * g + beta
True
sage: g.right_divides(h)
False
```

Remark 1.1.1. If K is a perfect field, the ring $K\{\tau\}$ is right-Euclidean, as per [Gos96, Section 1.6]. However, this is irrelevant to our work.

1.1.1.3 Separable Ore polynomials

Let $f \in K\{\tau\}$ be an Ore polynomial. The roots of f, seen as a q-polynomial, form a finite $\mathbb{F}_q$-vector space of $\overline{K}$, called the *kernel* of f and denoted $\mathrm{Ker}(f)$. Reciprocally, any regular polynomial whose roots form a $\mathbb{F}_q$-vector space in $\overline{K}$ is a q-polynomial, and as such, can be seen as an Ore polynomial. One says that f is *separable* whenever its kernel contains exactly $q^{\deg_\tau(f)}$ distinct elements, *i.e.* $\mathrm{Ker}(f)$ has $\mathbb{F}_q$-dimension $\deg_\tau(f)$. Equivalently, f is separable whenever its constant coefficient is nonzero. *Purely inseparable* Ore polynomials are, on the opposite, nonconstant Ore polynomials whose kernel is trivial, that is, nonzero powers of τ, up to a multiplicative factor in K.

Proposition 1.1.2. *Let $f \in K\{\tau\}$ be an Ore polynomial. We can decompose f as the product of a separable Ore polynomial $f_s \in K\{\tau\}$ and a purely inseparable one τ^h:*

$$f = f_s \tau^h$$

The integer h is called the *height* of f, and is denoted by $\mathrm{h}(f)$. This gives the following alternative formulation: an Ore polynomial is separable whenever its height is zero, and purely inseparable whenever its height is its τ-degree.

Remark 1.1.3. We can also decompose f as $f = \tau^h f_s'$. In fact, [LS24, § 1.3] writes $f_s\tau^h$ while [CL23, § 1.1.1] writes $\tau^h f_s'$. In [Gek91, § 1], Gekeler seems to choose $f_s\tau^h$. This bears little to no implication on our work.

Furthermore:

Proposition 1.1.4. *Let $f, g \in K\{\tau\}$ be two Ore polynomials. If f is separable,* $\mathrm{Ker}(f)$ *is in* $\mathrm{Ker}(g)$ *if and only if f right-divides g.*

Reciprocally, let V be a finite sub-$\mathbb{F}_q$-vector space of $\overline{K}$, such that the regular polynomial $\prod_{x\in V}(X+x)$ has coefficients in K. Then, by [Gos96, Theorem 1.2.1], it is a q-polynomial; it can thus be seen as an Ore polynomial. This induces a bijection between separable Ore polynomials—up to a multiplicative factor in K—and finite sub-$\mathbb{F}_q$-vector spaces of $\overline{K}$. The following is also true:

Proposition 1.1.5. *Let S be a nonempty set of Ore polynomials. The intersection of the kernels of elements of S is exactly the kernel of the* RGCD *of S.*

1.1.2 General Ore polynomials

Ore polynomials exist in greater generality than what is presented in § 1.1.1. Even if $K\{\tau\}$ is sufficient for defining Drinfeld modules, the material we present now is necessary for the framework of Chapter 6. For a more detailed survey on this topic, we refer to [Jac96, § I] or [Car17] (in French). In the course of our presentation, we also quickly review elementary results in the theory of central simple algebras; [Gos96, § 4.11] exposes this topic with Drinfeld modules in mind (see also [Car17, § 3]).

Let L be a ring equipped with a ring endomorphism

$$\theta : L \to L.$$

We form the ring

$$L[t;\theta],$$

whose elements are formal expressions of the form

$$a_0 + a_1 t + \cdots + a_n t^n \quad (n \in \mathbb{Z}_{\geqslant 0},\ a_0, \ldots, a_n \in L)$$

subject to the addition and multiplication driven by the rule

$$tb = \theta(b)t, \quad \forall b \in L.$$

The ring $L[t;\theta]$ is the ring of *Ore polynomials over L twisted by θ*; it is noncommutative unless θ is the identity morphism. From this point onward, we focus on the case where L is a field, as it is the scope of application of Chapter 6—in particular, when K is finite and over $\mathbb{F}_q$, $K\{\tau\}$ is $K[t;\mathrm{Frob}]$, where Frob is the q-Frobenius endomorphism of K. The ring $L[t;\theta]$ shares many properties with classical polynomial rings over fields. Notably, $L[t;\theta]$ is equipped with a notion of degree, and with a right-Euclidean division: given two Ore polynomials $f, g \in L[t;\theta]$ with $g \neq 0$, there exist uniquely determined $\alpha, \beta \in L[t;\theta]$ such that $f = \alpha g + \beta$ and $\deg \beta < \deg g$. As in the classical commutative case, this implies that $L[t;\theta]$ is left-Euclidean, and left-principal (*i.e.* all left ideals of $L[t;\theta]$ are generated by one element). From this property, we derive the existence of RGCD's: given $f, g \in L[t;\theta]$, the *right-greatest common divisor* of f and g, denoted by $\mathrm{RGCD}(f,g)$, is the unique monic polynomial satisfying the relation

$$L[t;\theta]\cdot f + L[t;\theta]\cdot g = L[t;\theta]\cdot \mathrm{RGCD}(f,g).$$

From now on, we further assume that θ has finite order d. This hypothesis ensures in particular that the center of $L[t;\theta]$ is large; precisely, it is the subring $F[t^d]$ where F denotes the subfield of L fixed by θ. By standard Galois theory, the extension L/F has degree d and it is Galois with cyclic Galois group generated by θ. In this situation, the *field of fractions of $L[t;\theta]$* can be defined by inverting the elements in the center: the noncommutative ring

$$\mathrm{Frac}(L[t;\theta]) = F(t^d) \otimes_{F[t^d]} L[t;\theta]$$

is a division algebra, and the smallest that contains $L[t;\theta]$. Besides, it is a central simple algebra over $F(t^d)$ [Jac96, Theorem 1.4.6], which provides us with a reduced norm map

$$N_{\mathrm{rd}} : \quad \mathrm{Frac}(L[t;\theta]) \quad \to \quad F(t^d).$$

The reduced norm is multiplicative and acts as the d-th power on $F(t^d)$; see [GS06, § 2.6] and [CL17a, § 3.3] (in French) for a precise definition.

We now explain how to compute $N_{\mathrm{rd}}(P)$, for nonzero P in $L[t;\theta]$. First of all, we form the quotient

$$D_P = L[t;\theta]/L[t;\theta]P,$$

which is an L-vector space of dimension $\deg(P)$ with basis $(1, t, \dots, t^{\deg(P)-1})$. Since t^d is a central element in $L[t;\theta]$, the multiplication by t^d defines an L-linear endomorphism of D_P, which we denote by

$$\gamma_P : \quad D_P \quad \to \quad D_P.$$

Its characteristic polynomial $\pi(\gamma_P)$ is a monic polynomial of degree $\deg(P)$. Most importantly, the reduced norm of P is retrieved by looking at the action of t^d (in our applications, this corresponds to the action of a Frobenius endomorphism) on the quotient D_P.

Proposition 1.1.6. *For all $P \in L[t;\theta]$, $P \neq 0$, we have*

$$N_{\mathrm{rd}}(P) = N_{L/F}\big(\mathrm{lc}(P)\big) \cdot \pi(\gamma_P)(t^d)$$

where $\mathrm{lc}(P)$ *is the leading coefficient of P and $N_{L/F}$ is the norm map from L to F (*i.e. $N_{L/F}(x) = \theta^0(x)\cdots\theta^{r-1}(x)$*).*

Proof. See [CL17a, Lemma 2.1.15]. □

Remark 1.1.7. Proposition 1.1.6 implies in particular that $N_{\mathrm{rd}}(P)$ is a polynomial whenever P is in $L[t;\theta]$ and that $\pi(\gamma_P)$ has coefficients in F. None of these properties seem immediate, from the definition.

1.2 Curves and function fields

While Drinfeld $\mathbb{F}_q[T]$-modules (§ 2.1) can be defined purely algebraically, without any reference to algebraic geometry, general Drinfeld modules (§ 2.1) on the other hand rely on curves and specific subrings of their function fields. We also need background on imaginary hyperelliptic curves and Mumford coordinates for Chapter 7.

Concretely, we review affine algebraic geometry in § 1.2.1, and build upon it to study projective algebraic geometry in § 1.2.2. In § 1.2.3, we define the degree-zero Picard group of a projective curve, and subsequently focus on imaginary hyperelliptic curves § 1.2.4. We conclude the section in § 1.2.5 by a brief analogy between number and function fields.

The content of this section is very classical, and largely inspired by [Séc20]. For details and proofs, we refer to [Sil09; Lor96; Vil06; Per08; Sil09; Rei88].

Finally, we let K be a field (not necessarily over $\mathbb{F}_q$, and not necessarily algebraically closed), and let also $\overline{K}$ be one of its algebraic closures.

1.2.1 Affine curves

While we mainly work with projective objects, affine geometry provides simpler definitions, that can be reused in projective geometry (§ 1.2.2).

1.2.1.1 Definition

We call *affine space of dimension n over* $\overline{K}$ and denote

$$\mathbb{A}^n(\overline{K})$$

the set $\overline{K}^n$. We now define two maps:

(i) For an ideal I in $K[X_1, \dots, X_n]$, we let $\mathrm{V}(I)$ be the set of elements in $\overline{K}$ that cancel every polynomial in I. A *point in* V is simply an element of V. With n being fixed, we call *K-affine algebraic set* or *algebraic set defined over K* any subspace of $\mathbb{A}^n(\overline{K})$ which equals $\mathrm{V}(I)$, for some ideal I of $K[X_1, \dots, X_n]$.

(ii) Conversely, to a subset V of $\mathbb{A}^n(\overline{K})$, one associates the ideal $\mathrm{I}(V)$ of polynomials in $K[X_1, \dots, X_n]$ annihilated by each point in V.

If an affine set is *irreducible*, i.e. when it is not the union of two nonempty affine sets with no inclusion of one into the other, we say that it is an *algebraic affine variety defined over K*, or *K-affine algebraic variety*. An algebraic affine set V is irreducible if and only if $\mathrm{I}(V)$ is a prime ideal. Notice that $\mathbb{A}^n(\overline{K})$ is the K-affine variety obtained from the zero ideal in $K[X_1, \dots, X_n]$. (From now on, we omit the adjective *algebraic*.)

1.2.1.2 Rational points

Let V be an affine K-variety defined in $\mathbb{A}^n(\overline{K})$. While K is an arbitrary field, notice that the affine space $\mathbb{A}^n(\overline{K})$ is defined on the algebraic closure $\overline{K}$. That way, any proper ideal I of $K[X_1, \dots, X_n]$ is associated with a nonempty variety $\mathrm{V}(I)$. However, being able to distinguish points that are defined over K (or any subextension L of $\overline{K}/K$) remains important. To do that, we define the *L-rational points of V*, whose set is denoted by

$$V(L),$$

as the points $(x_1, \dots, x_n)$ of V for which $x_1, \dots, x_n$ are in L. In particular, V equals $V(\overline{K})$, by definition.

1.2.1.3 Function fields

Let V be a K-affine variety of $\mathbb{A}^n(\overline{K})$. Consider the *coordinate ring of V*, defined as

$$K[V] = K[X_1, \dots, X_n]/\mathrm{I}(V).$$

Elements in $K[V]$ define functions from V to K. As V is irreducible, it is can be verified that $\mathrm{I}(V)$ is prime. We thus subsequently define the *function field of V* as the fraction field of the coordinate ring:

$$K(V) = \mathrm{Frac}(K[V]).$$

The elements of $K(V)$ are called *functions*.

One of the goals of algebraic geometry is to establish a duality between a geometric object and its function field; Hilbert's *Nullstellensatz* is a prime example of this philosophy [CLO15, § 4.1]. In that regard, it is important to be able to evaluate functions of $K(V)$. Let $P = (x_1, \dots, x_n)$ be a point (not necessarily K-rational) of V, and let f be a function of $K(V)$. If there exists g and h in $K[V]$ such that $f = \overline{g}/\overline{h}$ and $h(x_1, \dots, x_n)$ is not 0, then f can be evaluated at P, defining $f(P) = g(x_0, \dots, x_n)/h(x_0, \dots, x_n)$. In that case, we say that f is *well-defined* at P. However, $h(x_0, \dots, x_n)$ may be zero, and we need to allow ourselves using the notion of *pole*. We postpone this to § 1.2.1.6.

1.2.1.4 Dimension

Let V be as in § 1.2.1.3. The *dimension* of V is the transcendence degree of $K(V)$ over K. A *curve* is a variety with dimension one; its function field is an algebraic extension of $K(T)$. Consequently, the following characterization can be used as an alternative definition of function fields:

Proposition 1.2.1. *Algebraic function fields with dimension n over K are the finite algebraic extensions of* $K(X_1, \dots, X_n)$.

The simplest function field is $K(T)$, obtained as that of $\mathbb{A}^1(\overline{K})$, seen as a K-variety. Furthermore, every function field as defined by Proposition 1.2.1 occurs as the function field of an affine variety.

Remark 1.2.2. Although this is out of the scope of our needs, we mention that for a well-suited notion of morphism between varieties [Silo9, § I.3, § II.2], two affine varieties V and W are isomorphic if and only if $K[V]$ and $K[W]$ are isomorphic as K-algebras. This equivalence is explicit and contravariant, in the sense that a morphism of varieties $V \to W$ over K gives a morphism of K-algebras $K[W] \to K[V]$, and vice versa. In fact, the category of affine sets over K and that of reduced finite type K-algebras are anti-equivalent under the functor $V \to K[V]$.

1.2.1.5 Singular and nonsingular points

Let V and P be as in § 1.2.1.6, and let d be the dimension of V. We first define *singular* and *nonsingular* K-rational points. Our definition is classical, and relies on partial derivatives: one says that a point P is *nonsingular* when for any system of generators $g_1, \dots, g_r$ of $\mathrm{I}(V)$, the rank of the *Jacobian matrix*

$$\begin{pmatrix} \frac{\partial g_1}{\partial X_1} & \cdots & \frac{\partial g_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial g_r}{\partial X_1} & \cdots & \frac{\partial g_r}{\partial X_n} \end{pmatrix},$$

evaluated at P, is exactly $n - d$. Otherwise, P is said to be singular. We say that V is *smooth* when none of its points are singular. See § 1.2.1.7 for a more advanced study when the variety is a smooth curve.

1.2.1.6 Zeros and poles

Let V be as in § 1.2.1.3, and let $P = (x_1, \dots, x_n)$ be a point of $V(K)$; that is, P is K-rational. Recall the discussion at the end of § 1.2.1.3, and consider the ideal

$$\mathfrak{m}_{V,P} \subset K[V]$$

generated by the functions in $K[V]$ whose P is a zero, meaning functions $f = \overline{g}$ satisfying $g(x_1, \dots, x_n) = 0$. In concrete terms, $\mathfrak{m}_{V,P}$ is generated by the classes modulo $\mathrm{I}(V)$ of the polynomials $X_1 - x_1, \dots, X_n - x_n$. Therefore, $\mathfrak{m}_{V,P}$ is maximal, and we let

$$K[V]_P$$

be the localization of $K[V]$ at $\mathfrak{m}_{V,P}$. It is a crucial result that:

Proposition 1.2.3. *The ring* $K[V]_P$ *is integral, local and noetherian.*

The unique maximal ideal of $K[V]_P$ is denoted $\mathfrak{m}_P$, so that

$$\mathfrak{m}_{V,P} = \mathfrak{m}_P \cap K[V].$$

We now assume that P is nonsingular. Let now f be a function in $K(V)$: at least one of f or $1/f$ (if f is nonzero) is contained in $K[V]_P$, and:

— If f is contained in $\mathfrak{m}_P$, we say that P is a *zero* of f, and write $f(P) = 0$.

— If f is nonzero and P is a zero of $1/f$, we say that P is a *pole* of f and write $f(P) = \infty$.

We say that f *is regular at* P if P is not a pole of f. When P is neither a zero nor a pole, we define $f(P) = g(x_1, \dots, x_n)/h(x_1, \dots, x_n)$, for $f = \overline{g}/\overline{h}$.

1.2.1.7 Discrete valuations from nonsingular points

Let V and P be as in § 1.2.1.6, Under stricter hypotheses, zeros and poles can be classified. For curves, Proposition 1.2.3 extends to:

Proposition 1.2.4. *Assuming $C = V$ is a curve, then P is nonsingular if and only if $K[C]_P$ is a discrete valuation ring. In particular, C is smooth if and only if its coordinate ring $K[C]$ is a Dedekind domain.*

For the end of this section, let us assume that $C = V$ is a curve, and that P is nonsingular. The discrete valuation we consider in Proposition 1.2.4 is the $\mathfrak{m}_P$-adic valuation on $K(C)$. It is denoted by v_P. Let $f \in K(V)$ be a function. We classify zeros and poles as follows:

— If P is a zero of f, we call *order of P at f* the integer $v_P(f)$.

— If P is a pole of f, its we call *order of P at f* the integer $-v_P(f)$. In particular, the function P is regular at f if and only if $v_P(f) \geqslant 0$.

Remark 1.2.5. It is interesting to ask if all discrete valuations on $K(C)$ come from nonsingular points on $C(K)$. Taking the example of the curve $C = \mathbb{A}^1(K)$, we see that $K(C) = K(T)$, and that the degree map gives rise to a valuation whose valuation v_∞ defined by

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

This valuation, called the *valuation at infinity*, is the only one on $K(T)$ that does not correspond to any point of $\mathbb{A}^1(K)$. Projective curves conveniently lift this irregularity, introducing the notion of *point at infinity*. We formalize this in § 1.2.2.

1.2.2 Projective curves

Considering projective varieties allows for more liberty, while still relying on many statements of affine algebraic geometry (§ 1.2.1). In particular, elliptic and hyperelliptic curves are projective curves.

1.2.2.1 Projective space

We call *projective space of dimension n over* $\overline{K}$ and denote

$$\mathbb{P}^n(\overline{K})$$

the quotient of $\overline{K}^{n+1}$ by the following equivalence relation: two vectors x and x' in $\overline{K}^{n+1}$ are equivalent if $x = \lambda x'$ for some nonzero λ in $\overline{K}$. Therefore, elements in $\mathbb{P}^n(\overline{K})$ are represented by coordinates denoted

$$(x_0 : \cdots : x_n), \quad x_0, \ldots, x_n \in \overline{K}$$

that are not all zero. In practice, and given the definition of the projective space, one coordinate is often assumed to be 1.

1.2.2.2 Cancelling polynomials

To define projective varieties, a preliminary step is to assert when a polynomial is annihilated by an element of $\mathbb{P}^n(\overline{K})$. Let f be a polynomial in $K[X_0, \ldots, X_n]$ and $P = (x_0 : \cdots : x_n)$ be in $\mathbb{P}^n(\overline{K})$. Given that the coordinates of P are not unique, defining $f(P)$ is not possible. However, if f is homogeneous, then $f(x_0, \ldots, x_n)$ is zero if and only if, for any λ in $\overline{K}$, $f(\lambda x_0, \ldots, \lambda x_n)$ is zero. Consequently, we say that f *is zero at* P, and write $f(P) = 0$, whenever $f(x_0, \ldots, x_n) = 0$. We say that an ideal I of $K[X_0, \ldots, X_n]$ is *homogeneous* when it is generated by homogeneous polynomials.

1.2.2.3 Projective varieties

Following § 1.2.1, we define maps I and V. One slight difference is that V is only defined on homogeneous ideals.

(i) For an homogeneous ideal I of $K[X_0, \ldots, X_n]$, $\mathrm{V}(I)$ is the set of points P in $\mathbb{P}^n(\overline{K})$ such that $f(P) = 0$ for all homogeneous f in I.

(ii) Reciprocally, for a subset V of $\mathbb{P}^n(\overline{K})$, we let $\mathrm{I}(V)$ be the ideal of polynomials f in $K[X_0, \ldots, X_n]$ such that $f(P) = 0$ for every point P in V.

An *algebraic projective set defined over* K, or *K-algebraic projective set* is then defined as a subspace of $\mathbb{P}^n(\overline{K})$ of the form $\mathrm{V}(I)$, for some homogeneous ideal I of $K[X_0, \ldots, X_n]$. A *point of* V is, again, simply an element of V. An *irreducible* algebraic projective set is an algebraic projective set that cannot be written as the union of two nonempty algebraic projective sets with no inclusion of one into the other. Such a set is called an *algebraic projective variety defined over* K, or *K-algebraic projective variety*. An algebraic projective set V is irreducible if and only if $\mathrm{I}(V)$ is a prime ideal. Notice that $\mathbb{P}^n(\overline{K})$ is the K-projective variety obtained from the zero ideal in $K[X_0, \ldots, X_n]$. (And as before, we now elect to omit the adjective *algebraic*.)

1.2.2.4 Rational points

Let V be a K-projective variety of $\mathbb{P}^n(K)$. We now let L be a subextension of $\overline{K}/K$, the *L-rational* of V, following § 1.2.1.2. The *L-rational points of* V, whose set is denoted $V(L)$, are the points of V that admit a tuple of projective coordinates that are all in L. In particular, V equals $V(\overline{K})$, and a point of V is always assumed to be a point of $V(\overline{K})$.

1.2.2.5 Affine charts and function field

One may have notice that there exist embeddings from $\mathbb{A}^n(\overline{K})$ into $\mathbb{P}^n(\overline{K})$. In fact, those are very useful to define the function field of a projective variety. For any index $0 \leqslant i \leqslant n$, let U_i be the subset of $\mathbb{P}^n(\overline{K})$ with points whose i-th coordinate is nonzero. The canonical map

$$\begin{array}{rccc} \varphi_i : & \mathbb{A}^n(\overline{K}) & \to & U_i \\ & (x_1, \ldots, x_n) & \mapsto & [x_1 : \cdots : x_{i-1} : 1 : x_{i+1} : \cdots : x_n]. \end{array}$$

is a bijection, and we say that the couple (i, U_i) is an *affine chart*. Therefore, affine varieties can be embedded into the projective space, and projective varieties can be restricted to affine varieties. Let V be as in § 1.2.2.4.

(i) The projective subvarieties of $\mathbb{P}^n(\overline{K})$ form the closed subsets of a topological space. While the image $\varphi_i(V_\mathbb{A})$ is not a variety, we can consider its topological closure

$$\overline{\varphi_i(V_\mathbb{A})}.$$

Up to isomorphism of projective varieties, it does not depend on i, and we say that it is *the projective closure* of $\mathrm{V}_\mathbb{A}$. We denote it by $\overline{V_\mathbb{A}}$.

(ii) Reciprocally, any projective variety $V_\mathbb{P}$ can be restricted to an affine variety, by choosing an index $0 \leqslant i \leqslant n$ and considering $\varphi_i^{-1}(V_\mathbb{P} \cap U_i)$, which is either empty or an affine variety. In the latter case, we say that

$$\varphi_i^{-1}(V_\mathbb{P} \cap U_i)$$

is an *affine restriction* of $V_\mathbb{P}$. Most importantly, the projective closure of $\varphi_i^{-1}(V_\mathbb{P} \cap U_i)$, provided that $\varphi_i^{-1}(V_\mathbb{P} \cap U_i)$ is nonempty, is equal to $V_\mathbb{P}$.

Therefore, we define the *function field* of $V_\mathbb{P}$, up to isomorphism of K-algebra, as that of any of the nonempty affine restrictions of $V_\mathbb{P}$. This also allows to define the *dimension* of V as that of $V_\mathbb{P}$, and leads to the following definition:

Definition 1.2.6. A *function field with dimension n over K* is a field isomorphic to $K(V)$, where V is a K-projective variety of dimension n.

More prosaically, a function field with dimension n over K is isomorphic to an algebraic extension of $K(X_1, \ldots, X_n)$ (Proposition 1.2.1).

Remark 1.2.7. Recall Remark 1.2.5. Although we do not prove it, we mention that all valuations on $K(V)$—which is the function field of both an affine and a projective variety—correspond to points of V.

1.2.2.6 Evaluating functions

Let V be as in § 1.2.2.4, let f be a function in $K(V)$, and let P be a point (not necessarily K-rational) of V. Let (U_i, φ_i) be an affine chart such that U_i contains P, which always exists. The function f corresponds to a function f_i in $K(V_i)$, with

$$V_i = \varphi_i^{-1}(V \cap U_i).$$

Letting P_i be $\varphi_i^{-1}(P)$, and we can show that the value of $f_i(P_i)$ does not depend on the choice of the affine chart (j, U_j), provided that $\varphi_j^{-1}(V)$ is nonempty. Therefore, we define

$$f(P) = f_i(P_i).$$

Recalling § 1.2.1.6, we say that *P is a zero of f* (resp. *a pole*) whenever P_i is a zero (resp. *a zero*) of f_i.

Example 1.2.8. Defining function fields up to isomorphism and with respect to affine charts has the advantage of bypassing the need for *sheaves*. Despite this, evaluating a function can be tedious. Consider $C = \mathbb{P}^1(\overline{K})$, the K-projective curve generated by the zero ideal in $K[X, Y]$. It is often decomposed in an affine part of $\varphi_1^{-1}(U_1)$ and a single point at infinity $(1 : 0)$, contained in U_0. The function field of $\varphi_1^{-1}(U_1)$ is $K(X)$, and so $K(X)$ is the function field of $\mathbb{P}^1(K)$, up to isomorphism. Evaluating functions f of $K(X)$ on points of U_1 is easy: $f((x : 1)) = f(x)$; our goal is to define the evaluation of f at the point at infinity. For this purpose, consider a point $(x : y)$ of $\mathbb{P}^1(K)$ such that $xy \neq 0$. Such a point belongs to both U_0 and U_1.

(i) Writing $(x : y) = (1 : y/x) \in U_0$, we see that the function field of $\varphi_0^{-1}(U_0 \cap C)$ is $K(Y)$, and for any g_Y in $K(Y)$, one defines $g_Y((x : y)) = g_Y(y/x)$.

(ii) Writing $(x : y) = (x/y : 1) \in U_1$, we see that the function field of $\varphi_0^{-1}(U_1 \cap C)$ is $K(X)$, and for any g_X in $K(X)$, one defines $g_X((x : y)) = g_X(x/y)$.

Choosing g_Y and g_X representing the same function in the function field of $\mathbb{P}^1(K)$, the values $g_X(x/y)$ and $g_Y(y/x)$ must agree. This shows that the function $g_X(X)$ in $K(X)$ represents the function $g_X(1/Y)$ in $K(Y)$, and vice versa. Therefore, for any $f \in K(X)$, $f((1 : 0))$ is the evaluation of $f(1/X)$ at 0. Consequently, f has a pole at infinity if and only if $f(1/X)$ has a pole at zero. Write $f(X) = g(T)/h(T)$, where g and h are coprime. Then $f(X)$ has a pole at infinity if and only if $\deg(f(X)) > \deg(g(X))$. This proves that the discrete valuation ring

$$\{f(X)/g(X) : g(X) \neq 0, \deg(f) \leqslant \deg(g)\}$$

and its discrete valuation both correspond to the point at infinity in $\mathbb{P}^n(\overline{K})$.

Following Example 1.2.8 and Remark 1.2.5, we introduce the following fundamental definition:

Definition 1.2.9. We call *valuation at infinity on $K(T)$* the valuation corresponding to the unique point at infinity on $\mathbb{P}^1(\overline{K})$. It is denoted by v_∞, and defined by

$$\begin{array}{rccl} v_\infty : & K(T) & \to & \mathbb{Z} \cup \{-\infty\} \\ & f & \mapsto & \begin{cases} -\infty & \text{if} \quad f = 0, \\ \deg(h) - \deg(g) & \text{if} \quad f = g/h \text{ and } f \neq 0. \end{cases} \end{array}$$

Its associated valuation ring is

$$\left\{g/h \in K(T) : \deg(h) \geqslant \deg(g)\right\}$$

and the unique maximal ideal of the valuation ring is

$$\left\{g/h \in K(T) : \deg(h) > \deg(g)\right\}.$$

Remark 1.2.10. In the literature, it is common to use the concept of *place* instead of valuations and valuation rings. The three notions are equivalent; we refer to [Vilo6, § 2.2] for details.

1.2.3 Picard group

Having defined affine and projective curves, and their function fields in both those cases, we turn to a new object: the *Picard group*. The Picard group is an invariant attached to any projective curve; in some cases, it corresponds to the class group of the coordinate ring. This new characterization gives new algorithmic tools (namely, *Mumford coordinates* § 1.2.4.3), that we use in Chapter 7.

From now on, we assume that K is perfect. In our applications, this assumption will hold in virtue of K being a finite field.

1.2.3.1 Divisors

The notion of *Picard group* builds on that of *divisor*. Let C be a projective curve. We call *divisor on* C any formal sum

$$\sum_{P \in C} n_P P, \quad n_P \in \mathbb{Z}, \quad P \in C,$$

of points of C whose support is finite. Divisors on C form a group denoted $\mathrm{Div}(C)$. Let L be a subextension of $\overline{K}/K$. The galois group $\mathrm{Gal}(\overline{K}/L)$ of L over K acts on $\mathrm{Div}(C)$ via:

$$\begin{array}{rcl} \mathrm{Gal}(\overline{K}/L) \times \mathrm{Div}(C) & \to & \mathrm{Div}(C) \\ (\sigma, \sum_{P \in C} n_P P) & \mapsto & \sum_{P \in C} n_P P^\sigma, \end{array}$$

where if $P = (x_1 : \cdots : x_n)$, we set

$$P^\sigma = (\sigma(x_0) : \cdots : \sigma(x_n)).$$

One says that a divisor is *defined over* L when it is stable under the Galois action of $\mathrm{Gal}(\overline{K}/L)$. The subgroup they form is denoted $\mathrm{Div}_L(C)$; we have, $\mathrm{Div}(C) = \mathrm{Div}_{\overline{K}}(C)$.

1.2.3.2 Picard group

Among divisors, some come from functions in $K(C)$. Define the *degree* of a divisor $D = \sum_{P \in C} n_P C$ as the integer

$$\deg(D) = \sum n_P.$$

Consider a function $f \in K(C)$. It has zeros $P_0, \ldots, P_m$ with respective orders $m_0, \ldots, m_m$ and poles $P'_0, \ldots, P'_n$ with respective orders $m'_0, \ldots, m'_m$. We define

$$\mathrm{Div}(f) = \sum_i m_i P_i - \sum_i m'_i P'_i,$$

and call any such divisor (*i.e.* any divisor that is equal to $\mathrm{Div}(g)$ for some g in $K(C)$) a *principal divisor*. We can show that principal divisors are defined over K, and that they have degree zero. However, the converse is not true: not all degree zero divisors defined over K are principal. We then let

$$\mathrm{Div}^0(C)$$

be the subgroup of $\mathrm{Div}(C)$ generated by degree zero divisors, and

$$\mathrm{Pr}(C)$$

be the subgroup of $\mathrm{Div}^0(C)$ generated by principal divisors. We define the *degree zero-Picard group* (or simply *Picard group*) of C, and denote it as $\mathrm{Pic}^0(C)$, as the group quotient

$$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Pr}(C).$$

Remark 1.2.11. We refer to [Coh+12, § 14.1] for a geometrical interpretation of the definition of the Picard group. For elliptic curves, the Picard group is isomorphic to the group of rational points.

Remark 1.2.12. It is not clear how to efficiently represent the Picard group of C, given that the classes of $\mathrm{Div}^0(C)/\mathrm{Pr}(C)$ may involve points that are not K-rational. In § 1.2.4.3, we will see that in the case of imaginary hyperelliptic curves, efficient representation of and fast arithmetic in the Picard group are possible.

1.2.4 Imaginary hyperelliptic curves

We now turn to a specific class of projective curves and function fields: real and imaginary hyperelliptic function fields. Only the latter matter to us, due to their algorithmic properties.

1.2.4.1 Imaginary and real quadratic function fields

A *quadratic function field over K* is a degree two extension κ of $K(T)$, the function field of $\mathbb{P}^1(\overline{K})$. Following the terminology of algebraic number theory in number fields, we now introduce *real* and *imaginary* quadratic function fields. Consider the point at infinity on $\mathbb{P}^1(\mathbb{F}_q)$, together with its valuation v_∞ (Definition 1.2.9). There are two possibilities:

Definition 1.2.13. The valuation at infinity v_∞ extends to either one or two valuations on κ. In the former case, κ is called *real*; in the latter case, κ is called *imaginary*.

Remark 1.2.14. Let $\mathbb{Q}(\sqrt{d})$ be a quadratic number field, where d is a squarefree nonzero positive integer. A norm on $\mathbb{Z}$ is either a p-adic norm, or the euclidean norm, which is the analogue of the norm at infinity on $\mathbb{F}_q[T]$. If $d < 0$, *i.e.* $\mathbb{Q}(\sqrt{d})$ is imaginary, then the euclidean norm on $\mathbb{Q}$ only extends to the usual complex archimedean norm. If otherwise $d > 0$, *i.e.* $\mathbb{Q}(\sqrt{d})$ is real, then the euclidean norm extends to the usual archimedean norm, as well as to the norm defined by $a + \sqrt{d}b \mapsto \sqrt{a^2 + b^2}$. We refer to [Car18, Section 3.2] or to [Ros02] for details.

1.2.4.2 Imaginary hyperelliptic function fields

Among quadratic imaginary function fields, these obtained from a so-called *hyperelliptic curve* enjoy a privileged status. Such curves can be defined in various level of generality, and we refer to [Gal12, Section 10] or [Eng00] for details. In our applications, the only hyperelliptic curves that arise are *imaginary* and defined over $\mathbb{F}_q$, meaning that their function field is a quadratic imaginary function field over $\mathbb{F}_q$. We use the following characterization:

Proposition 1.2.15. *Let C be a projective curve of $\mathbb{P}^2(\overline{\mathbb{F}_q})$ defined by an affine equation of the form*

$$Y^2 + h(X)Y - f(X) = 0.$$

If C has no singularity in the affine plane, if $\deg(f) = 2g + 1$ for some $g \geqslant 2$, and if $\deg(h) \leqslant g$, then we say that C is an imaginary hyperelliptic curve with genus g over K.

Remark 1.2.16. Notice that f is not required to be monic: this would be incompatible with the hyperelliptic curves that naturally arise in Chapter 7. However, we warn the reader that for simplicity, many introductory texts on hyperelliptic curve assume f to be monic; see [Coh+12] or [JSS10, Chapter 14].

1.2.4.3 Mumford coordinates

A fundamental aspect of imaginary hyperelliptic curves defined over $\mathbb{F}_q$—and our main motivation to use them—is that arithmetic in their Picard group can be efficiently performed using so-called *Mumford coordinates*. Let $\mathcal{H}$ be a hyperelliptic curve as in Proposition 1.2.15. Recall that the coordinate ring $K[\mathcal{H}]$ of $\mathcal{H}$ is

$$K[X, Y]/(Y^2 + h(X)Y - f(X)).$$

As $\mathcal{H}$ is smooth in the affine plane, $K[\mathcal{H}]$ is a Dedekind domain, to which a class group is associated.

Theorem 1.2.17. *Any element of* $\mathrm{Pic}^0(\mathcal{H})$ *can then be represented by a couple of polynomials* (ρ, σ) *in* $K[X]^2$ *such that* u *is monic,* $\deg(\sigma) < \deg(\rho) \leqslant g$*, and* ρ *divides* $\sigma^2 + \sigma h - f$*. The pair* (ρ, σ) *represents the ideal class of* $(\sigma(X), Y - \rho(X))$ *in* $K[\mathcal{H}]$.

The pairs (ρ, σ) are called *Mumford coordinates*. Furthermore, given an ideal $\mathfrak{a}$ in $K[\mathcal{H}]$ presented by its generators, the Mumford coordinates associated to its class in $\mathrm{Cl}(A_{\mathcal{H}})$ can be efficiently computed using the reduction step of Cantor's algorithm [Coh+12, Algo. 14.7].

Remark 1.2.18. Mumford coordinates are traditionally denoted by (u, v). But in our case, u will refer to a morphism of Drinfeld modules.

1.2.5 Function fields and number fields

We conclude this section on curves and function fields by drawing classical analogies between number and function fields.

1.2.5.1 Function field analogues of $\mathbb{R}$ and $\mathbb{C}$

We now overview the basic parallel between function fields and number fields. We recall that by definition, number fields are finite extensions of $\mathbb{Q}$, that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the archimedean norm, and that $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$. We build analogue objects in the context of function fields, where the ring of polynomials $\mathbb{F}_q[T]$ plays the role of $\mathbb{Z}$. But on the side of function fields, algebraic structures interact with geometric structures. The fraction field $\mathbb{F}_q(T)$ of $\mathbb{F}_q[T]$ is also the function field of the smooth projective curve $\mathbb{P}^1(\mathbb{F}_q)$. Valuations on $\mathbb{F}_q(T)$ are all non archimedean, they either correspond to affine points, or to the unique point at infinity of $\mathbb{P}^1(\mathbb{F}_q)$. We define $\mathbb{R}_\infty$—the function field analogue of $\mathbb{R}$—as the completion of $\mathbb{F}_q(T)$ with respect to this valuation. The algebraic closure of $\overline{\mathbb{R}_\infty}$ of $\mathbb{R}_\infty$ is not complete, so we define $\mathbb{C}_\infty$ as the completion of an algebraic closure of $\overline{\mathbb{R}_\infty}$.

1.2.5.2 Quadratic imaginary fields

In algebraic number theory, quadratic imaginary number fields enjoy a special focus. First of all, the endomorphism ring of an elliptic curve is either $\mathbb{Z}$, a maximal order in a quaternion algebra, or an order in a quadratic imaginary number field, and each such order appears as the endomorphism ring of some elliptic curve (we will see in § 2.1.5 that a similar statement holds for Drinfeld modules). We in fact discuss

the computation of the order of the class group of an imaginary quadratic number field in § A.1.3.2. The computation we mention is very costly, while its function field analogue is completely doable. Second, the Hilbert class field (an important object from class field theory) of a quadratic imaginary number field can be explicitly described as the extension of K generated by the j-invariants of elliptic curves with complex multiplication in this field. The imaginary quadratic function fields we have defined in § 1.2.4 are exactly the function field analogues of these fields.

1.3 Algorithms and complexity

We now focus on complexity and algorithms. We begin by specifying our complexity model (§ 1.3.1), and put emphasis on the complexity of operations in a finite field. In the remaining subsections, we mention algorithmic primitives for finite fields (§ 1.3.2), polynomial matrices (§ 1.3.3), and Ore polynomials (§ 1.3.4). These primitives are used in most our algorithmic contributions.

1.3.1 Complexity model

All our algorithms involve arithmetic in an extension K of $\mathbb{F}_q$. We encounter three situations:

(i) When no further hypothesis on K is provided, we account for arithmetic operations in K (additions, subtractions, multiplications, divisions) and *applications of the Frobenius endomorphism* (*i.e.* computing x^q given $x \in K$); these are counted separately.

(ii) When K is a finite field with degree d over $\mathbb{F}_q$, then:

  (a) Either we keep separating arithmetic operations and applications of the Frobenius endomorphism.

  (b) Or, when relevant, we use Kedlaya and Umans' algorithm for modular composition [KU11] to speed up applications of the Frobenius endomorphism. In that case, both arithmetic operations in K and applications of the Frobenius endomorphism are accounted for under bit operations. See § 1.3.2 for details.

We use the following notations. For two positive quantities f and g depending on parameters, we write

— $g \in O(f)$ if there exists an absolute positive constant C such that $g \leqslant C \cdot f$ for all choices of parameters,

— $g \in O^{\sim}(f)$ if there exist absolute positive constants C and k such that $g \leqslant C \cdot f \log^k f$ for all choices of parameters,

— $g \in O^{\bullet}(f)$ if, for all $\varepsilon > 0$, there exists a positive constant C_ε such that $g \leqslant C_\varepsilon \cdot f^{1+\varepsilon}$ for all choices of parameters. In other words, $g \in O^{\bullet}(f)$ if and only if $g \in (f)^{1+o(1)}$.

Unsurprisingly, we have

$$O(f) \subset O^{\sim}(f) \subset O^{\bullet}(f).$$

1.3.1.1 Asymptotic complexity

All our algorithms are accompanied by asymptotic complexity analyses. However, we stress that asymptotic analyses are not to be considered as a prediction of real-world run times: *Big O* notations merely account for asymptotic behaviors with input sizes growing to infinity. In practice, many state of the art algorithms are called *galactic*, in the sense that their efficiency is only observed for inputs of significant size. This is the case for matrix multiplication (and consequently computation of determinants and characteristic polynomials), fast Ore polynomial arithmetics, and Kedlaya and Umans' algorithm for modular composition (and consequently Frobenius endomorphism applications). Those problems are actively being worked on: at the time of writing this thesis, the latest progress on algorithmic matrix computation were published in 2024 [Wil+24], while substantial substantial progress were made for power series compositions [KL24], opening new perspectives for modular composition. In the meantime, it is reasonable to build our implementations upon reliable and pre-existing algorithmic routines, such as Euclid's classical algorithm for Ore polynomials, or Karatsuba's algorithm for matrix multiplication. Those offer a balance between practical efficiency, asymptotic complexity, and ease of implementation. We also provide benchmarks of the algorithms we implemented (§ 4.4, § 5.4, and § 6.4).

1.3.2 Algorithms for finite fields

In this subsection, K is a finite extension of $\mathbb{F}_q$ of degree d.

1.3.2.1 Basic operations

We represent K as a quotient of $\mathbb{F}_q[T]$. Classical algorithms based on Fast Fourier Transform allows for performing all arithmetic operations in K for a cost of $O^{\sim}(d \log q)$ bit operations (see for instance [GG13, Chapter II]).

1.3.2.2 Cost of applying the Frobenius endomorphism

Estimating the cost of applying the Frobenius endomorphism of K is more challenging, even though partial results are available in the literature. Several options are possible:

(i) Fast-exponentiation allows to compute images under the Frobenius endomorphism for a cost of $O(d \log q)$ multiplications in $\mathbb{F}_q$, i.e. $O^{\sim}(d \log(q)^2)$ bit operations.

(ii) Kedlaya and Umans' algorithm [KU11] for fast modular composition can compute an application of the Frobenius endomorphism for a cost of $O^{\bullet}(d \log q)$ bit operations. However, if α denotes the image of T in K, an initial precompututation of α^q is required, for a cost of $O^{\sim}(d \log^2 q)$ bit operations using fast exponentiation. We note that, as far as we know, no practical implementation of Kedlaya and Umans' algorithm exists.

(iii) Representing K with a *normal basis* over $\mathbb{F}_q$, *i.e.* a basis of the form $(\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}})$ for some α in K, applications of the Frobenius endomorphism are performed by shifting coordinates, which costs $O(1)$ operations. However, multiplications in K would cost more. In best cases, when the normal basis is called *optimal*, a multiplication in K costs $O(d^2)$ multiplications in $\mathbb{F}_q$, which is too much for our needs. In [CL09], Couveignes and Lercier introduced *elliptic* and *elliptic normal* bases. In the latter, Frobenius endomorphism applications can still be computed by shifting coordinates, and other arithmetic operations in K can all be computed for a cost of $O^{\sim}(d \log(q)^4)$ operations in

$\mathbb{F}_q$. Couveignes and Lercier proved that each finite field extension can be equipped with a normal elliptic basis. However, the cost of building such bases was not yet formally investigated.

Taking all of this into account, we choose to follow the convention of [MS23] and opt for the second option: we make the assumption that all arithmetic operations in K—including applications of Frobenius endomorphism—in K cost $O^{\bullet}(d \log q)$ bit operations, plus a unique initial cost of $O^{\sim}(d \log^2 q)$ operations for the precomputation of α^q. The reader interested in keeping the distinction between regular operations and Frobenius operations may refer to complexity statements given for arbitrary fields.

1.3.3 Algorithms for polynomial matrices

Algorithms of Chapters 4, 5, and 6 require computing determinants and characteristic polynomials of *polynomial matrices* with coefficients in $K[T]$. We give a basic review of the literature on these computations. Let

$$2 \leqslant \omega \leqslant 3$$

be a *feasible exponent for matrix multiplication*, *i.e.* a real number ω such that two matrices of size s with coefficients in K may be multiplied with $O^{\sim}(s^{\omega})$ operations in K. For matrices with coefficients in a field, computations of determinants and characteristic polynomials reduce to matrix computation, and can also be achieved for a cost of $O^{\sim}(s^{\omega})$ operations in the base field [PS07; NP21].

When the coefficients are polynomials, this remains true for the sole determinant [GJV03; JV06]; as of the time of writing this thesis, no reduction from characteristic polynomial computation to matrix multiplication has been found for polynomial matrices. Kaltofen and Villard propose algorithms to compute such characteristic polynomials for a cost of $O^{\sim}(s^{\Omega} n)$ operations in K, taking Ω approximately equal to 2.69497 [Kal92; KV05]. Therefore, we will let

$$\Omega$$

denote a *feasible exponent for characteristic polynomial computation of polynomial matrices*. For comparison, as of today, the best feasible exponent for matrix multiplication ω roughly equals 2.37286 [AW21].

Remark 1.3.1. In § 4.3.1.1, we derive two lemmas enhancing the complexity of computing the characteristic polynomial of a polynomial matrix in some specific cases that we will encounter.

1.3.4 Algorithms for Ore polynomials

The algorithmic toolbox of Ore polynomials is quite developed. With minor modifications to the classical Euclidean algorithm, Ore Euclidean divisions and RGCD' may be computed in polynomial time; see § 4.3.1.2 for precise statements. In the meantime, we review fast arithmetics for Ore polynomials, as initially developed by Caruso and Leborgne [CL17a; CL17b]. In these papers, the complexity is given in number of operations in the ground field $\mathbb{F}_q$, and the algorithms are Las Vegas.

Remark 1.3.2. We warn that the authors assume that applying the Frobenius endomorphism of K requires at most $O^{\sim}(d)$ operations in $\mathbb{F}_q$. Consequently one operation in $\mathbb{F}_q$ in the setting of [CL17b] corresponds to $O^{\bullet}(\log q)$ bit operations. We also mention that there is a typo in [CL17b]: the critical exponent is not $\frac{5-\omega}{2}$ but $\frac{2}{5-\omega}$.

We assume K to be an extension of $\mathbb{F}_q$ with degree d and let $\mathrm{SM}(n,d)$ denote a function such that multiplying two Ore polynomials in $K\{\tau\}$ of degree less than n costs $O^\bullet(\mathrm{SM}(n,d)\log q)$ bit operations. At the time of writing this thesis, the best known value of SM is given in [CL17b]:

$$\begin{aligned}\mathrm{SM}(n,d) &= n^{\frac{\omega+1}{2}}d && \text{for } n \leqslant d^{\frac{2}{5-\omega}},\\ &= n^{\omega-2}d^2 && \text{for } d^{\frac{2}{5-\omega}} \leqslant n \leqslant d,\\ &= nd^{\omega-1} && \text{for } d \leqslant n.\end{aligned}$$

Let also $\mathrm{SM}^{\geqslant 1}$ be the smallest log-concave function above SM, defined by

$$\mathrm{SM}^{\geqslant 1}(n,d) = \sup_{0<m\leqslant n} \mathrm{SM}(m,d)\frac{n}{m}.$$

Computing the right-Euclidean division of Ore polynomials in $K\{\tau\}$ of degree less than n requires at most $O^\bullet(\mathrm{SM}^{\geqslant 1}(n,d)\log q)$ bit operations [CL17b]. With the above values for $\mathrm{SM}(n,d)$, we have

$$\begin{aligned}\mathrm{SM}^{\geqslant 1}(n,d) &= n^{\frac{\omega+1}{2}}d && \text{for } n \leqslant d^{\frac{2}{5-\omega}},\\ &= nd^{\frac{4}{5-\omega}} && \text{for } d^{\frac{2}{5-\omega}} \leqslant n.\end{aligned}$$

Remark 1.3.3. One must not forget the initial Frobenius computation, for a cost of $O^{\sim}(d\log^2 q)$, as explained in § 1.3.2.2.

Chapter 2
Drinfeld modules and Anderson motives

This chapter covers basic vocabulary on Drinfeld modules, which we define in two steps. Let $\mathbb{F}_q$ be a finite field with q elements, and K be an extension of $\mathbb{F}_q$.

(i) In § 2.1, we define the simplest Drinfeld modules: those for which the so-called *function ring* is $\mathbb{F}_q[T]$. They are called *Drinfeld* $\mathbb{F}_q[T]$*-modules*. In that context, the base field K has in addition a structure of $\mathbb{F}_q[T]$-algebra given by a morphism

$$\gamma : \mathbb{F}_q[T] \to K.$$

(ii) In § 2.2, we extend our definitions to general *Drinfeld modules*: those whose *function ring* A is not restricted to $\mathbb{F}_q[T]$, but can be a ring of functions on a curve C that are regular everywhere, except on a given fixed point. Those Drinfeld modules are called *Drinfeld* A*-modules*, and one obtains Drinfeld $\mathbb{F}_q[T]$-modules by picking $\mathbb{P}^1(\mathbb{F}_q)$ and its point at infinity. In that context, K is equipped with a morphism

$$\gamma : A \to K$$

of $\mathbb{F}_q$-algebras. Most definitions from Drinfeld $\mathbb{F}_q[T]$-modules naturally extend to that of general Drinfeld A-modules, but algorithms in the latter context are significantly more sophisticated, as we will see. However, the importance of general Drinfeld A-modules cannot be underestimated: they are used to prove the most important theoretical result of Chapter 7, and we describe methods for computing norms of isogenies and characteristic polynomials of endomorphisms in Chapters 4, 5 and 6.

Classical references on Drinfeld modules include the textbooks [Gos96; Ros02; Vil06; Pap23]. Papikian's [Pap23] is written in the spirit of Silverman's [Sil09], and holds significant value for those seeking a rigorous yet gentle approach to Drinfeld $\mathbb{F}_q[T]$-modules. Some other introductory resources include Poonen's and Hayes' respective surveys [Poo21; Hay11], and some research articles may also help: Gekeler's [Gek91] proposes an in-depth study of Drinfeld modules whose base field K is finite; [Hei04] is an accessible resource to learn about Drinfeld modules, Anderson motives and Abelian modules for a general function ring A. French speakers eager to find a common framework for Drinfeld modules and elliptic curves may find interest in [GJ23], where the authors introduce *elementary modules* (*module élémentaire*), a notion that encapsulates properties of both elliptic curves and Drinfeld modules; elementary modules are then proved to correspond to either elliptic curves or Drinfeld modules. As far as computational aspects are concerned, we refer to several PhD theses. Caranay's thesis [Car18] adapts to Drinfeld modules some results and algorithms of the seminal thesis of Kohel [Koh96]. She proposes an algorithmic study of endomorphism rings of ordinary rank two Drinfeld modules and their isogeny graphs. Ayotte's thesis, which focuses on computational aspects of Drinfeld modular forms [Ayo23]. Musleh's thesis focused [MS23] on efficient computations of the characteristic polynomial of the Frobenius endomorphism of an $\mathbb{F}_q[T]$-module. His work also includes methods to compute spaces of morphisms and endomorphisms of Drinfeld $\mathbb{F}_q[T]$-modules over a finite field (see § 2.1.6).

2.1 Drinfeld $\mathbb{F}_q[T]$-modules

The simplest Drinfeld modules are those for which the so-called *function ring* is $\mathbb{F}_q[T]$. These are called *Drinfeld $\mathbb{F}_q[T]$-modules*, and can be studied without any allusion to algebraic geometry and curves other than $\mathbb{P}^1(\mathbb{F}_q)$. From an algorithmic point of view, Drinfeld $\mathbb{F}_q[T]$-modules are very convenient, as they can be represented by a single Ore polynomial; the same is true for their isogenies.

We also introduce the notion of *Anderson $\mathbb{F}_q[T]$-motive*, which are free modules with rank r over $K[T]$, where K is the base field of the Drinfeld modules, and r is an explicit integer called the *rank*. Most importantly, Drinfeld module and Anderson motives are dual constructions, in the form of a contravariant fully faithful functor from the category of Drinfeld modules to that of Anderson motives. This allows to represent morphisms of Drinfeld modules by polynomial matrices, leading to much more efficient representations than what exists for isogenies of elliptic curves.

2.1.1 Drinfeld modules and Anderson motives

Drinfeld $\mathbb{F}_q[T]$-modules over K are not $\mathbb{F}_q[T]$-modules in the classical term, but formal objects to which classical modules are attached. We define two of them.

(i) The first one is an $\mathbb{F}_q[T]$-module which plays the role for Drinfeld modules of the abelian group of points of an elliptic curve.

(ii) The second one is the *Anderson $\mathbb{F}_q[T]$ motive*, which is a module over $K\{\tau\} \otimes_{\mathbb{F}_q} \mathbb{F}_q[T]$. When restricting scalars to $K[T]$, the Anderson motives becomes free, with finite rank.

We introduce all these objects now, as well as their morphisms. We also introduce an invariant for Drinfeld modules called the *rank*, which happens to be the rank of the Anderson $\mathbb{F}_q[T]$-motive, seen as a module over $K[T]$.

2.1.1.1 Drinfeld modules

Recall that we have fixed a morphism of $\mathbb{F}_q$-algebras

$$\gamma : \quad \mathbb{F}_q[T] \quad \to \quad K.$$

Definition 2.1.1. A *Drinfeld $\mathbb{F}_q[T]$-module over K* is a morphism of $\mathbb{F}_q$-algebras

$$\phi : \mathbb{F}_q[T] \to K\{\tau\}$$

such that the image of ϕ is larger than K, and such that for any a in $\mathbb{F}_q[T]$, the constant coefficient of ϕ_a—a shorthand for $\phi(a)$—is $\gamma(a)$.

A *morphism* of Drinfeld $\mathbb{F}_q[T]$-modules from ϕ to ψ is the datum of an Ore polynomial $u \in K\{\tau\}$ satisfying

$$u\phi_a = \psi_a u,$$

for all a in $\mathbb{F}_q[T]$. An *isogeny* is a nonzero morphism.

Remark 2.1.2. We warn the reader that even though a morphism of Drinfeld modules and the Ore polynomial that defines it are distinct objects, we denote them by the same symbol as to not burden the notations.

Let ϕ and ψ be two Drinfeld $\mathbb{F}_q[T]$-modules over K, which we use for the remaining the section. As $\mathbb{F}_q[T]$ is generated over $\mathbb{F}_q$ by T, the Drinfeld $\mathbb{F}_q[T]$-module ϕ is defined by the sole image ϕ_T of T. We then obtain ϕ_a, for any $a = \sum_{i=0}^{n} a_i T^i$ in $\mathbb{F}_q[T]$, as

$$\phi_a = a(\phi_T) = \sum_{i=0}^{n} a_i \phi_T^i.$$

Consequently, an Ore polynomial $u \in K\{\tau\}$ defines a morphism from ϕ to ψ if and only if

$$u\phi_T = \psi_T u.$$

We call *τ-degree* of a morphism the τ-degree of the Ore polynomial that defines it. The composition of morphisms is given by the multiplication of Ore polynomials, which forces isomorphisms to be the morphisms with zero τ-degree. It also follows that endomorphisms of ϕ form a ring, denoted by

$$\mathrm{End}(\phi).$$

As for any a in $\mathbb{F}_q[T]$, ϕ_a defines an endomorphism of ϕ (for $\phi_a\phi_T = \phi_{Ta} = \phi_{aT} = \phi_T\phi_a$), the ring $\mathrm{End}(\phi)$ contains a copy of $\mathbb{F}_q[T]$ as a subring, and has the structure of an $\mathbb{F}_q[T]$-algebra. On the other hand, if K is a finite extension of $\mathbb{F}_q$ with degree d, the Ore polynomial $\tau_K = \tau^d$ defines an endomorphism of ϕ, called the *Frobenius endomorphism*. It is denoted by π, so that $\mathrm{End}(\phi)$ would contain a copy of $\mathbb{F}_q[T][\pi]$ as a subring, and be an $\mathbb{F}_q[T][\pi]$-algebra.

The set of morphisms from ϕ to ψ is simply denoted by

$$\mathrm{Hom}(\phi, \psi).$$

While it is not a ring, $\mathrm{Hom}(\phi, \psi)$ is an $\mathbb{F}_q[T]$-module, and even an $\mathbb{F}_q$-vector space.

Remark 2.1.3. The fact that $\mathrm{Hom}(\phi, \psi)$ is an $\mathbb{F}_q$-vector space plays an instrumental role in the computation of $\mathrm{Hom}(\phi, \psi)$, or $\mathrm{End}(\phi)$; see § 2.1.6 and [Wes22; Mus23] for details. On the contrary, isogenies of elliptic curves form a $\mathbb{Z}$-module, but not a vector space.

Example 2.1.4. In the following example, `Fq` is $\mathbb{F}_4$, `K` has degree 3 over `Fq`, and γ is implicitly defined as the morphism mapping `T` to a generator `z` of `K` over the prime field, *i.e.* an element with order $4^3 - 1$.

```
sage: Fq = GF(4)
sage: A.<T> = Fq[]
sage: K.<z> = Fq.extension(3)
```

```
sage: phi = DrinfeldModule(A, [z, 1, 1])
sage: psi = DrinfeldModule(A, [z, z^5, z^3])
sage: rho = DrinfeldModule(A, [z, z^5 + z + 1, z^5 + z])
```

```
sage: t = phi.ore_variable()  # \tau
sage: t^3 in End(phi)  # Frobenius endomorphism
True
sage: a = A.random_element()
sage: phi(a) in End(phi)
True
```

We can observe that `phi` and `psi` are isogenous, and that `phi` and `rho` are isomorphic:

```
sage: isog = z^4*t + z^5 + z^2 + z
sage: isog * phi(T) - psi(T) * isog
0
sage: isom = z^4 + z^3 + z + 1
sage: isom * phi(T) - rho(T) * isom
0
```

Therefore, `isog * isom(^-1)` defines an isogeny from `rho` to `psi`:

```
sage: isog * isom^(-1)
(z^4 + z^3 + z^2 + z)*t + z^5 + z^4 + z^3 + 1
sage: isog * isom^(-1) in Hom(rho, psi)
True
```

Remark 2.1.5. We already observe a difference between Drinfeld modules and elliptic curves: while representing morphisms of algebraic varieties can be quite technical, morphisms of Drinfeld modules are defined and represented very easily, taking inspiration from morphisms of lattices, which are related to both elliptic curves and Drinfeld modules (see § 2.2.2.1).

In the above definitions and examples, morphisms and isogenies are K-rational, in the sense that they come from elements in $K\{\tau\}$. If L is a subextension of $\overline{K}/K$, and u is an Ore polynomial in $L\{\tau\}$, one says that u is an L-morphism if $u\phi_T = \psi_T u$. In this thesis, isogenies are mostly assumed to be K-isogenies, except for occasional interventions of $\overline{K}$-endomorphisms and $\overline{K}$-isomorphisms.

2.1.1.2 Rank

Before defining the two main classical modules associated to a Drinfeld module, we introduce the notion of *rank*.

Definition 2.1.6. The *rank* of a Drinfeld $\mathbb{F}_q[T]$-module ϕ, denoted $\mathrm{r}(\phi)$, is the τ-degree of the *generator* ϕ_T.

Rank r Drinfeld $\mathbb{F}_q[T]$-modules over K and their morphisms form a category, denoted $\mathrm{Dr}_r(\mathbb{F}_q[T], K)$.

Remark 2.1.7. It is easily seen that isogenies can only exist between Drinfeld modules of same rank. This indicates that the rank of a Drinfeld module is not an analogue of the genus or the dimension of an abelian variety, as abelian varieties related by a morphism (but not an isogeny) may have different dimensions and genera. Drinfeld modules of any rank r are in fact objects of dimension 1: they correspond to *abelian modules* of rank r and dimension 1, as defined by Van der Heiden in [Hei04]. Abelian modules can exist with any arbitrary integer dimension. The rank, on the contrary, organizes Drinfeld modules in different classes: rank one Drinfeld modules correspond to roots of unity and cyclotomic function fields (see § 2.2.2.2), whilst rank two Drinfeld modules share numerous similarities with elliptic curves. It is fortunate that these classes of objects can be unified under a common definition.

We now assume that both ϕ and ψ have rank r.

2.1.1.3 The module associated to a Drinfeld module

While the points of an elliptic curve form an abelian group, *i.e.* a $\mathbb{Z}$-module, a Drinfeld $\mathbb{F}_q[T]$-module over K endows $\overline{K}$ with the following structure of $\mathbb{F}_q[T]$-module:

Definition 2.1.8. We let $\mathbb{E}(\phi)$ be the left $\mathbb{F}_q[T]$-module given by

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, z) & \mapsto & \phi_a(z). \end{array}$$

If $u : \phi \to \psi$ is a morphism of Drinfeld $\mathbb{F}_q[T]$-modules, one gets a morphism of $\mathbb{F}_q[T]$-modules:

$$\begin{array}{rccl} \mathbb{E}(u) : & \mathbb{E}(\phi) & \to & \mathbb{E}(\psi) \\ & z & \mapsto & u(z). \end{array}$$

In other words, $\mathbb{E}$ is a covariant functor from the category of Drinfeld $\mathbb{F}_q[T]$-modules to the category of $\mathbb{F}_q[T]$-modules.

2.1.1.4 Anderson motives

To a rank r Drinfeld $\mathbb{F}_q[T]$-module ϕ, one can associate a second linear object: its *Anderson* $\mathbb{F}_q[T]$-*motive* $\mathbb{M}(\phi)$. Unless specified otherwise, all tensor products are taken over $\mathbb{F}_q$.

Definition 2.1.9. The *Anderson* $\mathbb{F}_q[T]$-*motive* associated to ϕ, denoted $\mathbb{M}(\phi)$, is the left $K\{\tau\} \otimes \mathbb{F}_q[T]$-module given by

$$\begin{array}{rcl} (K\{\tau\} \otimes \mathbb{F}_q[T]) \times K\{\tau\} & \to & K\{\tau\} \\ (\sum g_i \otimes a_i, f) & \mapsto & \sum g_i f \phi_{a_i}. \end{array}$$

Morphisms of Drinfeld modules give rise to contravariant morphisms on the associated Anderson motives: for any morphism of Drinfeld modules $u : \phi \to \psi$, we define the morphism of $K\{\tau\} \otimes \mathbb{F}_q[T]$-modules

$$\begin{array}{rccl} \mathbb{M}(u) : & \mathbb{M}(\psi) & \to & \mathbb{M}(\phi) \\ & f & \mapsto & fu. \end{array}$$

Remark 2.1.10. While $\mathbb{E}(\phi)$ is the function field analogue of $E(\overline{\mathbb{F}_q})$, E being an elliptic curve, the Anderson $\mathbb{F}_q[T]$-motive $\mathbb{M}(\phi)$ does not seem to have any computationally efficient equivalent on E. In fact, the Anderson motive of ϕ is the analogue of a *motive*, in the sense of Grothendieck, who envisioned the motive of an algebraic variety to be *the* object encoding all its linear (or more technically, cohomological) properties. Using this theoretical object for algorithmic purposes in the context of elliptic curves remains an open challenge.

Being a $K\{\tau\} \otimes \mathbb{F}_q[T]$-motive with underlying set $K\{\tau\}$, the Anderson motive $\mathbb{M}(\phi)$ is evidently a free $K\{\tau\} \otimes \mathbb{F}_q[T]$ with rank 1. As $K[T]$ can be decomposed as $K \otimes \mathbb{F}_q[T]$, it can be seen as a subring of $K\{\tau\} \otimes \mathbb{F}_q[T]$. Thus, $\mathbb{M}(\phi)$ can be seen as a module over $K[T]$. This reveals one of the most important theoretical facts used in this thesis:

Theorem 2.1.11. *The Anderson* $\mathbb{F}_q[T]$-*motive* $\mathbb{M}(\phi)$ *of* ϕ*, viewed as a* $K[T]$-*module, is free with rank* r*. A basis is given by*

$$(1, \tau, \ldots, \tau^{r-1}).$$

This basis is called the canonical basis *of* $\mathbb{M}(\phi)$.

Remark 2.1.12. Theorem 2.1.11 is essential for the algorithms of Chapters 4 and 5, as it allows to represent isogenies of Drinfeld $\mathbb{F}_q[T]$-modules by polynomial matrices with size r-by-r.

This classical fact [Pap23, Lemma 3.4.4] has an algorithmic nature. Write $\phi_T = g_0 + \cdots + g_r\tau^r$, with $g_r \neq 0$. The coordinates of Ore polynomials with degree less than r are their own coefficients, whereas τ^r has coordinates

$$\left(\frac{T - g_0}{g_r}, \frac{-g_1}{g_r}, \cdots, \frac{-g_{r-1}}{g_r}\right).$$

Thus, the coefficients of any f in $\mathbb{M}(\phi)$ may be computed recursively. In § 4.3.1.3, we derive several algorithms to perform computations in this basis, and study their complexities. Another important consequence of Theorem 2.1.11 is that morphisms of Drinfeld modules can be represented by matrices with coefficients in $K[T]$.

Remark 2.1.13. The functor $\mathbb{M}$ is contravariant and fully faithful, which identifies the category of Drinfeld modules as a subcategory of finitely generated free modules. It is possible to describe these modules—called *Anderson motives*—more explicitly, and independently from Drinfeld modules. However, the category of Anderson motives is larger than that of Drinfeld modules, meaning that not all Anderson motives come from a Drinfeld module. This has several advantages: for one thing, this larger category allows to form tensor products of Anderson motives, which cannot be directly done on Drinfeld modules. This allows, for example, to build the Weil pairing for Drinfeld modules [Hei04; Pap23]. Anderson motives were originally studied by Anderson for the case $\mathbb{F}_q[t]$ (rather denoted by $\mathbb{F}_q[T]$ in this thesis) and named *t-modules* [And86]; they were subsequently defined in the full generality of § 2.2; see [Hei04; CG24].

2.1.2 Function field characteristic

We now define the notion of $\mathbb{F}_q[T]$-characteristic, which is an analogue for function fields of the classical integer characteristic. While in our context, the latter is always positive, it is important to derive a theory of Drinfeld $\mathbb{F}_q[T]$-modules and function fields with a notion of characteristic that is a polynomial (or later for general Drinfeld A-modules, an ideal in A), such that distinguishing between zero and prime characteristic is possible. Therefore, we define the $\mathbb{F}_q[T]$-*characteristic of* K as the kernel of the morphism

$$\gamma : \mathbb{F}_q[T] \to K.$$

If γ is injective, we say that K *has* $\mathbb{F}_q[T]$-*characteristic zero*; in the other case, we say that K *has prime* $\mathbb{F}_q[T]$-*characteristic*, and the kernel is often denoted $\mathfrak{p}$, with monic generator $p \in \mathbb{F}_q[T]$.

We say that an element a in $\mathbb{F}_q[T]$ is *away from the characteristic* if K has $\mathbb{F}_q[T]$-characteristic zero or if (a) is coprime to $\mathfrak{p}$, when K has prime $\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$. While in the case of rings R, the morphism $\mathbb{Z} \to R$ is unique, many choices are available for $\gamma : \mathbb{F}_q[T] \to K$.

Let us now assume that K has prime $\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$, and that $\mathfrak{p}$ is generated by a monic polynomial p. Then, as an Ore polynomial, ϕ_p is not separable (this is because the constant coefficient of ϕ_p is $\gamma(p)$, and $\gamma(p)$ is zero by definition of p). For some rarer Drinfeld modules, ϕ_p is even purely inseparable:

```
sage: Fq = GF(2)
sage: A.<T> = Fq[]
sage: k.<zk> = Fq.extension(2)
sage: K.<z> = k.extension(2)
```

```
sage: phi = DrinfeldModule(A, [K(zk), 0, 1])
sage: psi = DrinfeldModule(A, [K(zk), 1, 1])
sage: p = phi.characteristic()
sage: p
T^2 + T + 1
```

To quantify this phenomenon, we introduce a new invariant: the *height*. It is related to the *height* (see § 1.1.1.3) of the Ore polynomial ϕ_p. Notice that $\deg(p)$ divides the height of ϕ_p. Let $u_h\tau^h$ be the smallest monomial (*i.e.* that with smallest τ-degree) appearing in ϕ_p. Having $\phi_p\phi_T = \phi_T\phi_p$, it necessarily happens that $u_h\tau^h\gamma(T) = \gamma(T)u_h\tau^h$, implying that $\gamma(T)^{q^h} = \gamma(T)$. As the image of γ is a field with order $q^{\deg(p)}$ generated by $\gamma(T)$, we see that $\deg(p)$ divides h.

Definition 2.1.14. The *height* of ϕ, denoted $\mathrm{h}(\phi)$, is the integer

$$\mathrm{h}(\phi) = \mathrm{h}(\phi_p)/\deg(p).$$

Drinfeld modules for which ϕ_p is purely inseparable are known as *supersingular* Drinfeld modules [Pap23, Def. 4.1.9]:

Definition 2.1.15. We say that ϕ is *ordinary* if its height is one, and *supersingular* if its height is its rank.

In rank two, a Drinfeld $\mathbb{F}_q[T]$-module is either supersingular or ordinary, and these two classes have very distinctive behaviors, beginning by the structures of their endomorphism rings (§ 2.1.5). More generally, Drinfeld modules with high height are expected to exist in fewer quantity that those with low height: assuming that the coefficients of ϕ_p are uniformly distributed in $K^{\mathrm{r}(\phi)\deg(p)-1}$, the Ore polynomial ϕ_p has fewer chances to be purely inseparable, *i.e.* to have many first coefficients equal to zero. To count isomorphism classes of supersingular rank r Drinfeld $\mathbb{F}_q[T]$-modules, we refer to [Gek91, Section 4].

```
sage: phi.height()
1
sage: phi.is_supersingular()
False
sage: psi.height()
2
sage: psi.is_supersingular()
True
```

```
sage: rho = DrinfeldModule(A, [K(zk), 1, 1, z^3])
sage: rho(p)
(z^3 + z^2 + z + 1)*t^6 + (z^2 + z + 1)*t^5 + (z^2 + 1)*t^4
sage: rho.height()
2
sage: rho.is_ordinary()
False
sage: rho.is_supersingular()
False
```

Recalling the correspondence between Ore polynomials and finite $\mathbb{F}_q$-vector spaces (§ 1.1.1.3), we can define ordinarity and supersingularity using the kernel of ϕ_p. This is one of the objectives of § 2.1.3.

2.1.3 Torsion and Tate modules

We now study the torsion of the $\mathbb{F}_q[T]$-module $\mathbb{E}(\phi)$. In this subsection, the $\mathbb{F}_q[T]$-characteristic is not necessarily prime.

2.1.3.1 Torsion spaces

For any a in $\mathbb{F}_q[T]$, the *a-torsion* of ϕ is defined as the a-torsion of $\mathbb{E}(\phi)$; it is denoted by $\mathbb{E}_a(\phi)$. In other words, as sets, one has

$$\mathbb{E}_a(\phi) = \mathrm{Ker}(\phi_a) = \{z \in \overline{K} : \phi_a(z) = 0\}.$$

We can avoid picking a generator of $\mathfrak{a}$ by setting

$$\mathbb{E}_{\mathfrak{a}}(\phi) = \bigcap_{a \in \mathfrak{a}} \mathbb{E}_a(\phi).$$

The $\mathfrak{a}$-torsion is obviously a module over $\mathbb{F}_q[T]/(a)$, and the following holds [Pap23, Section 3.5]:

Proposition 2.1.16. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two coprime ideals of $\mathbb{F}_q[T]$. We have:*

$$\mathbb{E}_{\mathfrak{a}\mathfrak{b}}(\phi) \simeq \mathbb{E}_{\mathfrak{a}}(\phi) \times \mathbb{E}_{\mathfrak{b}}(\phi).$$

If $\mathfrak{a}$ is away from the $\mathbb{F}_q[T]$-characteristic of K (that is if the $\mathbb{F}_q[T]$-characteristic is zero, or if $\mathfrak{a}$ is coprime to it), then, for any positive integer n, we have

$$\mathbb{E}_{\mathfrak{a}^n}(\phi) \simeq (\mathbb{F}_q[T]/\mathfrak{a}^n)^{\mathrm{r}(\phi)},$$

If K has prime $\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$:

$$\mathbb{E}_{\mathfrak{p}^n}(\phi) \simeq (\mathbb{F}_q[T]/\mathfrak{p})^{\mathrm{r}(\phi)-\mathrm{h}(\phi)}$$

Remark 2.1.17. The a-torsion is usually denoted $\phi[a]$; we employ our notation to highlight the functorial properties of $\mathbb{E}$.

Remark 2.1.18. Computing $\mathbb{E}_{\mathfrak{a}}(\phi)$ can be costly, and requires to work over possibly large extensions of the ground field. In § 4.2, we exhibit a correspondence between $\mathbb{E}_{\mathfrak{a}}(\phi)$ and the space $\mathbb{M}(\phi)/\mathfrak{a}\mathbb{M}(\phi)$, which is defined at the level of K (see Theorem 4.2.5). This makes computations easier, and plays a major role in Chapters 4 and 5.

Remark 2.1.19. Let E be an elliptic curve, let m, n be two coprime integers and let k be a positive integer. Let $E[n]$ denote the n-torsion of E, *i.e.* the n-torsion of its abelian group of points. Then, provided that n is coprime to the characteristic, $E[n^k] \simeq (\mathbb{Z}/n^k\mathbb{Z})^2$, $E[nm] \simeq E[n] \times E[m]$ and when the ground field has positive characteristic p, $E[p^k]$ is either trivial or isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$. This classification highlights that, out of all possibles ranks, rank two Drinfeld modules are closest to elliptic curves.

2.1.3.2 Tate modules

For a prime ideal $\mathfrak{q}$ of $\mathbb{F}_q[T]$, the information of all the $\mathfrak{q}^n$-torsion spaces, n varying in $\mathbb{Z}_{\geqslant 0}$, can be encapsulated in the following object:

Definition 2.1.20. The $\mathfrak{q}$-adic *Tate module of* ϕ, denoted $\mathbb{T}_\mathfrak{q}(\phi)$, is the inverse limit

$$\mathbb{T}_\mathfrak{q}(\phi) = \varprojlim_{n \in \mathbb{Z}_{\geqslant 0}} \mathbb{E}_{\mathfrak{q}^n}(\phi).$$

The $\mathfrak{q}$-adic Tate module is a module over $\mathbb{F}_q[T]_\mathfrak{q}$, the completion of $\mathbb{F}_q[T]$ with respect to the $\mathfrak{q}$-adic valuation. When $\mathfrak{q}$ is away from the characteristic, $\mathbb{T}_\mathfrak{q}(\phi)$ has rank r; otherwise, it has rank $r - h$, where h is the height of ϕ. It is important to note that:

— ϕ is supersingular whenever $\mathbb{T}_\mathfrak{p}(\phi)$ has $\mathbb{F}_q[T]_\mathfrak{p}$-rank zero,

— ϕ is ordinary whenever $\mathbb{T}_\mathfrak{p}(\phi)$ has $\mathbb{F}_q[T]_\mathfrak{p}$ rank $r - 1$.

As for the functor $\mathbb{E}$, which it derivates from, $\mathbb{T}_\mathfrak{q}$ is a covariant functor: any morphism of Drinfeld modules $u : \phi \to \psi$ yields a morphism of $\mathbb{F}_q[T]_\mathfrak{q}$-modules

$$\begin{array}{rccc} \mathbb{T}_\mathfrak{q}(u) : & \mathbb{T}_\mathfrak{q}(\phi) & \to & \mathbb{T}_\mathfrak{q}(\psi) \\ & ((z_i)_{i \in \mathbb{Z}_{\geqslant 0}}) & \mapsto & ((u(z_i)_{i \in \mathbb{Z}_{\geqslant 0}}). \end{array}$$

The case of endomorphisms is particularly interesting. The map

$$\begin{array}{ccc} \mathrm{End}(\phi) & \to & \mathrm{End}_{\mathbb{F}_q[T]_\mathfrak{q}}(\mathbb{T}_\mathfrak{q}(\phi)) \\ u & \mapsto & \mathbb{T}_\mathfrak{q}(u) \end{array}$$

identifies $\mathrm{End}(\phi)$ as a subalgebra of $\mathcal{M}_r(\mathbb{F}_q[T]_\mathfrak{q})$, the space of r-by-r matrices with coefficients in $\mathbb{F}_q[T]_\mathfrak{q}$. From that, we can deduce a proof that $\mathrm{End}(\phi)$ is free over $\mathbb{F}_q[T]$ with rank $\leqslant r^2$ (Theorem 2.1.31). Furthermore, we can associate to u and $\mathfrak{q}$ a *characteristic polynomial*: that of the linear endomorphism $\mathbb{T}_\mathfrak{q}(u)$, which we study in § 2.1.4, and compute in Chapters 4 and 6.

2.1.4 Characteristic polynomials of endomorphisms

Let u be an endomorphism of ϕ. In this section, we attach to u an invariant called its *characteristic polynomial*, which is a monic polynomial of $\mathbb{F}_q[T][X]$ with degree r. We define it with Tate modules, even though it has a description at the level of $\mathbb{M}(\phi)$, which will be particularly useful later. Indeed, the computation of characteristic polynomials of endomorphisms is one of the main prospects of this thesis (Chapters 4, 6). Besides, the case of the Frobenius endomorphism is particularly interesting, and applications are presented in Chapter 7.

2.1.4.1 General endomorphisms

Let $\mathfrak{q}$ be a prime ideal of $\mathbb{F}_q[T]$, away from the characteristic. As u is an endomorphism of ϕ, we can consider its action $\mathbb{T}_\mathfrak{q}(u)$ on the Tate module $\mathbb{T}_\mathfrak{q}(\phi)$. As a linear endomorphism on a free $\mathbb{F}_q[T]_\mathfrak{q}$-module with rank r, $\mathbb{T}_\mathfrak{q}(\phi)$ has a characteristic polynomial, which according to Theorem 3.6.6 of [Pap23] does not depend on $\mathfrak{q}$.

Definition 2.1.21. The *characteristic polynomial of u*, denoted by $\chi(u)$, is the characteristic polynomial of $\mathbb{T}_\mathfrak{q}(u)$.

In practical terms, this means that there exist coefficients $a_0, \dots, a_r \in \mathbb{F}_q[T]$ such that

$$\begin{cases} \chi(u) = a_0 + \cdots + a_r X^r, \\ \phi_{a_0} u + \cdots + \phi_{a_r} u^r = 0. \quad \text{(Equality as endomorphisms of D. M., or Ore polynomials.)} \end{cases}$$

Definition 2.1.21 follows that of elliptic curves, but is not the most practical. Indeed, computing the characteristic polynomial of u with it would mean computing the kernel of many Ore polynomials. This would require working over possibly large extensions of K. However, the Tate module can be replaced by another linear object: the Anderson motive.

Theorem 2.1.22. *If u is an endomorphism, its characteristic polynomial is that of $\mathbb{M}(u)$.*

Theorem 2.1.22 is established, for example, in [Pap23, Proposition 3.6.7], but we generalize this statement for general Drinfeld A-modules in Theorem 4.2.7.

Remark 2.1.23. As mentioned, the characterization of Theorem 2.1.22 allows to design efficient algorithms to compute $\chi(u)$ (Algorithm 6), which are also implemented (see Chapter 3).

```
sage: Fq = GF(3)
sage: A.<T> = Fq[]
sage: k.<zk> = Fq.extension(3)
sage: K.<z> = k.extension(2)
```

```
sage: phi = DrinfeldModule(A, [K(zk), 1, z])
sage: psi = DrinfeldModule(A, [K(zk), 2*z + z^2 + z^4, z^3])
sage: a = T^2 + 1
sage: phi_a = End(phi)(T^2 + 1)
sage: phi_a.charpoly()
X^2 + (T^2 + 1)*X + T^4 + 2*T^2 + 1
sage: phi_a.charpoly()(phi_a)
Endomorphism of Drinfeld module defined by T |--> z*t^2 + t + 2*z^5 + 2*z^4 + 2
  Defn: 0
```

2.1.4.2 The special case of the Frobenius endomorphism

Assume now that K is a finite field with degree d over $\mathbb{F}_q$. The special case of the Frobenius endomorphism holds significant importance, as it encodes many properties of the Drinfeld module. First, we fix some vocabulary. Following § 2.1.4.1, write the characteristic polynomial of the Frobenius endomorphism as

$\chi(u) = a_0 + \cdots + a_r X^r$. We call the coefficient a_0 the *Frobenius norm* of ϕ, and if the rank is two, then a_1 is called the *Frobenius trace*. We also let π denote the Frobenius endomorphism of ϕ.

We have already seen that a Drinfeld $\mathbb{F}_q[T]$-module over K is supersingular if and only if ϕ_p is a purely inseparable polynomial (Definition 2.1.15). This information can actually be read at the level of the characteristic polynomial of π.

Example 2.1.24. Let us do some computations. Suppose that there exists a nonzero element α of $\mathbb{F}_q$ such that

$$\phi_p = \alpha\tau^{r\deg(p)},$$

where r is the rank of ϕ, which happens if and only if ϕ is supersingular. Let m be such that $m\deg(p)$ equals d. Then

$$\phi_p^m = \tau^{r\deg(p)m} = \tau_K^r.$$

This implies that the polynomial

$$X^r - p^m,$$

is an annihilator polynomial of π. It is monic and has degree r, but we warn the reader that it needs not be $\chi(\pi)$. Indeed, consider the special case $m = r$. In that case, $r\deg(p)$ equals d, and π is annihilated by the polynomial

$$X - \alpha^{-1}p.$$

As this polynomial is monic and has degree one, it is the minimal polynomial of π, [Gek91, Section 3]. As $\chi(\pi)$ is a power of the minimal polynomial [Gek91, Lemma 3.3], this implies that

$$\chi(\pi) = (X - \alpha^{-1}p)^r.$$

In particular, we observe that under our hypothesis that m equals r, the coefficients of $\chi(\pi)$ are all multiples of p. If $m = r = 2$, we have

$$\chi(\pi) = X^2 - 2\alpha^{-1}pX + \alpha^{-2}\mathfrak{p}^2,$$

which is different than $X^r - p^m$. In fact, the following holds ([Gek83, Lem. (5.2) and Satz (5.3)]):

Proposition 2.1.25. *A Drinfeld $\mathbb{F}_q[T]$-module over K is supersingular if and only if the $\mathbb{F}_q[T]$-characteristic of K divides the Frobenius trace.*

In fact, the characteristic polynomial of the Frobenius endomorphism of characterizes the K-isogeny class of ϕ, whether or not ϕ is ordinary or supersingular (on an algebraic closure of K, all supersingular Drinfeld $\mathbb{F}_q[T]$-modules with rank r are isogenous, per [Pap23, Lemma 4.4.3]), as pointed out in [Gek91, Theorem 3.5]:

Theorem 2.1.26. *Two Drinfeld $\mathbb{F}_q[T]$-modules over K are isogenous if and only if they share the same characteristic polynomial of the Frobenius endomorphism.*

As a consequence, rank r Drinfeld $\mathbb{F}_q[T]$-modules over K which share a common characteristic polynomial χ_π of the Frobenius endomorphism form a subcategory of $\mathrm{Dr}_r(\mathbb{F}_q[T], K)$, denoted $\mathrm{Dr}_r(\mathbb{F}_q[T], K)_{\chi_\pi}$, in which any two objects are connected via an isogeny. This is an important construction in Chapter 7).

Example 2.1.27. The Drinfeld $\mathbb{F}_q[T]$-modules `phi` and `psi` are isogenous, and as such, they have the same characteristic polynomial of the Frobenius endomorphism. But the $\mathbb{F}_q[T]$-characteristic does not divide the trace (`phi` and `psi` have rank two), and so `phi` and `psi` are ordinary

```
sage: t = phi.ore_variable()
sage: (z^3 * t^3) * phi(T) == psi(T) * (z^3 * t^3)
True
sage: phi.frobenius_charpoly()
X^2 + (T^3 + T^2 + 2*T)*X + 2*T^6 + 2*T^4 + T^3 + 2*T^2 + 2*T + 2
sage: psi.frobenius_charpoly()
X^2 + (T^3 + T^2 + 2*T)*X + 2*T^6 + 2*T^4 + T^3 + 2*T^2 + 2*T + 2
```

To give other examples, we now briefly change the setting and find, up to $\overline{K}$-isomorphism, all Drinfeld $\mathbb{F}_q[T]$-modules defined over K that are supersingular:

```
sage: supersingulars = list()
sage: for j in K:
....:     coeffs = [K(zk), 1, j^(-1)] if j != 0 else [K(zk), 0, K(1)]
....:     rho = DrinfeldModule(A, coeffs)
....:     if rho.is_supersingular():
....:         supersingulars.append(rho)
sage: [rho(T) for rho in supersingulars]
[t^2 + 2*z^5 + 2*z^4 + 2, (z^5 + z^4)*t^2 + t + 2*z^5 + 2*z^4 + 2, (z^5 + z^4 + 2)*t^2 + t +
     2*z^5 + 2*z^4 + 2, (z^5 + z^4 + 1)*t^2 + t + 2*z^5 + 2*z^4 + 2]
```

All these Drinfeld modules have the same characteristic polynomial of the Frobenius endomorphism:

```
sage: charpolys = {rho.frobenius_charpoly() for rho in supersingulars}
sage: charpolys
{X^2 + (T^3 + 2*T + 1)*X + T^6 + T^4 + 2*T^3 + T^2 + T + 1}
```

We observe that $X^2 - \alpha^{-2}\mathfrak{p}$ annihilates the Frobenius endomorphism while being different than its characteristic polynomial:

```
sage: rho = supersingulars[0]
sage: p = rho.characteristic()
sage: alpha = Fq(rho(p).leading_coefficient())
sage: frob = rho.frobenius_endomorphism()
sage: frob_charpoly = frob.charpoly()
sage: X = frob_charpoly.variables()[0]
sage: ann_pol = X^2 - alpha^(-2) * p^2
sage: ann_pol(frob)
Endomorphism of Drinfeld module defined by T |--> t^2 + 2*z^5 + 2*z^4 + 2
  Defn: 0
sage: ann_pol == frob_charpoly
False
```

However, the Frobenius norm is always a power (up to a multiplicative factor in $\mathbb{F}_q$) of the $\mathbb{F}_q[T]$-characteristic. Furthermore, it is possible to estimate the degrees of the coefficients of $\chi(\pi)$. The following

lemma is proven in [Pap23, Theorem 4.2.7], and we provide alternative proofs using Anderson motives in Remark 4.3.8.

Lemma 2.1.28. *Let $\chi(\pi) = a_0 + \cdots + a_r X^r$ be the characteristic polynomial of the Frobenius endomorphism of ϕ, and let Δ be the leading coefficient of ϕ_T. For $0 \leqslant i \leqslant r-1$, we have*

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

Furthermore,

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

and

$$\deg(a_0) = d.$$

We finish this subsection by turning to the rank two case. Then, it may happen that the characteristic polynomial of the Frobenius endomorphism, which can be seen as a bivariate polynomial in $\mathbb{F}_q[T, X]$, defines an imaginary hyperelliptic curve over $\mathbb{F}_q$, as defined in § 1.2.4. This is an important aspect of Chapter 7.

Example 2.1.29. It is not hard to find Drinfeld modules that have the desired property. If the extension degree d is odd, then given that the Frobenius norm has degree d, the curve defined by $\chi(\pi)$ is imaginary hyperelliptic if it is smooth, *i.e.* the discriminant of $\chi(\pi)$ is squarefree. If d is even, however, the curve defined by $\chi(\pi)$ is real, which is not suitable for our later purposes.

```
sage: phi.frobenius_charpoly()
X^2 + (T^3 + T^2 + 2*T)*X + 2*T^6 + 2*T^4 + T^3 + 2*T^2 + 2*T + 2
sage: phi.frobenius_charpoly().discriminant().is_squarefree()
True
sage: h = (T^3 + T^2 + 2*T)
sage: f = 2*T^6 + 2*T^4 + T^3 + 2*T^2 + 2*T + 2
sage: HyperellipticCurve(f, h)
Hyperelliptic Curve over Finite Field of size 3 defined by y^2 + (x^3 + x^2 + 2*x)*y = 2*x^6 +
      2*x^4 + x^3 + 2*x^2 + 2*x + 2
```

2.1.5 Endomorphism rings of rank two Drinfeld modules

We now turn to the study of the structure of $\mathrm{End}(\phi)$. The rank two case is particularly interesting, and important for Chapter 7. Furthermore, we reuse the notions of § 2.1.4. Consider $\mathrm{End}^\circ(\phi)$, the *algebra of endomorphisms of ϕ*, defined by

$$\mathrm{End}^\circ(\phi) = \mathrm{End}(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T).$$

The endomorphism ring of ϕ is an *order* in $\mathrm{End}^\circ(\phi)$: $\mathrm{End}(\phi)$ is a subalgebra of $\mathrm{End}^\circ(\phi)$, it is finitely generated as an $\mathbb{F}_q[T]$-module and it obviously contains an $\mathbb{F}_q(T)$-basis of $\mathrm{End}^\circ(\phi)$. As $\mathrm{End}(\phi)$ is free over $\mathbb{F}_q[T]$ of rank $\leqslant r^2$, $\mathrm{End}^\circ(\phi)$ has dimension $\leqslant r^2$ over $\mathbb{F}_q(T)$. Furthermore, an elementary computation reveals that $\mathrm{End}^\circ(\phi)$ is a division algebra. Let us now assume that ϕ has rank two.

— If ϕ is ordinary, then $\mathrm{End}^\circ(\phi)$ is an imaginary quadratic function field ([Car18, Theorem 6.4.2]) generated by the Frobenius endomorphism π of ϕ. In other words, we have an isomorphism of $\mathbb{F}_q[T]$-algebras
$$\mathrm{End}^\circ(\phi) \simeq \mathbb{F}_q[T][X]/(\chi(\pi)).$$
Imaginary quadratic function fields contain a single maximal order (by order, we mean an $\mathbb{F}_q[T]$-order—for elliptic curves, we mean $\mathbb{Z}$-orders): their ring of integers. If $O_{\mathrm{End}^\circ(\phi)}$ is the maximal order of the algebra of endomorphisms, its orders are are exactly the sets of the form $O = \mathbb{F}_q[T] + fO_{\mathrm{End}^\circ(\phi)}$ for f in $\mathbb{F}_q[T]$. The polynomial f is called the *conductor* of O. It is such that $O_{\mathrm{End}^\circ(\phi)}/O$ has index $|f|_\infty = q^{\deg(f)}$, where $|\cdot|_\infty$ is the norm at infinity obtained from the valuation at infinity on $\mathbb{F}_q(T)$. Among these orders, only the maximal order is a Dedekind domain.

— If ϕ is supersingular, and as r equals two, $\mathrm{End}^\circ(\phi)$ has rank $\leqslant 4$. As it contains the quadratic field generated by the Frobenius endomorphism, which has degree two, then $\mathrm{End}^\circ(\phi)$ has degree two or four over $\mathbb{F}_q(T)$. In the latter case, it is a quaternion algebra over $\mathbb{F}_q(T)$, *i.e.* a central simple $\mathbb{F}_q(T)$-algebra with dimension four. In that case, $\mathrm{End}(\phi)$ is a maximal order in $\mathrm{End}^\circ(\phi)$. However, if $\mathrm{End}^\circ(\phi)$ has degree two over $\mathbb{F}_q(T)$, it is the quadratic imaginary function field generated by the Frobenius endomorphism of ϕ, like in the ordinary case. This situation depends on the values of so-called *Weil numbers* associated to the Drinfeld module; we refer to [Car18, Section 6.4] (and Remark 6.3.25) for details. This reveals that the classification of supersingular rank two Drinfeld modules slightly differs from that of supersingular elliptic curves, as the endomorphism ring of a supersingular elliptic curve is always a maximal order in a quaternion algebra (see Remark 2.1.30).

Remark 2.1.30. The situation is very similar to that of elliptic curves. Let E be an elliptic curve, let $\mathrm{End}(E)$ be its endomorphism ring, and consider its algebra of endomorphisms $\mathrm{End}^\circ(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. It is proven that $\mathrm{End}^\circ(E)$ is a division algebra of which $\mathrm{End}(E)$ is an order. We also know that $\mathrm{End}(E)$ is a free module over $\mathbb{Z}$ of rank 1, 2 or 4 (this corresponds to $r = 2$ for Drinfeld modules). Consequently, $\mathrm{End}(E)$ is only one of three things:

(i) $\mathrm{End}(E)$ is isomorphic to $\mathbb{Z}$; the curve is called *non-CM*.

(ii) $\mathrm{End}(E)$ contains extra endomorphisms and $\mathrm{End}^\circ(E)$ is a quadratic imaginary number field of which $\mathrm{End}(E)$ is an order; the curve is called *CM*.

(iii) $\mathrm{End}(E)$ contains extra endomorphisms and $\mathrm{End}^\circ(E)$ is a quaternion algebra of which $\mathrm{End}(E)$ is a maximal order; the curve is called *supersingular*.

In characteristic zero, curves can only be CM or non-CM; in positive characteristic, they can only be CM or supersingular. A typical example is that of elliptic curves defined over $\mathbb{F}_q$, which have a noninteger *Frobenius endomorphism*. Let E be such a curve, defined by a Weierstraß equation. Its Frobenius endomorphism π_E is defined by $(x, y) \mapsto (x^q, y^q)$, raising the coordinates to the q-th power. It has a characteristic polynomial in $\mathbb{Z}[T]$ of the form:
$$\chi(\pi_E) = X^2 - tX + q,$$
satisfying
$$\chi(\pi_E)(\pi_E) = \pi_E^2 - t\pi_E + q = 0.$$
When the curve is CM, $\mathrm{End}^\circ(\phi)$ is isomorphic to $\mathbb{Q}(\pi_E) \simeq \mathbb{Q}[T]/(\chi(\pi_E))$. The curve E is supersingular if and only if p divides t, the *Frobenius trace*. For Drinfeld modules, Papikian defines a Drinfeld

module to be CM whenever its endomorphism ring has rank r (corresponding to the case of rank 2 for elliptic curves) over $\mathbb{F}_q[T]$ (see Definition 3.4.20 of [Pap23]).

2.1.6 Computing isogenies

We now leave endomorphisms, and turn to general isogenies. Having presented a criterion to assert if two Drinfeld $\mathbb{F}_q[T]$-modules over a finite field are isogenous (Theorem 2.1.26), we enquire about the computation of said isogenies. We recall that ϕ and ψ have rank r, and that $\mathrm{Hom}(\phi, \psi)$ is a module over $\mathbb{F}_q[T]$, and a vector space over $\mathbb{F}_q$ (§ 2.1.1.1). It is an important result ([Pap23, Theorem 3.4.1]) that

Theorem 2.1.31. *As an $\mathbb{F}_q[T]$-module, $\mathrm{Hom}(\phi, \psi)$ is free of rank $\leqslant r^2$.*

As K is finite, the subspace

$$\mathrm{Hom}_n(\phi, \psi).$$

of morphisms with τ-degree less than n is a finite $\mathbb{F}_q$-vector space. Let then $u = u_0 + \cdots + u_n\tau^n$ be an Ore polynomial, and write $\phi_T = g_0 + \cdots + g_r\tau^r$ and $\psi_T = g'_0 + \cdots + g'_r\tau^r$. Developing $u\phi_T - \psi_T u$ we obtain

$$\sum_{j=0}^{n}\sum_{i=0}^{r} u_j g_i^{q^j}\tau^{i+j} - \sum_{i=0}^{r}\sum_{j=0}^{n} g'_i u_j^{q^i}\tau^{i+j}.$$

We obtain a recursive system of identities.

$$\sum_{i=0}^{\min(k,n)} u_i g_{k-i}^{q^i} - g'_{k-i}u_i^{q^{k-i}} = 0, \quad \forall 0 \leqslant k \leqslant n+r. \tag{2.1}$$

By treating the u_i's as variables, we obtain a system of equations. Its solutions are the coefficients of all the morphisms of $\mathrm{Hom}_n(\phi, \psi)$. Preliminary studies suggest that recursively solving this system leads to an algorithm whose complexity is exponential in n; see [CGS20, Section 8] and [LS22, Section 4.2]. However, Wesolowski noticed [Wes22] that the system is $\mathbb{F}_q$-linear. A basis of $\mathrm{Hom}_n(\phi, \psi)$ over $\mathbb{F}_q$ is then computed as the solution of a system over $\mathbb{F}_q$ with $d(n+r+1)$ equations and $d(n+1)$ variables. This is achieved for a cost of $O(d^2 n^\omega(n+r))$ operations in $\mathbb{F}_q$, and will be used in § 7.3.2, as well as § A.2.4.

```
sage: Fq = GF(3)
sage: A.<T> = Fq[]
sage: K.<z> = Fq.extension(4)
```

```
sage: phi = DrinfeldModule(A, [z, z, 0, 1])
sage: psi = DrinfeldModule(A, [z, z^2 + z, 0, 2 + z^2 + z^3])
sage: phi.frobenius_charpoly() == psi.frobenius_charpoly()  # phi and psi are isogenous
True
sage: Hom(phi, psi).Fq_basis(0)  # phi and psi are not isomorphic
[]
sage: Hom(phi, psi).Fq_basis(1)
[]
sage: Hom(phi, psi).Fq_basis(2)
[]
sage: Hom(phi, psi).Fq_basis(3)
[Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t + z
  To:   Drinfeld module defined by T |--> (z^3 + z^2 + 2)*t^3 + (z^2 + z)*t + z
  Defn: (z^3 + z^2 + z)*t^3 + (z^3 + 2*z^2 + 1)*t + 2*z^2 + z + 1]
```

The above example highlights that not knowing the smallest τ-degree of an isogeny from a Drinfeld module to another sometimes leads to tedious basis computations. This is because $\mathbb{F}_q$ is finite, making it impossible for $\mathrm{Hom}(\phi, \psi)$ to possess a finite $\mathbb{F}_q$-basis. One way to consider arbitrary families of isogenies is to consider $\mathrm{Hom}(\phi, \psi)$ as a module over $\mathbb{F}_q[T]$ or $\mathbb{F}_q[\pi]$, which are two infinite rings. In [Mus23, Section 7.3], algorithms to compute $\mathbb{F}_q[T]$-bases and $\mathbb{F}_q[\pi]$-bases of $\mathrm{Hom}(\phi, \psi)$ are described. They are implemented, and the following computes a basis over $\mathbb{F}_q[\pi]$.

```
sage: Hom(phi, psi).basis()
[Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t + z
  To:   Drinfeld module defined by T |--> (z^3 + z^2 + 2)*t^3 + (z^2 + z)*t + z
  Defn: (2*z^3 + 2*z^2 + 2*z)*t^5 + (z^3 + z^2 + z)*t^4 + (2*z^2 + z)*t^3 + (z^3 + 2*z^2 + 1)*
        t + 2*z^3 + 2*z^2 + 2*z + 1, Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t + z
  To:   Drinfeld module defined by T |--> (z^3 + z^2 + 2)*t^3 + (z^2 + z)*t + z
  Defn: (2*z^3 + 2*z^2 + 2*z)*t^9 + (2*z^2 + z)*t^7 + (z^2 + 2*z)*t^6 + (2*z^3 + z + 1)*t^5 +
        (z^3 + z^2)*t^4 + (2*z^2 + 2)*t^3 + (z^2 + z)*t^2 + (2*z^3 + z^2)*t + z^3 + 2*z^2 + z,
        Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t + z
  To:   Drinfeld module defined by T |--> (z^3 + z^2 + 2)*t^3 + (z^2 + z)*t + z
  Defn: (2*z^3 + 2*z^2 + 2*z)*t^5 + (2*z^3 + z^2)*t^3 + (2*z^3 + z)*t^2 + (2*z^3 + 2*z^2 + 2*z
        )*t + 2*z^3 + z^2, Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t + z
  To:   Drinfeld module defined by T |--> (z^3 + z^2 + 2)*t^3 + (z^2 + z)*t + z
  Defn: (z^3 + z^2 + z)*t^11 + (z^3 + z^2 + z)*t^10 + (z^3 + 2*z^2 + 1)*t^9 + 2*z^3*t^8 + (2*z
        ^3 + 2*z^2 + z + 2)*t^7 + (2*z^3 + 2*z^2 + z)*t^6 + t^5 + (2*z^2 + 2)*t^3 + (2*z^3 + z
        ^2 + 2*z)*t^2 + (z^3 + 2*z)*t + z^3]
```

Furthermore, these algorithms readily apply to the computation of $\mathrm{End}(\phi)$.

```
sage: End(phi).basis()
[Identity morphism of Drinfeld module defined by T |--> t^3 + z*t + z, Endomorphism of
    Drinfeld module defined by T |--> t^3 + z*t + z
  Defn: 2*t^3 + 2*z*t + 2*z, Endomorphism of Drinfeld module defined by T |--> t^3 + z*t + z
  Defn: t^9 + (2*z^3 + 2)*t^7 + (2*z^3 + 2)*t^6 + (z^3 + z^2 + 2*z + 2)*t^5 + z^3*t^4 + (2*z^3
       + z^2 + 2*z + 1)*t^3 + t^2 + (2*z^3 + 2*z^2 + 2*z)*t + z^3 + z^2, Endomorphism of
      Drinfeld module defined by T |--> t^3 + z*t + z
  Defn: 2*t^13 + (z^3 + 1)*t^11 + (z^3 + 1)*t^10 + (2*z^3 + 2*z^2 + z + 2)*t^9 + 2*z^3*t^8 +
      (2*z^2 + z + 2)*t^7 + 2*z^3*t^6 + (2*z^3 + 2*z^2 + z + 2)*t^5 + 2*z^3*t^4 + (z^3 + 2*z
      ^2 + z)*t^3 + 2*z^3*t^2 + (z^3 + z^2 + 2*z + 2)*t + z^3]
```

Remark 2.1.32. The fact that $\mathrm{Hom}(\phi, \psi)$ is a vector space over $\mathbb{F}_q$ plays a major computational role, and epitomizes a recurrent theme of this thesis: $\mathbb{F}_q$-linear structures favor computations on Drinfeld modules, while elliptic curves do not have such properties: the endomorphism ring of a curve is a $\mathbb{Z}$-module which cannot be seen as a vector space on a field, as no field lies behind $\mathbb{Z}$. It is an important algorithmic problem to compute isogenies between (or the endomorphism ring of) supersingular elliptic curves [PW23].

2.1.7 Separable isogenies

We introduce *separable* isogenies, which are very convenient to work with. An isogeny of Drinfeld modules is called *separable*, *inseparable* or *purely inseparable* when its underlying Ore polynomial has the same property. In zero $\mathbb{F}_q[T]$-characteristic all isogenies are separable, and an Ore polynomial in $K\{\tau\}$ defines an isogeny on ϕ if and only if its kernel is a sub-$\mathbb{F}_q[T]$-module of $\mathbb{E}(\phi)$. When K has prime $\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$, we have the following statement [Gek91, Par. 1.4], [Pap23, Proposition 3.3.11]:

Proposition 2.1.33. *An Ore polynomial u of $K\{\tau\}$ defines an isogeny from ϕ to some other Drinfeld module ψ if and only if* $\mathrm{Ker}(u)$ *is a sub-$\mathbb{F}_q[T]$-module of $\mathbb{E}(\phi)$ and the height of u divides that of ϕ. In that case:*

(i) if K has $\mathbb{F}_q[T]$-characteristic zero, then u is separable;

(ii) if K has prime $\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$, then u is the product $u_s \cdot \tau^h$ of a separable and a purely inseparable Ore polynomial. Then, there exists a Drinfeld module ψ' such that τ^h defines an isogeny $\phi \to \psi'$ and u_s defines an isogeny $\psi' \to \psi$. Moreover, $\deg(\mathfrak{p})$ *divides h.*

No matter the $\mathbb{F}_q[T]$-characteristic, we define the height $\mathrm{h}(u)$ of u as that of its underlying Ore polynomial u, and similarly define its τ-degree. In $\mathbb{F}_q[T]$-characteristic zero, it is always zero, while in the context of Proposition 2.1.33, the height is h.

Remark 2.1.34. The Frobenius endomorphism is purely inseparable, but it may not be the purely inseparable isogeny with smallest τ-degree; the latter is always $\tau^{\deg(p)}$, which is the Frobenius endomorphism only if $d = [K : \mathbb{F}_q]$ equals $\deg(p)$. For elliptic curves, the situation is similar: the Frobenius endomorphism $(x, y) \mapsto (x^q, y^q)$ is purely inseparable, and the map $(x, y) \mapsto (x^p, y^p)$ defines a purely inseparable isogeny—the one with smallest norm—that is an endomorphism only if the elliptic curve is defined on the prime field $\mathbb{F}_p$.

```
sage: Fq = GF(3)
sage: A.<T> = Fq[]
sage: k.<zk> = Fq.extension(3)
sage: K.<z> = k.extension(3)
```

```
sage: phi = DrinfeldModule(A, [K(zk), 1, z])
sage: t = phi.ore_variable()
sage: psi = phi.velu(t^3)
sage: psi
Drinfeld module defined by T |--> (z^6 + z^2 + 2*z + 1)*t^2 + t + 2*z^6 + 2*z^4 + z^2 + z + 2
sage: t^3 in Hom(phi, psi)  # tau^deg(p)
True
sage: t^3 in End(phi)
False
sage: t^9 in End(phi)  # Frobenius endomorphism
True
sage: t^9 in End(psi)  # Frobenius endomorphism
True
```

Having defined separable isogenies, we can now turn to the definition of the *isogeny norm*.

2.1.8 Norms of isogenies

We have defined in § 2.1.4 the characteristic polynomial of an endomorphism. If u is not an endomorphism, but only an isogeny, we cannot define a characteristic polynomial. However, another invariant is available: the *norm*, which is an ideal of $\mathbb{F}_q[T]$ which measures the size of u. Computing isogeny norms is one of the main objects of this thesis, which we do in Chapter 5. To do so, one of our goal will be to take inspiration from characteristic polynomials of endomorphisms and to compute the norm of an isogeny as the determinant of a polynomial matrix, using Anderson motives (see Theorem 2.1.36 or Equation (3.2) of [Gek91]). But before that, it is necessary to define the *Euler-Poincaré characteristic*.

2.1.8.1 Euler-Poincaré characteristic

The norm of an isogeny is defined in terms of the *Euler-Poincaré characteristic*. Let R be a Dedekind domain. The *Euler-Poincaré characteristic* on R, denoted ξ_R, is a map from the class of finite R-modules to the set of ideals in R. It is defined by the following properties. Firstly, for every short exact sequence of finite R-modules

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

one has

$$\xi_R(M_2) = \xi_R(M_1)\xi_R(M_3).$$

If further $\mathfrak{a}$ is a nonzero ideal of R, we impose

$$\xi_R(R/\mathfrak{a}) = \mathfrak{a}.$$

Those conditions imply that for any finite R-module M, the Euler-Poincaré characteristic $\chi_R(M)$ only depends on the isomorphism class of M. If M is torsion, Noether's theorem on the structure of finitely generated modules over Dedekind domains [Eis95, Exercise 19.6] implies that M decomposes as

$$M \simeq R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_\ell,$$

where $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell$ are ideals of R. In that case,

$$\xi_R(M) = \mathfrak{a}_1 \cdots \mathfrak{a}_\ell.$$

The formation of Euler-Poincaré characteristic commutes with flat scalar extension. In particular, given a finitely generated R-module M and a maximal ideal $\mathfrak{q} \subset R$, we have

$$\xi_R(M) \otimes_R R_{\mathfrak{q}} = \xi_{R_{\mathfrak{q}}}(M \otimes_R R_{\mathfrak{q}}).$$

Similarly, if R' is another Dedekind domain containing R as a subring, we have

$$\xi_R(M) \otimes_R R' = \xi_{R'}(M \otimes_R R').$$

2.1.8.2 Defining norms of isogenies

Now that we have introduced the Euler-Poincaré characteristic, we may define the norm of an isogeny, following [Gek91, § 3]. The definition varies, depending on the $\mathbb{F}_q[T]$-characteristic of K.

Definition 2.1.35. The norm of u, denoted $\mathfrak{n}(u)$, is defined as follows:

(i) If K has $\mathbb{F}_q[T]$-characteristic zero, u is separable, then we set

$$\mathfrak{n}(u) = \xi_{\mathbb{F}_q[T]}(\mathrm{Ker}(\mathbb{E}(u))).$$

(ii) Otherwise, we let $\mathfrak{p}$ be the $\mathbb{F}_q[T]$-characteristic of K, and $\mathrm{h}(u)$ be the height of u, then we set

$$\mathfrak{n}(u) = (\mathfrak{p})^{\mathrm{h}(u)/\deg(p)} \xi_{\mathbb{F}_q[T]}(\mathrm{Ker}(\mathbb{E}(u))).$$

For any a in $\mathbb{F}_q[T]$, Proposition 2.1.16 implies that the norm of the endomorphism defined by ϕ_a is (a^r). If K has prime $\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$, then we recall that $\tau^{\deg(p)}$ defines an isogeny; its norm is $(\mathfrak{p})$ and the Frobenius endomorphism has norm $(\mathfrak{p}^{d/\deg(p)})$.

```
sage: # The norm of phi_a is a^r
sage: a = T^3 + T^2 + T + 1
sage: End(phi)(a).norm() == A.ideal(a^phi.rank())
True
sage: # The norm of tau^deg(p) is p
sage: p = phi.characteristic()
sage: u = Hom(phi, psi)(t^3)
sage: u.norm() == p
True
sage: p
T^3 + 2*T + 1
sage: # The Frobenius norm is p^(d/deg(p))
sage: frob = End(phi)(t^9)
sage: frob.norm()
Principal ideal (T^9 + 2*T^3 + 1) of Univariate Polynomial Ring in T over Finite Field of size
      3
sage: p^3
T^9 + 2*T^3 + 1
```

As for endomorphisms, the norm can be defined using the Anderson motive $\mathbb{M}(\phi)$ and its canonical basis. More precisely, Theorem 2.1.22 extends to the following:

Theorem 2.1.36. *The norm of u is generated by the determinant of $\mathbb{M}(u)$, seen as a matrix with respect to the canonical bases of $\mathbb{M}(\phi)$ and $\mathbb{M}(\psi)$.*

The properties of $\xi_{\mathbb{F}_q[T]}$ imply that the norm is multiplicative: if ψ' is a third Drinfeld $\mathbb{F}_q[T]$-module and v is an isogeny from ψ to ψ', then the norm of vu is the product $\mathfrak{n}(v)\mathfrak{n}(u)$ of the norms.

Remark 2.1.37. Recall Remark 1.1.3. As the isogeny norm is multiplicative and commutative, one can compute the norm of u by splitting it as $\tau^h u_s$ or $u_s\tau^h$.

Remark 2.1.38. To measure the size of an isogeny of Drinfeld modules, an obvious choice would have been to consider its τ-degree. However, a norm defined as such would not be multiplicative, but additive. Rather, the above definition is inspired of elliptic curves: the norm of a separable isogeny α of elliptic curves is the order of its kernel, which is exactly its Euler-Poincaré characteristic $\xi_{\mathbb{Z}}(\mathrm{Ker}(\alpha))$, where the torsion is considered over an algebraic closure of the base field. See also Remark 7.1.2.

2.1.8.3 Dual isogenies

Isogenies with norm (a^r), $a \in \mathbb{F}_q[T]$, can be thought of generalizations of the endomorphism defined by ϕ_a. In this paragraph, we state that *being isogenous* is an equivalence relation; an isogeny from ϕ to ψ exists if and only if one exists from ψ to ϕ. Most isogenies are not isomorphisms, and inverses for this equivalence relation are called *dual isogenies*; the composition of an isogeny and its dual is an endomorphism related to the norm. Let u be an isogeny from ϕ to ψ.

Proposition 2.1.39. *Let (ℓ) be the norm of u. There exists an isogeny $\hat{u} : \psi \to \phi$ such that*

$$\begin{cases} \phi_\ell = \hat{u}u, \\ \psi_\ell = u\hat{u}. \end{cases}$$

Proof. Let a be an element of a_k such that every element of $\mathrm{Ker}(\mathbb{E}(u))$ is of a-torsion for ϕ. Such a always exists: one may decompose $\mathrm{Ker}(\mathbb{E}(u))$ as a product

$$\mathbb{F}_q[T]/(a_1) \times \cdots \times \mathbb{F}_q[T]/(a_k), \quad a_1, \ldots, a_k \in \mathbb{F}_q[T],$$

and take

$$a = a_1 \cdots a_k.$$

Then, $\mathrm{Ker}(\mathbb{E}(u))$ is a subspace of $\mathbb{E}_a(\phi)$. Let u_s be the separable part of u, as defined in Proposition 2.1.33. Its kernel is the same as that of u, and included is the a-torsion. As u_s is separable, then u_s right-divides ϕ_a. If u is a separable isogeny, then (a) is the norm of u, and we are done.

If u is not separable, then the $\mathbb{F}_q[T]$-characteristic is a prime ideal $\mathfrak{p}$, generated by a monic polynomial $p \in \mathbb{F}_q[T]$. Let then h be the height of u, which is nonzero. By definition, the norm of u is generated by the polynomial

$$\ell = p^{h/\deg(p)} a.$$

Let now h_0 be the height of ϕ_p. The height of $\phi_{p^{h/\deg(p)}}$ is $h_0 \cdot h/\deg(p)$. As $\deg(p)$ divides h_0, then

$$h_0 \cdot h/\deg(p) \geqslant h.$$

Therefore, τ^h right-divides $\phi_{p^{h/\deg(p)}}$, and we conclude that $u = \tau^h u_s$ right-divides ϕ_n.

We now show that $\hat{u}$, the right-division of ϕ_ℓ by u, defines an isogeny from ψ to ϕ. This is because $\phi_\ell\phi_T = \phi_T\phi_\ell$ and $\phi_\ell = \hat{u}u$. Indeed, $\phi_T\phi_\ell = \phi_T\hat{u}u = \hat{u}u\phi_T = \hat{u}\psi_T u$, so that $\hat{u}\psi_T = \phi_T\hat{u}$, by right-dividing by u.

Finally, the fact that $\psi_\ell = \hat{u}u$ is true because every element of $\mathrm{Ker}(\hat{u}u)$ is of ℓ-torsion for ψ. As $\hat{u}u$ and ψ_ℓ necessarily have equal degrees, this concludes the proof. □

```
sage: ell = u.norm().gen()
sage: dual_u = u.dual_isogeny()
sage: dual_u
Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> (z^6 + z^2 + 2*z + 1)*t^2 + t + 2*z^6 + 2*z^4 + z^2
      + z + 2
  To:   Drinfeld module defined by T |--> z*t^2 + t + 2*z^6 + 2*z^4 + z^2 + z + 2
  Defn: (2*z^8 + 2*z^7 + 2*z^6 + z^5 + z^3 + z^2 + z + 2)*t^3 + (z^7 + z^5 + z^3 + 2*z^2 + 2*z
        + 2)*t^2 + (2*z^3 + z^2 + 2)*t + 2*z^3 + z + 1
sage: End(phi)(ell) == dual_u * u
True
sage: End(psi)(ell) == u * dual_u
True
```

Remark 2.1.40. Let $\hat{u}$ and ℓ be as in Proposition 2.1.39. We stress that (ℓ) is the norm of $\hat{u}$ if and only if $r = 2$. In the general case, $\hat{u}$ has norm (n^{r-1}). The rank two case, once again, is very similar to the situation of elliptic curves.

Definition 2.1.41. Let $a \in \mathbb{F}_q[T]$, and u' be an isogeny from ψ to ϕ such that $\phi_a = u'u$, and $\psi_a = uu'$. Then, one says that u' is the *a-dual isogeny of* u, or equivalently that u is the *a-dual isogeny of* u'. In particular, with the notations of Proposition 2.1.39, u is an ℓ-isogeny.

2.1.9 Isomorphism classes

We have seen that K-isogeny classes, when K is finite, are encoded by the characteristic polynomial of the Frobenius endomorphism (Theorem 2.1.26). In rank two, the invariant encoding the isomorphism class is rather simple: it is only an element of K, called the *j-invariant*, and it is easily demonstrated that any element of K appears as the j-invariant of a Drinfeld module (§ 2.1.9.1). In larger rank, the situation is more complicated (§ 2.1.9.2).

2.1.9.1 In rank two

In rank, $\overline{K}$-isomorphism classes of Drinfeld $\mathbb{F}_q[T]$-modules are given by so-called j-*invariants*. Let ϕ have rank two and be defined by $\phi_T = \gamma(T) + g\tau + \Delta\tau^2$. Its *j-invariant* is the element

$$\mathrm{j}(\phi) = g^{q+1}/\Delta \in K.$$

It is elementary to verify that two Drinfeld $\mathbb{F}_q[T]$-modules defined over K are isomorphic over $\overline{K}$ if and only if they share the same j-invariant.

```
sage: Fq = GF(5)
sage: A.<T> = Fq[]
sage: K.<z> = Fq.extension(4)
```

```
sage: phi = DrinfeldModule(A, [z, 1, z^3])
sage: psi = DrinfeldModule(A, z * phi(T) * z^(-1))
sage: z in Hom(phi, psi)
True
sage: phi.j_invariant()
4*z^3 + z^2 + 3*z
sage: psi.j_invariant()
4*z^3 + z^2 + 3*z
```

For any scalar j in K, there exists a Drinfeld module whose j-invariant is j: it is defined by $\gamma(T) + \tau^2$ if j equals zero, and $\gamma(T) + \tau + j^{-1}\tau^2$ otherwise.

2.1.9.2 In larger rank

In rank r larger than two, isomorphism classes cannot be encoded in K. Although this bears no importance for our work, we mention Potemine's results [Pot98]. Let ϕ be defined by $\phi_T = g_0 + \cdots + g_r\tau^r$. Potemine defined a family of j-invariants indexed by couples of tuples $((k_1, \cdots, k_n), (d_1, \cdots, d_n, d_r))$ such that:

(i) n is an integer satisfying $n \leqslant r - 1$;

(ii) $1 \leqslant k_1 < \cdots < k_n \leqslant r - 1$;

(iii) $d_r(q^r - 1) = \sum_{i=1}^{n} d_i(q^{k_i} - 1)$.

Then, the $((k_1, \cdots, k_n), (d_1, \cdots, d_n, d_r))$-j-*invariant* of ϕ is

$$\mathrm{j}^{d_1,\cdots,d_n,d_r}_{k_1,\cdots,k_n}(\phi) = \frac{1}{g_r^{d_r}} \prod_{i=1}^{n} g_{k_i}^{d_i}.$$

Any such j-invariant is called *basic* whenever the integers $d_1, \ldots, d_n, d_n$ verify

$$\begin{cases} \gcd(d_1, \cdots, d_n, d_r) = 1 \\ 0 \leqslant d_i \leqslant (q^r - 1)/(q^{\mathrm{GCD}(i,r)} - 1). \end{cases}$$

Potemine proves in [Pot98] that two rank r Drinfeld $\mathbb{F}_q[T]$-modules defined over K are isomorphic over the separable closure of K if and only if their j-invariants agree for any couple of tuples

$$((k_1, k_2, \ldots, k_n), (d_1, d_2, \ldots, d_n, d_r)).$$

This is true if and only if they have the same basic j-invariants. In rank two, the classical j-invariant is the sole basic j-invariant.

```
sage: rho = DrinfeldModule(A, [z, z, 1, z + 1])
sage: rho.basic_j_invariants()
{((1,), (31, 1)): 2*z^3 + 3*z^2 + 2*z + 2, ((1, 2), (1, 5, 1)): 2*z^3 + 3*z^2 + 4, ((1, 2),
    (7, 4, 1)): z^3 + 3*z^2 + 3*z, ((1, 2), (8, 9, 2)): 4*z^3 + 4*z^2 + z + 1, ((1, 2), (9,
    14, 3)): 4*z^3 + z, ((1, 2), (10, 19, 4)): 4*z^3 + z^2, ((1, 2), (11, 24, 5)): 3*z^3 + 3*
    z^2 + 3*z + 3, ((1, 2), (12, 29, 6)): 3*z^3 + 3*z, ((1, 2), (13, 3, 1)): z^3 + 4*z^2 + 2*
    z + 1, ((1, 2), (15, 13, 3)): z^3 + 3*z^2 + 2, ((1, 2), (17, 23, 5)): 4*z^2 + 3*z + 2,
    ((1, 2), (19, 2, 1)): 4*z^2 + z + 3, ((1, 2), (20, 7, 2)): 2*z^3 + 2*z^2 + 2*z + 4, ((1,
    2), (22, 17, 4)): 3*z^3 + 3*z^2 + 2*z + 4, ((1, 2), (23, 22, 5)): 2*z^3 + z^2 + 2*z + 3,
    ((1, 2), (25, 1, 1)): z^2, ((1, 2), (27, 11, 3)): z^3 + 3*z^2 + 2*z + 3, ((1, 2), (29,
    21, 5)): 4*z^3 + 2*z^2 + z + 4, ((1, 2), (31, 31, 7)): 3*z^3 + 3*z^2 + 3*z + 4, ((2,),
    (31, 6)): 3*z^3 + 2*z^2 + 2*z + 4}
```

Remark 2.1.42. We warn the reader that different naming conventions may be employed. We chose to follow that of Potemine, which is also used in the SageMath implementation of Drinfeld modules (3). But in [Pap23], the author uses the following convention:

— the j-invariants of [Pap23] correspond to the basic j-invariants of Potemine;

— the basic j-invariants of [Pap23] correspond to the so-called j_k invariants of Potemine: for any $1 \leqslant k \leqslant r-1$, the j_k invariant of ϕ is the j-invariant $g_k^{(q^r-1)/(q^{\gcd k,r-1})} / g_r^{(q^k-1)/(q^{\gcd k,r-1})}$.

Remark 2.1.43. The fact that in larger rank, the j-invariant does not reduce to a single element in K reminds us of a similar situation in the classical settings: invariants of abelian varieties in dimension larger than one is harder than that of elliptic curves. However, we warn the reader that the rank of a Drinfeld module is not to be considered an analogue of the dimension of a variety; see Remark 2.1.7.

2.2 Drinfeld A-modules

We now define general Drinfeld A-modules, and briefly review some of their features. While the definition is very similar to the case of § 2.1, algorithmics on general Drinfeld modules is far more complicated, mainly due to the fact in that context, an Anderson motive is not free, but only projective. We define Drinfeld modules within the following context. We let C be an algebraic projective curve that is smooth and geometrically connected, and ∞ be a point on C. We fix A, the ring of functions in $\mathbb{F}_q(C)$ that are regular outside ∞. As we have seen in § 1.2, A is a Dedekind domain. We recall that for an ideal $\mathfrak{a}$ of A, the degree of $\mathfrak{a}$ is the dimension the finite $\mathbb{F}_q$-vector space $A/\mathfrak{a}$; the degree of an element a of A is that of (a). Now, we let K denote an extension of $\mathbb{F}_q$, and $\gamma : A \to K$ be a morphism of $\mathbb{F}_q$-algebras.

2.2.1 From $\mathbb{F}_q[T]$ to a general function ring A

This subsection recalls the most important definitions and statements of § 2.1, and generalizes them.

2.2.1.1 Definitions

A *Drinfeld A-module over K* is a morphism of $\mathbb{F}_q$-algebras $\phi : A \to K\{\tau\}$ whose image is not contained in K, and such that the coefficient of ϕ_a is $\gamma(a)$, for any a in A (the notation ϕ_a for $\phi(a)$ is used, as before). Drinfeld $\mathbb{F}_q[T]$-modules are obtained by choosing $C = \mathbb{P}^1(\mathbb{F}_q)$ with its unique point at infinity. A

morphism u of Drinfeld A-modules from ϕ to ψ is defined by an Ore polynomial u in $K\{\tau\}$ such that, for all a in A, $u\phi_a = \psi_a u$. An *isogeny* is a nonzero morphism, and endomorphisms as well as isomorphisms are defined as before. This time, the *A-characteristic* of K—the kernel of γ—is an ideal which may not be principal. It is still possible, however, to distinguish between zero (when γ is injective) and prime A-characteristic (otherwise). The definitions of $\mathbb{E}(\phi)$ (an A-module), $\mathbb{E}(u)$ (a morphism of A-modules), $\mathbb{M}(\phi)$ (a $K\{\tau\} \otimes A$-module) and $\mathbb{M}(u)$ (a morphism of $K\{\tau\} \otimes A$-modules) are unchanged.

2.2.1.2 Rank and height

Let ϕ and ψ be two Drinfeld A-modules. One defines the *rank* of ϕ as the unique and well-defined positive integer r such that $\deg_\tau(\phi_a) = r \deg(a)$, for all a in A. For the height, one again has to assume that K has prime A-characteristic $\mathfrak{p}$. Then, there exists a unique nonnegative integer h such that for any a in A, the height of ϕ_a is $hv_\mathfrak{p}(a)\deg(p)$, where $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation on $K(C)$. As before, isogenies can only exist between Drinfeld modules of equal rank.

2.2.1.3 Restricting general Drinfeld A-modules

If A' is a second function ring satisfying the previous conditions, equipped with a morphism $\gamma' : A' \to K$, and a ring morphism $f : A' \to A$ such that $\gamma' = \gamma \circ f$, we find that f endows A with a structure of integer ring over A', and as such, of finitely generated algebra over A'. If $\phi : A \to K\{\tau\}$ is a Drinfeld module, the composite

$$\phi \circ f : A' \to A \to K\{\tau\}$$

defines a Drinfeld module over A', denoted by $f^*\phi$ and referred to as the *restriction of ϕ along f*.

Considering two Drinfeld A-modules ϕ and ψ as well as a morphism $u : \phi \to \psi$, one checks that the Ore polynomial u defining u also defines an isogeny $f^*\phi \to f^*\psi$, which we denote by f^*u. The construction f^* is therefore a functor from the category of Drinfeld modules over A to the category of Drinfeld modules over A'. The action of f^* on the Anderson motives is easy to describe: the motive $\mathbb{M}(f^*\phi)$ is simply $\mathbb{M}(\phi)$ with the restricted action of A and, and—up to the above identification—the maps $\mathbb{M}(f^*u)$ and $\mathbb{M}(u)$ are the same.

Example 2.2.1. Notice that ϕ and $f^*\phi$ may have different ranks. For example, consider a rank two Drinfeld $\mathbb{F}_q[T]$-module ϕ' over a finite field K, with its Frobenius endomorphism π. Assume that the characteristic polynomial $\chi(\pi)$ of π (a degree 2 polynomial in X with coefficients in $\mathbb{F}_q[T]$) defines a smooth curve, and set $A = \mathbb{F}_q[T][X]/(\chi(\pi))$. Consider the Drinfeld module ϕ defined by $\phi_{\overline{X}} = \phi'_T$ and $\phi_{\overline{Y}} = \pi$, which is well defined because ϕ'_T and π commute. In fact, ϕ' is exactly the restriction of ϕ alongside the canonical injection $\mathbb{F}_q[T] \to A$. However, while $\phi_{\overline{X}}$ has τ-degree two, the dimension over $\mathbb{F}_q$ of $A/(\overline{Y})$ is two, so that $\overline{Y}$ has degree two. Therefore, ϕ has rank one. This example will appear systematically in Chapter 7.

2.2.1.4 Isogenies and endomorphisms

Morphisms between two Drinfeld A-modules ϕ and ψ still form a vector space over $\mathbb{F}_q$, and $\mathrm{End}(\phi)$ also contains a subcommutative ring isomorphic to the function ring A. If K is a finite field, the Frobenius endomorphism is well-defined, as τ^d is a central element in $K\{\tau\}$. We define the height and τ-degree of an isogeny as before. We say that an isogeny is *separable*, *inseparable* or *purely inseparable* when its underlying Ore polynomial u is. Proposition 2.1.33 extends as is to general Drinfeld modules [Gos96, Proposition 4.7.11].

2.2.1.5 Torsion and Tate modules

Let then $\mathfrak{a}$ be an ideal of A. The $\mathfrak{a}$-torsion of ϕ, denoted $\mathbb{E}_\mathfrak{a}(\phi)$, is the $\mathfrak{a}$-torsion of the A-module $\mathbb{E}(\phi)$, *i.e.* the intersection of all $\mathbb{E}_a(\phi)$ for a in $\mathfrak{a}$. Of course, $E_a(\phi)$ and $E_{(a)}(\phi)$ are equal for any a in A. It remains true (Proposition 2.1.16) that $\mathbb{E}_{\mathfrak{a}^n}(\phi) \simeq (A/\mathfrak{a}^n)^r$, provided that $\mathfrak{a}$ is away from the characteristic, and that if this A-characteristic is prime and denoted $\mathfrak{p}$, then $\mathbb{E}_{\mathfrak{p}^n}(\phi) \simeq (A/\mathfrak{p}^n)^{r-h}$, where r and h are respectively the rank and height of ϕ. Let now $\mathfrak{b}$ be a second ideal, coprime to $\mathfrak{a}$. Then $E_{\mathfrak{a}\mathfrak{b}}(\phi) \simeq E_\mathfrak{a}(\phi) \times E_\mathfrak{b}(\phi)$.

From that, and given a prime ideal $\mathfrak{q}$, we define the $\mathfrak{q}$-adic Tate module $\mathbb{T}_\mathfrak{q}(\phi)$ as the inverse limit $\varprojlim_{n\in\mathbb{Z}_{\geqslant 0}} \mathbb{E}_{\mathfrak{q}^n}(\phi)$. It is a free module over $A_\mathfrak{q}$, the completion of A with respect to its $\mathfrak{q}$-adic valuation. If $\mathfrak{q}$ is away from the characteristic, then $\mathbb{T}_\mathfrak{q}(\phi)$ has rank r; otherwise, it has rank $\mathrm{r}(\phi) - \mathrm{h}(\phi)$.

2.2.1.6 Norms and characteristic polynomials

Let $u : \phi \to \psi$ be an isogeny with height h. Its *norm* $\mathfrak{n}(u)$ is $\mathfrak{p}^{h/\deg(p)}\xi_A(\mathrm{Ker}(\mathbb{E}(u)))$ if K has prime A-characteristic $\mathfrak{p}$, and $\mathfrak{n}(u) = \xi_A(\mathrm{Ker}(\mathbb{E}(u)))$ otherwise. If u is an endomorphism, then the *characteristic polynomial* $\chi(u)$ of u is the characteristic polynomial of $\mathbb{T}_\mathfrak{q}(u)$, for any prime ideal $\mathfrak{q}$ of A away from the characteristic; this polynomial has coefficients in A and does not depend on $\mathfrak{q}$ (we prove this in Theorem 4.2.7). It has degree r.

2.2.1.7 Default of principality of A

When A is not $\mathbb{F}_q[T]$, it is not true that $Hom(\phi, \psi)$ is free. However, the A-module $\mathrm{End}(\phi)$ remains projective, with projective-rank $\leqslant r^2$ [Gos96, Theorem 4.7.8]. As far as the Anderson motive $\mathbb{M}(\phi)$ of ϕ is concerned, it is not free over $K \otimes A$ anymore, but only projective, with projective-rank r [Hei04, Section 2]. This significantly hinders the efficiency of algorithms relying on Anderson motives, as linear algebra techniques require working over familiar finite-rank free modules or vector spaces. In this context, it is also not clear how to define j-invariants, or to compute isogenies.

2.2.2 Cultural remarks

We now mention a few more aspects of the theory of general Drinfeld module. While they may not have direct applications in this thesis, we believe they offer valuable insight. Sections 2.2.2.1 exposes the analytical construction of Drinfeld modules. It shows that Drinfeld A-modules over $\mathbb{C}_\infty$ exist, and the construction builds so-called *exponential functions* for function fields as a byproduct. We then turn to another feat of Drinfeld modules, the construction of cyclotomic function fields (§ 2.2.2.2). This insight actually explains the construction of some Drinfeld module-based (broken) cryptosystems (Appendix A).

2.2.2.1 Building general Drinfeld modules

Defining Drinfeld modules when A is not $\mathbb{F}_q[T]$ is not evident. Assuming A is generated by elements $a_1, \ldots, a_n$, this means finding Ore polynomials $f_1, \ldots, f_n$ that pairwise commute and satisfy the algebraic relations between the a_i'. Or as Rosen points out, finding a commutative subring of $K\{\tau\}$ [Ros02, P. 231]. Although it is not required for this thesis, we take the time to mention the *analytic construction of Drinfeld modules*. Let $\mathbb{C}_A$ be constructed as $\mathbb{C}_\infty$, substituting A for $\mathbb{F}_q[T]$, and consider a *lattice* Λ of $\mathbb{C}_A$, *i.e.* a discrete sub-A-module of $\mathbb{C}_A$ that is finitely generated. To Λ, we associate a so-called *exponential function*

$$e_\Lambda : \mathbb{C}_A \to \mathbb{C}_A,$$

defined by

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

This defines a function from $\mathbb{C}_A$ to $\mathbb{C}_A$ that is:

(i) entire, meaning that e_Λ is defined by a power series $\sum_{n=0}^{\infty} e_n z^n$ in $\mathbb{C}_A[[z]]$;

(ii) $\mathbb{F}_q$-linear.

Combined, these two properties imply that e_Λ can be seen as a series in τ, in the same way as q-polynomials can be seen as Ore polynomials. Relabelling the coefficients, we write

$$e_\Lambda(z) = \sum_{i=0}^{\infty} e_i \tau^i(x).$$

The exponential function associated to Λ is the unique entire function of $\mathbb{C}_A$ that has simple zeros on Λ and whose constant coefficient (as a series in τ) is 1. It makes the following sequence exact:

$$0 \longrightarrow \Lambda \longrightarrow \mathbb{C}_A \xrightarrow{e_\Lambda} \mathbb{C}_A \longrightarrow 0$$

While for a in $\mathbb{F}_q$, we have $e_\Lambda(az) = a e_\Lambda(z)$, this is not true if $a \in A$. In that case, assuming a to be nonzero, we now see that the deformation of $e_\Lambda(z)$ by a is given by a Drinfeld A-module over $\mathbb{C}_A$. More precisely, consider the polynomial in x defined by

$$P_a^\Lambda = x \prod_{\overline{\alpha} \in a^{-1}\Lambda/\Lambda} \left(1 - \frac{x}{e_\Lambda(\alpha)}\right).$$

First of all, $a^{-1}\Lambda$ is a sublattice of Λ with same rank, so that the quotient is a finite $\mathbb{F}_q$-vector space. Second, the polynomial does not depend on the choice of representatives. In fact, P_a^Λ is a q-polynomial, and can therefore be seen as an element of $\mathbb{C}_A\{\tau\}$. Setting $P_0^\Lambda = 0$, Theorem 13.23 in [Ros02] states that the map

$$\begin{array}{rccc} \phi^\Lambda : & A & \to & \mathbb{C}_A\{\tau\} \\ & a & \mapsto & a P_a^\Lambda \end{array}$$

defines a Drinfeld A-module over $\mathbb{C}_A$ whose rank r is that of Λ.

The exponential function e_Λ can be recovered from ϕ^Λ by picking an element a of A that is not in $\mathbb{F}_q$, setting $e = \sum_{n=0}^{\infty} e_n \tau^n$, $e_0 = 1$, and solving the equations

$$\left(\sum_{n=0}^{\infty} e_n \tau^n\right) a = \phi_a \left(\sum_{n=0}^{\infty} e_n \tau^n\right).$$

Both members of the equations belong to $\mathbb{C}_A\{\tau\}$; when A is $\mathbb{F}_q[T]$, it suffices to pick $a = T$ to obtain a solvable recursive system of equations. We have actually defined a bijection and its inverse between the set of Drinfeld A-modules of rank r over $\mathbb{C}_A$ and lattices of rank r in $\mathbb{C}_A$. With an appropriate notion of morphism for lattices, this extends to an equivalence of categories. Given that such lattices of rank r always exist, this proves that Drinfeld A-modules of rank r over $\mathbb{C}_A$ always do as well.

Remark 2.2.2. This construction sheds light on both similarities and differences between Drinfeld modules over $\mathbb{C}_A$ and elliptic curves over $\mathbb{C}$. Let us recall that roots of unity are typical "rank one objects", while elliptic curves would be "rank two objects".

— The n-th roots of unity famously form a cyclic group of order n, *i.e.* isomorphic to $\mathbb{Z}/n\mathbb{Z}$. This is also the n-torsion of the quotient of abelian groups $\mathbb{C}/\mathbb{Z}$, equipped with its canonical structure of $\mathbb{Z}$-module.

— Elliptic curves over $\mathbb{C}$, on the other hand, correspond to rank two lattices of $\mathbb{C}$. For each such elliptic curve E, there exists a lattice Λ_E such that, as an abelian group, $E(\mathbb{C})$ is isomorphic to the torus $\mathbb{C}/\Lambda_E$. From Λ_E, the elliptic curve E is recovered using the Weierstraß function, and this correspondence is a bijection, induces an equivalence of categories, once again provided a relevant notion of morphism between lattices. Here, we see the "rank two" appear by taking the n-torsion of $\mathbb{C}/\Lambda_E$, which is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

The fact that $\mathbb{C}$ has dimension two over $\mathbb{R}$ forces lattices to have rank 1 or 2. On the other hand, $\mathbb{C}_A$ is not finite dimensional over $\mathbb{R}_A$; lattices exist in arbitrary rank. In particular, rank one Drinfeld A-modules over $\mathbb{C}_A$ do exist, as we have shown, and provide function fields with their versions of cyclotomic fields and roots of unity (see § 2.2.2.2). Drinfeld modules however appear in far greater generality, and embody in function fields both the aspects of cyclotomy and elliptic curves. For more details, we refer to Chapter 13 of [Ros02] or Chapter 5 of [Pap23].

Remark 2.2.3. The process described in the previous paragraph is called the *analytic uniformization* of Drinfeld modules. As any lattice defines an exponential function, and vice versa, this puts Drinfeld A-modules over $\mathbb{C}_A$ at the heart of the "complex analysis" in $\mathbb{C}_A$. For example, we mention that in function fields, an analogue of the constant $\pi = 3.14\cdots$ is defined with Drinfeld modules. We pick $A = \mathbb{F}_q[T]$ and let C be the so-called *Carlitz module* on $\mathbb{C}_\infty$, defined by $C_T = T + \tau$ [Car35]. Let Λ_C be the rank one lattice associated to C, coming with its exponential function e_C. Using the notations of Papikian in [Pap23, Section 5.4], we let π_C be a generator of Λ, and let $\mathbf{i}$ be a root in $\mathbb{C}_\infty$ of $-(T^q - T)$. Then $\pi_C\mathbf{i}^{-1}$ is an element of $\mathbb{R}_\infty$, which, up to multiples in $\mathbb{F}_q$, is the analogue of π for $\mathbb{C}_\infty$. In his book, Papikian goes on to list several series approximation of this constant, and relates it to zeta functions in $\mathbb{C}_\infty$. Series developments of e_C and its logarithm in terms of binomial coefficients are also given. This construction is obviously inspired from the fact that the classical exponential function is a morphism from $\mathbb{C}$ to $\mathbb{C}^*$ whose kernel is $2i\pi\mathbb{Z}$.

2.2.2.2 Carlitz module and cyclotomic function fields

The Kronecker-Weber theorem is one of the most important results of class field theory, and asserts that any abelian number field lies within a cyclotomic field, *i.e.* an extension of $\mathbb{Q}$ generated by the n-th roots of unity, for some n. Let $\mathbb{Q}_n$ denote such a field. We can also observe that $\mathbb{Q}(\zeta_n)$ is generated by the n-torsion of the $\mathbb{Z}$-module

$$\begin{array}{rcl} \mathbb{Z}\times\mathbb{Q}^* & \to & \mathbb{Q}^* \\ (n,x) & \mapsto & x^n. \end{array}$$

The Galois group of $\mathbb{Q}_n$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. In function fields, cyclotomic fields are defined in terms of Drinfeld modules. Consider the Carlitz module C on $\mathbb{F}_q(T)$, defined by $C_T = T + \tau$. We call *cyclotomic function field over* $\mathbb{F}_q$ any extension generated by the a-torsion $\mathbb{E}_a(C)$ of C, for an a in A. We also note that with this, one can define Carlitz cyclotomic polynomials: if a is monic, the *a-th Carlitz*

cyclotomic polynomial is the product over the primitive elements ζ_a of $\mathbb{E}_a(C)$ of the monomials $x - \zeta$; this polynomial, among other things, has coefficients in A [Pap23, Proposition 7.1.5]. Let us now fix a in A, and let $\mathbb{F}_q(T)_a$ denote $\mathbb{F}_q(T)(\mathbb{E}_a(C))$. There is, this time, an isomorphism between $\mathrm{Gal}(\mathbb{F}_q(T)_a/\mathbb{F}_q(T))$ and $(\mathbb{F}_q[T]/a\mathbb{F}_q[T])^\times$. However, ramification properties of the valuation at infinity of $\mathbb{F}_q(T)$ imply that not every abelian finite extension of $\mathbb{F}_q(T)$ is contained within a cyclotomic function field $\mathbb{F}_q(T)_a$ for some a in A. Papikian discusses two possible solutions. The first one ([Pap23, Theorem 7.1.23]) is to restrict abelian extensions of $\mathbb{F}_q(T)$ to these that are *totally real*. The second one, also explained in [Ros02, Chapter 12], is to enlarge the class of cyclotomic fields. This highlights that while number fields and function fields hold very strong similarities, differences may occur, which embody important distinctions.

Part II
Contributions

Chapter 3
Implementing Drinfeld modules in SageMath

We present and discuss implementations details of the first implementation of Drinfeld modules integrated to the standard distribution of SageMath.

Joint-work with David Ayotte, Xavier Caruso, and Joseph Musleh. See [Ayo+23].

3.1 Overview

Computer algebra systems like SageMath, Magma, Maple, etc, allow users to manipulate complex mathematical objects with ease and reliability. At the beginning of our thesis, Drinfeld modules were unfortunately present in no such system. Consequently, we decided to implement them in SageMath, a widely used free and open source computer algebra system. Our aim was to propose a general interface, with which users would perform all kinds of computations related to Drinfeld modules. No specific application was targeted, and we rather focused on tightly integrating our framework within the SageMath ecosystem. In particular, we were constantly vigilant with maintaining the simplicity of the interface, the clarity and completeness of the documentation, and a thorough coverage of unit tests. Concretely, each class, method or function is augmented with a *doctest* that has a description, tests and examples. The entry point of the documentation is the so-called *docstring* of the *class* `DrinfeldModule`, accessed in the SageMath console by running `DrinfeldModule?`. For a more friendly interface, we refer to the online manual (see also § 3.2.2), which has a section devoted to Drinfeld modules:

```
https://doc.sagemath.org/html/en/reference/drinfeld_modules/index.html
https://doc.sagemath.org/pdf/en/reference/drinfeld_modules/drinfeld_modules.pdf
```

All code showcased in this thesis can be reproduced. Most features are already merged in SageMath, and some are in course of being so. We suggest to directly try our implementation with the latest SageMath version, but also provide instructions to run a Docker image with a fixed SageMath version (in the way of a specific *Git branch*), or to directly build this version. Instructions can be found at:

```
https://github.com/kryzar/thesis
```

Remark 3.1.1. While the code of the fixed version will not be subject to modifications, we warn the reader that any interface element of the standard SageMath distribution may change in the future; such is the way of software.

Development was supported by active engagement with the SageMath developer community. This is an important aspect of free software contribution, which aims at achieving interface and implementation coherence on a global scale. We began working in April of 2022 (Github Issue #33713), and with the help of David Ayotte, Xavier Caruso and Joseph Musleh, the first version was merged in the standard distribution in March of 2023 (Github Pull Request #35026). Since then, many new enhancements and contributions based on our implementation have been proposed (Github Pull Requests #37923, #35386, #36325, #35269, #35991, #35527, #35057, #35260, #35519, #35275, #38174, #38199, #38303). Our library is completely open and as such, we encourage all mathematicians and computer scientists to improve it with any contribution that may interest them.

In § 3.2, we present our interface and some of its capabilities; in § 3.3, we discuss some implementation challenges, and the choices we made to solve them.

3.2 Presentation

Let us briefly recall the definition of Drinfeld $\mathbb{F}_q[T]$-modules. Let K be a field over $\mathbb{F}_q$, coming with a morphism $\gamma : \mathbb{F}_q[T] \to K$ of $\mathbb{F}_q$-algebras. We let $K\{\tau\}$ denote the ring of Ore polynomials twisted by the Frobenius endomorphism $x \mapsto x^q$ of K. It is a noncommutative ring, and a Drinfeld $\mathbb{F}_q[T]$-module ϕ is a morphism of $\mathbb{F}_q$-algebras

$$\phi : \quad \mathbb{F}_q[T] \quad \to \quad K\{\tau\}$$

defined by an image ϕ_T of T satisfying:

$$\phi_T = \gamma(T) + g_1\tau + \cdots + g_r\tau^r$$

and

$$g_r \neq 0.$$

The integer r is the *rank* of the Drinfeld module ϕ. A morphism of $\mathbb{F}_q[T]$-Drinfeld modules u from ϕ to ψ is the datum of an Ore polynomial $u \in K\{\tau\}$ such that

$$u\phi_T = \psi_T u.$$

An isogeny is a nonzero morphism.

3.2.1 Creating Drinfeld modules

To define a Drinfeld $\mathbb{F}_q[T]$-module, specify its function ring $\mathbb{F}_q[T]$ (thereafter `A`) and the list of coefficients of its generator ϕ_T (thereafter `[i, 1, 1]`).

```
sage: Fq = GF(2)
sage: K.<i> = Fq.extension(2)
sage: A.<T> = Fq[]
```

```
sage: phi = DrinfeldModule(A, [i, 1, 1])
sage: phi
Drinfeld module defined by T |--> t^2 + t + i
```

To evaluate elements of $\mathbb{F}_q[T]$ (here, `A`) under the Drinfeld module, simply treat the Drinfeld module object (here, `phi`) as a function.

```
sage: phi(1)
1
sage: phi(T)
t^2 + t + i
sage: phi(T^2 + T + 1)
t^4
```

Notice that the user does not need to specify the ground field K and the morphism γ. Those are inferred by SageMath from the input data: K is recovered as the smallest field extension of $\mathbb{F}_q$ containing the coefficients of ϕ_T, while γ is defined internally as the map which sends the generator of `A` (here, `T`) to the constant coefficient of the generator (here, `i`)—see § 3.3.2. To account for the fact that the morphism γ is an important parameter of the category of Drinfeld modules to which ϕ belongs, the method `base` (or equivalently, `base_ring`) returns an object `RingExtension` rather than an object `Field`. Furthermore, the $\mathbb{F}_q[T]$-characteristic of K, when possible, is automatically computed:

```
sage: phi.base()
Finite Field in i of size 2^2 over its base
sage: phi.base() is K
False
sage: phi.base().backend() is K
True
sage: phi.base_morphism()  # gamma
Ring morphism:
  From: Univariate Polynomial Ring in T over Finite Field of size 2 (using GF2X)
  To:   Finite Field in i of size 2^2 over its base
  Defn: T |--> i
sage: phi.characteristic()
T^2 + T + 1
```

The base morphism γ characterizes the category of Drinfeld modules of which ϕ is an object. In fact, this category is automatically created with ϕ, and the methods `base`, `base_morphism`, etc, are simply shortcuts to these of the category of ϕ. Moreover, the category can be used as a shorter way to create new Drinfeld modules:

```
sage: drinfeld_modules = phi.category()
sage: drinfeld_modules
Category of Drinfeld modules over Finite Field in i of size 2^2 over its base
sage: drinfeld_modules(phi)
Drinfeld module defined by T |--> t^2 + t + i
sage: drinfeld_modules.object([i, i+1, 0, 1, i])
Drinfeld module defined by T |--> i*t^4 + t^3 + (i + 1)*t + i
sage: drinfeld_modules.random_object(rank=3)
Drinfeld module defined by T |--> (i + 1)*t^3 + i*t^2 + t + i
```

When the ground field K is finite, it is possible to recover an element a of $\mathbb{F}_q[T]$ knowing the Ore polynomial ϕ_a. This is done by solving a linear system over $\mathbb{F}_q$.

```
sage: a = T^3 + T^2 + 1
sage: phi.invert(phi(a))
T^3 + T^2 + 1
```

It is also possible to recover the Ore polynomial ring $K\{\tau\}$ that was created when ϕ was instantiated, and to define Drinfeld modules directly with an Ore polynomial rather than a list of coefficients:

```
sage: Ktau = phi.ore_polring()
sage: t = phi.ore_variable()
sage: phi(T) == i + t + t^2
True
```

Note that q may be composite and that the choice of the ground field is not restricted to finite fields:

```
sage: Fq = GF(25)
sage: A = PolynomialRing(Fq, 'T')
sage: K.<T> = FunctionField(Fq)
sage: phi = DrinfeldModule(A, [T, T^2+1, 1/T])
sage: phi
Drinfeld module defined by T |--> 1/T*t^2 + (T^2 + 1)*t + T
```

Remark 3.2.1. At the time of writing this thesis, it is not possible to pick a function ring other than $\mathbb{F}_q[T]$. This is because of the current lack of implementation of such objects in SageMath.

3.2.2 Getting help

Our implementation is accompanied by an extensive documentation, which includes examples and explanations. A special entry for Drinfeld modules was added to the *SageMath Reference Manual*:

`https://doc.sagemath.org/html/en/reference/drinfeld_modules/index.html`
`https://doc.sagemath.org/pdf/en/reference/drinfeld_modules/drinfeld_modules.pdf`

Using SageMath through the interactive console, the user may, at any time, access parts of the documentation, by appending `?` to the name of a variable. For example:

```
sage: DrinfeldModule?
```

opens a text document with all the documentation for the Drinfeld module `phi`;

```
sage: phi?
```

opens a text document with all the documentation for the class `DrinfeldModule`;

```
sage: phi.frobenius_charpoly?
```

opens a text document with all the documentation relevant to compute the characteristic polynomial of the Frobenius endomorphism.

Finally, to list all the methods available for an object, one uses the `dir` function.

```
sage: [method for method in dir(phi) if not method.startswith('_')]
['Hom', 'action', 'an_element', 'base', 'base_morphism', 'base_over_constants_field', '
     base_ring', 'basic_j_invariant_parameters', 'basic_j_invariants', 'categories', 'category
     ', 'characteristic', 'coefficient', 'coefficients', 'coerce', 'coerce_embedding', '
     coerce_map_from', 'constant_coefficient', 'convert_map_from', 'dump', 'dumps', '
     element_class', 'exponential', 'function_ring', 'gen', 'gens_dict', 'gens_dict_recursive
     ', 'get_action', 'get_custom_name', 'goss_polynomial', 'has_coerce_map_from', 'height', '
     hom', 'inject_variables', 'is_exact', 'is_finite', 'is_isomorphic', 'j_invariant', '
     jk_invariants', 'latex_name', 'latex_variable_names', 'logarithm', 'morphism', 'objgen',
     'objgens', 'ore_polring', 'ore_variable', 'parent', 'rank', 'register_action', '
     register_coercion', 'register_conversion', 'register_embedding', 'rename', 'reset_name',
     'save', 'scalar_multiplication', 'variable_name', 'variable_names', 'velu']
```

3.2.3 Morphisms and isogenies

Our library contain various facilities to manipulate morphisms and spaces of morphisms.

3.2.3.1 Morphism objects

Our implementation also handles morphisms and isogenies between Drinfeld modules. Let us first define the following objects.

```
sage: Fq = GF(3)
sage: A.<T> = Fq[]
sage: K.<z> = Fq.extension(2)
sage: phi = DrinfeldModule(A, [z, 0, z, 1])
sage: psi = DrinfeldModule(A, [z, 1, 2, 1])
sage: t = phi.ore_variable()  # tau
```

Most morphism computations are accessed through the so-called *homset* of the Drinfeld modules, which is created using the `Hom` (or `End` for endomorphisms) constructor:

```
sage: Hom(phi, psi)
Set of Drinfeld module morphisms from (gen) t^3 + z*t^2 + z to (gen) t^3 + 2*t^2 + t + z
sage: End(phi)
Set of Drinfeld module morphisms from (gen) t^3 + z*t^2 + z to (gen) t^3 + z*t^2 + z
```

If a is an element of the function ring, one can create the endomorphism ϕ_a by treating `End(phi)` as a function; similarly, any Ore polynomial that defines an endomorphism or an isogeny, can be used to create a `DrinfeldModuleMorphism` object:

```
sage: End(phi)(T + 1)
Endomorphism of Drinfeld module defined by T |--> t^3 + z*t^2 + z
  Defn: t^3 + z*t^2 + z + 1
sage: End(phi)(t^2) == phi.frobenius_endomorphism()
True
sage: Hom(phi, psi)(2*t + z + 1)
Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t^2 + z
  To:   Drinfeld module defined by T |--> t^3 + 2*t^2 + t + z
  Defn: 2*t + z + 1
```

Conversely, if an Ore polynomial is given, it is easy to check if it defines an isogeny, and if so, to find its codomain. To do that, one uses the method `velu`, named after Vélu's formulae for elliptic curves [Vél71]:

```
sage: phi.velu(1 + (z + 1)*t)
Drinfeld module defined by T |--> 2*t^3 + 2*t^2 + 2*t + z
```

3.2.3.2 Computing bases

One is then able to compute various bases of $\mathrm{Hom}(\phi, \psi)$ or $\mathrm{End}(\phi)$—see § 2.1.6. First of all, Wesolowski's algorithm computes, for any $n \in \mathbb{Z}_{\geqslant 0}$, a basis of the $\mathbb{F}_q$-vector space of Drinfeld modules morphisms with degrees less than n; it has been implemented by Musleh (Github Pull Request #35386).

```
sage: Hom(phi, psi).Fq_basis(1)
[Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t^2 + z
  To:   Drinfeld module defined by T |--> t^3 + 2*t^2 + t + z
  Defn: 2*t + z + 1]
sage: Hom(phi, psi).Fq_basis(2)
[Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t^2 + z
  To:   Drinfeld module defined by T |--> t^3 + 2*t^2 + t + z
  Defn: 2*t^2 + (2*z + 2)*t + 1, Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t^2 + z
  To:   Drinfeld module defined by T |--> t^3 + 2*t^2 + t + z
  Defn: t^2 + z*t + z]
sage: End(phi).Fq_basis(3)
[Identity morphism of Drinfeld module defined by T |--> t^3 + z*t^2 + z, Endomorphism of
    Drinfeld module defined by T |--> t^3 + z*t^2 + z
  Defn: t^3 + z*t^2 + z, Endomorphism of Drinfeld module defined by T |--> t^3 + z*t^2 + z
  Defn: t^2]
```

To compute a basis of $\mathrm{Hom}(\phi, \psi)$ or $\mathrm{End}(\phi)$ over $\mathbb{F}_q[\pi]$, where π is in both cases the Frobenius endomorphism of ϕ, one uses the method `basis`:

```
sage: Hom(phi, psi).basis()
[Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t^2 + z
  To:   Drinfeld module defined by T |--> t^3 + 2*t^2 + t + z
  Defn: t + 2*z + 2, Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t^2 + z
  To:   Drinfeld module defined by T |--> t^3 + 2*t^2 + t + z
  Defn: t^3 + 2*z*t^2 + z*t + z]
sage: End(phi).basis()
[Identity morphism of Drinfeld module defined by T |--> t^3 + z*t^2 + z, Endomorphism of
     Drinfeld module defined by T |--> t^3 + z*t^2 + z
  Defn: 2*t^3 + 2*z*t^2 + 2*z]
```

To pick an endomorphism with a certain τ-degree, call `random_element` on the homset:

```
sage: isogeny = Hom(phi, psi).random_element(5)
sage: isogeny
Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> t^3 + z*t^2 + z
  To:   Drinfeld module defined by T |--> t^3 + 2*t^2 + t + z
  Defn: 2*t^5 + (z + 2)*t^4 + (z + 1)*t^3 + (z + 2)*t + 2*z + 1
sage: endomorphism = End(phi).random_element(7)
sage: endomorphism
Endomorphism of Drinfeld module defined by T |--> t^3 + z*t^2 + z
  Defn: 2*t^7 + (2*z + 2)*t^6 + t^5 + 2*t^3 + 2*z + 2
```

3.2.3.3 Norms and dual isogenies

Those methods act on the *homset*, and it is also possible to directly act on morphisms and isogenies; these have their own type `DrinfeldModuleMorphism`. The norm of an isogeny is computed through the method `norm` and using Algorithm 7 (which is presented in Chapter 5).

```
sage: isogeny_norm = isogeny.norm()
sage: isogeny_norm
Principal ideal (T^5 + 2*T^4 + T^2 + 2*T + 2) of Univariate Polynomial Ring in T over Finite
     Field of size 3
```

Notice that the result is an ideal, following the definition of the norm (see Definition 2.1.35). Let a be its monic generator. Letting u denote the isogeny (here, `isogeny`) and $\hat{u}$ be its dual isogeny (thereafter, `dual_isogeny`), we have $\phi_a = \hat{u}u$ and $\psi_a = u\hat{u}$. The a-dual isogeny $\hat{u}$ can be computed with the method `dual_isogeny`:

```
sage: a = isogeny_norm.gen()
sage: a
T^5 + 2*T^4 + T^2 + 2*T + 2
sage: dual_isogeny = isogeny.dual_isogeny()
sage: End(phi)(a) == dual_isogeny * isogeny
True
sage: End(psi)(a) == isogeny * dual_isogeny
True
```

3.2.3.4 Characteristic polynomials

As for norms, we can compute characteristic polynomials. For general endomorphisms, we use Algorithm 6, which is presented in Chapter 4.

```
sage: charpoly = endomorphism.charpoly()
sage: charpoly
X^3 + (T^2 + T + 2)*X^2 + (2*T^4 + T^3 + T^2 + T)*X + T^7 + T^6 + 2*T^5 + T^3 + 1
sage: charpoly(endomorphism)
Endomorphism of Drinfeld module defined by T |--> t^3 + z*t^2 + z
  Defn: 0
```

In the case of the Frobenius endomorphism, several algorithms are implemented:

(i) the algorithm based on crystalline cohomology of Musleh and Schost [MS23], used with the argument `'crystalline'` (labeled "Musleh-Schost" in Figure 6.1);

(ii) Algorithm 6, used with the argument `'motive'` (labeled `F-MFF` in Figure 6.1);

(iii) Algorithm 9, used with the argument `'CSA'` (labeled `F-CSA` in Figure 6.1);

(iv) and Algorithm of Gekeler presented in [Gek08] and adapted by Musleh for ranks greater than two.

The user can choose either of these by using the `algorithm` option, but does not need to do so: the `'crystalline'` algorithm is automatically picked when the extension degree d is less than the rank, and the `'CSA'` algorithm is picked otherwise:

```
sage: phi.frobenius_charpoly(algorithm='CSA')
X^3 + X^2 + (T + 2)*X + 2*T^2 + T + 1
sage: phi.frobenius_charpoly(algorithm='crystalline')
X^3 + X^2 + (T + 2)*X + 2*T^2 + T + 1
sage: phi.frobenius_charpoly(algorithm='gekeler')
X^3 + X^2 + (T + 2)*X + 2*T^2 + T + 1
sage: phi.frobenius_charpoly(algorithm='motive')
X^3 + X^2 + (T + 2)*X + 2*T^2 + T + 1
```

Various benchmarks are presented in § 4, and most of all in § 6.4.

In rank two and over a finite field, quickly computing the characteristic polynomial of the Frobenius endomorphism allows to efficiently determine if the Drinfeld module is ordinary, supersingular, or neither of these, by Proposition 2.1.25.

```
sage: phi.is_ordinary()
True
sage: phi.is_supersingular()
False
```

We warn the user that `phi.frobenius_endomorphism().norm()` returns a different result than `phi.frobenius_norm()`. This is because the former sees `phi.frobenius_endomorphism()` as an isogeny, and its norm, which is an ideal generated by a monic polynomial.

```
sage: phi.frobenius_norm()
2*T^2 + T + 1
sage: phi.frobenius_endomorphism().norm()
Principal ideal (T^2 + 2*T + 2) of Univariate Polynomial Ring in T over Finite Field of size 3
```

3.2.3.5 Isogeny and isomorphism classes

As two Drinfeld $\mathbb{F}_q[T]$-modules over a finite field are isogenous if and only if they have the same characteristic polynomial of the Frobenius endomorphism, the method `is_isogenous` is easily implemented:

```
sage: phi.is_isogenous(psi)
True
```

To check if two Drinfeld modules are isomorphic, it would be possible to use the definitions and results of § 2.1.9.2. As pointed out by Caruso in the Github Pull Request #35527, this is not the most efficient approach. One can instead directly check if there exists an element ι in $\overline{K}$ such that $\iota\phi_T = \psi_T\iota$. Write $\phi_T = g_0 + \cdots + g_r\tau^r$ and $\psi_T = g'_0 + \cdots + g'_r\tau^r$, and note that if there exists an index $0 \leqslant j \leqslant r$ such that one of g_j or g'_j is zero while the other is not, then the Drinfeld modules are not isomorphic. We thus assume that this does not happen, and we then $I = \{i_1, \ldots, i_n\}$ be the ordered subset of nonzero indices for which both g_i and g'_i are nonzero (one necessarily has $i_1 = 0$ and $i_n = r$). Then:

Lemma 3.2.2. *For any $1 \leqslant j \leqslant n$, let*

$$\begin{cases} y_j = g_{i_j}/g'_{i_j}, \\ a_j = q^{i_j} - 1. \end{cases}$$

Fix $x_1 = y_1$, $e_1 = a_1$, and consider the following sequences, defined recursively for all $1 \leqslant j \leqslant n$ by:

$$\begin{cases} e_j = s_j e_{j-1} + a_j t_j, \\ x_j = x_{j-1}^{s_j} y_j^{t_j}, \end{cases}$$

where e_j is the gcd of e_{j-1} and t_j, while a_j, and s_j and t_j are the associated Bézout coefficients.

Then, ϕ and ψ are isomorphic (over the algebraic closure) if and only if x_n is a solution to all equations

$$x^{a_j/e_n} = y_j, \quad 1 \leqslant j \leqslant n. \tag{3.1}$$

In that case, an isomorphism (over the algebraic closure) is given by any e_n-th root of x_n.

Proof. An isomorphism from ϕ to ψ is a solution over $\overline{K}$ in x to the following system of equations:

$$g'_i x^{q^i - 1} = g_i, \quad 0 \leqslant i \leqslant r.$$

As explained, one can only consider indices in I, and instead solve for x in

$$x^{a_j} = y_j, \quad 1 \leqslant j \leqslant n. \tag{3.2}$$

One then has to verify the claim that Equation 3.2 has a solution (over $\overline{K}$) if and only if x_n is a solution of the system 3.1.

It is elementary to verify that if α is any solution to the system 3.1, then any of its e_n-th root is a solution to the system 3.2, *i.e.* defines an isomorphism.

We thus focus on proving that if ι is a solution to the system 3.2, then x_n is a solution to the system 3.1. The first step is to assert the following identities:

$$x_j^{a_j} = \iota^{e_j}, \quad 1 \leqslant j \leqslant n.$$

This is true for $j = 1$, as we have $i_1 = 0$, and so $x_1 = y_1 = g_0/g_0' = 1$ and $a_1 = q^0 - 1 = 1$. We then proceed by induction, letting $2 \leqslant j \leqslant n$, and assuming that $x_{j-1} = \iota^{e_{j-1}}$. As $x_j = x_{j-1}^{s_j} y_j^{t_j}$, we have $x_j = (\iota^{e_{j-1}})^{s_j} y_j^{t_j}$. But by definition of ι, we also have $\iota^{a_j} = y_j$. We end up with

$$\begin{aligned} x_j &= \iota^{e_{j-1}s_j} \iota^{t_j a_j} \\ &= \iota^{e_{j-1}s_j + t_j a_j} \\ &= \iota^{e_j} \end{aligned}$$

This finishes the induction. The rest of the proof is straightforward: for any $1 \leqslant j \leqslant n$, we have

$$x_n^{a_j/e_n} = (\iota^{e_n})^{a_j/e_n} = \iota^{a_j} = y_j,$$

and we conclude. □

Remark 3.2.3. Lemma 3.2.2 and its proof actually showcase a method for computing solutions to finite system of equations of the form $x^{a_i} = b_i$.

```
sage: phi.is_isomorphic(psi)
False
sage: rho = DrinfeldModule(A, [z, z^2, z+1])
sage: j = rho.j_invariant()
sage: sigma = DrinfeldModule(A, [z, 1, 1/j])
sage: rho.is_isomorphic(sigma)
True
```

3.2.4 Potemine j-invariants

As seen in § 2.1.9.2, Potemine j-invariants are implemented. This implementation is due to Ayotte (see Github Pull Request `#35057`, and less importantly, Github Pull Request `#37630`). As the Potemine j-invariant may exist in infinite quantity, the implementation focuses on *basic* j-invariants, and their subset of j_k-invariants. To get the parameters $((k_1, \cdots, k_n), (d_1, \cdots, d_n, d_r))$ of all the basic j-invariants, use `basic_j_invariant_parameters`, which relies on algorithms for convex polyhedra.

```
sage: phi.basic_j_invariant_parameters()
[((1,), (13, 1)), ((1, 2), (1, 3, 1)), ((1, 2), (5, 2, 1)), ((1, 2), (6, 5, 2)), ((1, 2), (7,
    8, 3)), ((1, 2), (8, 11, 4)), ((1, 2), (9, 1, 1)), ((1, 2), (11, 7, 3)), ((1, 2), (13,
    13, 5)), ((2,), (13, 4))]
```

For a given parameter, one computes the corresponding j-invariant using the `j_invariant` method. Also, the method `basic_j_invariants` returns the ordered list of all basic j-invariants, while the method `jk_invariants` returns the sublist of j_k-invariants.

```
sage: phi.basic_j_invariants()
{((1,), (13, 1)): 0, ((1, 2), (1, 3, 1)): 0, ((1, 2), (5, 2, 1)): 0, ((1, 2), (6, 5, 2)): 0,
     ((1, 2), (7, 8, 3)): 0, ((1, 2), (8, 11, 4)): 0, ((1, 2), (9, 1, 1)): 0, ((1, 2), (11, 7,
      3)): 0, ((1, 2), (13, 13, 5)): 0, ((2,), (13, 4)): 2*z}
```

```
sage: phi.jk_invariants()
{1: 0, 2: 2*z}
```

Many options are available, and we refer to the documentation for more details.

3.2.5 Exponential, logarithm and Drinfeld modular forms

We now showcase computational capabilities in $\mathbb{F}_q[T]$-characteristic zero. While representing the field $\mathbb{C}_\infty$ remains a challenge, it is still possible to define Drinfeld modules over $\mathbb{F}_q(T)$, or any function field whose field of constants is $\mathbb{F}_q$ that can be represented in SageMath.

```
sage: q = 25
sage: Fq = GF(q)
sage: A = PolynomialRing(Fq, 'T')
sage: K.<T> = FunctionField(Fq)
sage: phi = DrinfeldModule(A, [T, T + 1/T, T^2])
```

Thanks to a contribution of Ayotte (Github Pull Request `#35260`), one can compute the logarithm and exponential series associated to a Drinfeld Module; see § 2.2.2.1 for an overview of these objects. For Drinfeld $\mathbb{F}_q[T]$-modules defined over $\mathbb{F}_q(T)$, these series have coefficients in $\mathbb{F}_q(T)$, and they can be computed using simple formulas. They also are q-series, in the sense that only coefficients whose index is a power of q are nonzero. The SageMath objects we compute are called *lazy* series, meaning that the n-th coefficient is returned on demand:

```
sage: phi_exponential = phi.exponential()
sage: phi_exponential
z + O(z^8)
sage: phi_exponential[q]
1/(T^24 + 4*T^22 + T^20 + 4*T^18 + T^16 + 4*T^14 + T^12 + 4*T^10 + T^8 + 4*T^6 + T^4 + 4*T^2)
sage: phi_exponential[q^2]
(T^603 + 4*T^553 + T^503 + 4*T^453 + T^403 + 4*T^353 + T^303 + 4*T^253 + T^203 + 4*T^153 + T
     ^103 + 4*T^53 + T^2 + 1)/(T^1226 + 4*T^1176 + T^1126 + 4*T^1076 + T^1026 + 4*T^976 + T
     ^926 + 4*T^876 + T^826 + 4*T^776 + T^726 + 4*T^676 + 4*T^602 + T^552 + 4*T^502 + T^452 +
     4*T^402 + T^352 + 4*T^302 + T^252 + 4*T^202 + T^152 + 4*T^102 + T^52)
```

```
sage: phi_logarithm = phi.logarithm()
sage: phi_logarithm
z + O(z^8)
sage: phi_logarithm[q]
4/(T^24 + 4*T^22 + T^20 + 4*T^18 + T^16 + 4*T^14 + T^12 + 4*T^10 + T^8 + 4*T^6 + T^4 + 4*T^2)
sage: phi_logarithm[q^2]
(4*T^51 + T^50 + T^49 + 4*T^47 + T^45 + 4*T^43 + T^41 + 4*T^39 + T^37 + 4*T^35 + T^33 + 4*T^31
      + T^29 + 1)/(T^674 + 4*T^672 + T^670 + 4*T^668 + T^666 + 4*T^664 + T^662 + 4*T^660 + T
     ^658 + 4*T^656 + T^654 + 4*T^652 + 4*T^50 + T^48 + 4*T^46 + T^44 + 4*T^42 + T^40 + 4*T^38
      + T^36 + 4*T^34 + T^32 + 4*T^30 + T^28)
```

We conclude this section by mentioning Drinfeld modular forms, which are the function field analogues of classical modular forms; see [Gos80; Gek88] for definitions and [Ayo+23] for algorithms. They have been implemented by Ayotte (Github Pull Request #36538) and are related to Drinfeld modules. One link between the Drinfeld modules and Drinfeld modular forms is given by *Goss polynomials*, which are defined in the third section of [Gek88]. To each Drinfeld $\mathbb{F}_q[T]$-module over a function field K with zero $\mathbb{F}_q[T]$-characteristic, one associates a family (indexed over $\mathbb{Z}_{\geqslant 0}$) of Goss polynomials.

```
sage: phi.goss_polynomial(0)
0
sage: phi.goss_polynomial(1)
X
sage: phi.goss_polynomial(2)
X^2
```

3.3 Discussion

We now discuss various implementation decisions.

3.3.1 The base type of Drinfeld modules

In SageMath, every type inherits a larger type. Choosing which is an important part of the development process; we propose to discuss this issue.

In SageMath (and more generally, in Python since, as of the third version), the notion of *type* coincides with that of *class*. *Classes* are a way for programmers to specify how a collection of data should be represented and accessed by an external user, and to specify operations on (but not restricted to) this data. Those operations are called *methods*. For a mathematician, the concept of class is very natural: they understand that a vector is a collection of scalars in a space, and that vectors can be added through a dedicated + operation. To computationally represent these, they could create the following class:

```
sage: class Vector:
....:     def __init__(self, coefficients):
....:         self.coefficients = coefficients
....:     def add(self, other):
....:         coeffs = self.coefficients
....:         coeffs_other = other.coefficients
....:         new_coeffs = [coeffs[i] + coeffs_other[i] for i in range(len(coeffs))]
....:         return Vector(new_coeffs)
....:     def norm(self):
....:         return sqrt(sum(a^2 for a in self.coefficients))
```

Once the class has been created, we can create objects for this class.

```
sage: x = Vector([0, 1])
sage: y = Vector([2, -1])
sage: z = x.add(y)
sage: z.coefficients
[2, 0]
sage: z.norm()
2
```

While a class is not itself a collection of data and methods, it can be thought of as the factory which produces these collections, the same way that a type is not an object of itself; the objects created using a class are called *instances* of the class. The fact that classes and types coincide means that the type of an object is simply and exactly the factory that produced it. Therefore, two distinct factories cannot produce two similar objects, as these would not have the same type.

Defining a very basic class for Drinfeld modules would look like this:

```
sage: class DrinfeldModule_:
....:     def __init__(self, function_ring, gen):
....:         self.function_ring = function_ring
....:         self.gen = gen
....:     def rank(self):
....:         return self.gen.degree()
....:     def eval(self, a):
....:         return a(self.gen)
```

We have specified the data (`function_ring` and `gen`) and methods (`rank` and `eval`). Now, instances of `DrinfeldModule_` could be created as

```
sage: Fq = GF(2)
sage: K.<i> = GF(4)
sage: frob = K.frobenius_endomorphism()
sage: Ktau.<t> = OrePolynomialRing(K, frob)
sage: function_ring.<T> = Fq[]
sage: gen = i + t + t^2
sage: drinfeld_module_ = DrinfeldModule_(function_ring, gen)
sage: drinfeld_module_.rank()
2
sage: drinfeld_module_.eval(T)
t^2 + t + i
```

In SageMath, classes follow an inheritance logic: every class derivates from a larger, parent class. Think about it this way: a class representing an elliptic curve would inherit a class representing schemes, because an elliptic curve is a scheme satisfying extra conditions, for which extra functionalities (*e.g.* a Weil pairing) are available. But an elliptic curve remains a scheme, and an instance of the `EllipticCurve` class is also an instance of the `Scheme` class. More generally, instances of a child class are instances of all its parent classes, and child classes can have multiple parent classes. In the context of SageMath, every object is usually one of three abstract things:

(i) a category (class `Category` and its derivatives),

(ii) a set (class `Parent` and its derivatives) which is an object in some category,

(iii) or an element (class `Element` and its derivatives) which is an element in a set.

This is the `Parent/Element` framework, a cornerstone of most of the inner workings of SageMath. For example, the so-called *Test Suite* of any parent verifies that its category is a subcategory of that of sets, or that it can create elements with a method called `an_element`; the *Test Suite* of a `Morphism` objects verify that the domain and codomain are both parents, etc. However, Drinfeld modules have no underlying sets. We faced several possibilities.

(i) Making Drinfeld modules `Elements` whose `Parent` is the set of morphisms $\mathbb{F}_q[T] \to K\{\tau\}$ (the so-called *homsets* in SageMath). This approach follows the traditional `Parent/Element` but does not account for the fact that the "set" of Drinfeld modules should rather be viewed as a category.

(ii) Making Drinfeld modules `Parents` without `Elements`. From a mathematical point of view, this acknowledges the fact that not all categories are subcategories of the category of sets. This approach also follows the implementation of elliptic curves—in SageMath, an elliptic curve `E` is a scheme, and `E.an_element()` return an element whose `Parent` is not `E`, but the group `G` of points of `E`. This option makes the implementation of morphisms between Drinfeld modules (and, more generally, of the category of Drinfeld modules) easier than the previous one. Besides, seeing Drinfeld modules as function field analogues of elliptic curves, it has a strong mathematical basis. However, this approach requires revisiting the testing process, as SageMath expects subclasses of `Parent` to have elements.

(iii) Making Drinfeld modules instances of the `CategoryObject`. This class does exist in SageMath and it is not expected to have elements. Unfortunately, its usage is sporadic, and currently incompatible with `Morphism` objects. This class is no longer maintained and is possibly intended to eventually disappear eventually.

We discussed all these options at length with the SageMath core developers (see Github Pull Request `#37313` and Github Pull Request `#34534`). At some point, the third option looked to us the most mathematically appealing; however given that `CategoryObject` is not fully supported, we decided to rule out this possibility. On the other hand, the first option seems more practical but we believed that it was too mathematically misleading; it would also have required a workaround to make morphisms work. We then ultimately chose the second option.

3.3.2 Testing

We implemented testing on two levels:

(i) Ensuring the user can only create sound objects.

(ii) Ensuring that computations are correct.

For the first point, most of the difficulty lies in checking the input of `DrinfeldModule`. Recall from § 3.2 that to create a Drinfeld $\mathbb{F}_q[T]$-module over a field K, the user provides $\mathbb{F}_q[T]$ and the coefficients defining ϕ_T:

```
sage: Fq = GF(2)
sage: K.<i> = Fq.extension(2)
sage: A.<T> = Fq[]
sage: phi = DrinfeldModule(A, [i, 1, 1])
sage: phi
Drinfeld module defined by T |--> t^2 + t + i
```

SageMath then proceeds as follows:

(i) The input A is checked to be a ring of polynomials (class `PolynomialRing_general`) whose ring of coefficients is a finite field (method `base_ring` on A and then methods `is_finite` and `is_field` on the base ring of A).

(ii) The second input is checked to be either a list or an `OrePolynomial` object.

  (a) In the first case, the smallest space containing all the coefficients is created (using the `universe` method of the `Sequence` class). It will later be checked to be an extension of $\mathbb{F}_q$.

  (b) In the second case, the underlying Ore polynomial ring is kept in memory and will be reused as the associated Ore polynomial ring of the Drinfeld module. In particular, the variable representing τ will be that used for the Drinfeld module.

  If the second input is neither a list nor an Ore polynomial, an error is raised.

(iii) The Ore polynomial is checked to have a nonzero constant coefficient.

(iv) The ground space of the Ore polynomial ring is checked to be an extension of $\mathbb{F}_q$ (ensuring that this space has a method `has_coerce_map_from` and that this method returns `True` when evaluated on $\mathbb{F}_q$).

(v) Then, an object `RingExtension`—representing the field K with its structure of $\mathbb{F}_q[T]$-algebra given by γ—is created. In SageMath, a `RingExtension` object is created by specifying a ring R and a morphism $S \to R$, where S is another ring. We have three possibilities.

(a) If the user gives an Ore polynomial as second input, and the base space of the parent Ore polynomial ring is already a `RingExtension` object, this object is kept.

(b) If the base field has a canonical map from the function ring (in the SageMath idiom, a *coerce map*, which is checked with `has_coerce_map_from`) and that the coerce map maps T to the constant coefficient, then the ring extension is built with the coerce map.

(c) If the base field has no coerce map from the function ring, SageMath tries to define a map which maps T to the constant coefficient, and to use it to define the ring extension.

(vi) Now that we have valid input, the category of Drinfeld modules can be built. Its only input is the `RingExtension` object created at the previous step. Among other things, it is the category that handles the creation of the Ore polynomial ring.

(vii) Then, the `OrePolynomial` object representing ϕ_T is created, and the `DrinfeldModule` object is created following the multiple possibilities of § 3.3.3.

Although we only present the `DrinfeldModule` class, every construction of an object related to Drinfeld modules (*e.g.* a `DrinfeldModuleMorphism` object or the category `DrinfeldModules`) is checked in a similar fashion. With this approach, we aim at earning the confidence of the user in our implementation, and to allow them writing code that is meaningful to their work.

As far as the computations are concerned (*e.g.* norm or characteristic polynomial computation), tests are written for each method. They verify "normal" as well as edge cases. These tests can be run manually, and they are run automatically at least once before each new SageMath release.

3.3.3 The specialized Drinfeld module classes

Although all objects representing Drinfeld modules are instances of the `DrinfeldModule` class, we have introduced several subclasses of `DrinfeldModule` (*i.e.* classes that inherit `DrinfeldModule`), whose role is to specialize on specific cases.

(i) Drinfeld modules whose ground field is finite are `DrinfeldModule_finite` objects. Methods involving the Frobenius endomorphism, ordinarity and supersingularity, and the `inverse` method, are implemented in this class.

(ii) Drinfeld modules whose ground field has zero $\mathbb{F}_q[T]$-characteristic are `DrinfeldModule_charzero` objects (see Github Pull Request `#36325`). Methods involving logarithm and exponential series, and Goss polynomials, are implemented in this class.

Notice that this is transparent to the user, who does not to manually select the specialized class.

```
sage: Fq = GF(11)
sage: A.<T> = Fq[]
```

```
sage: # Charzero Drinfeld modules
sage: K = Frac(A)
sage: phi = DrinfeldModule(A, [K(T), 1])
sage: from sage.rings.function_field.drinfeld_modules.charzero_drinfeld_module import
     DrinfeldModule_charzero
sage: isinstance(phi, DrinfeldModule)
True
sage: isinstance(phi, DrinfeldModule_charzero)
True
```

```
sage: # Finite Drinfeld modules
sage: K.<z> = Fq.extension(5)
sage: phi = DrinfeldModule(A, [z, 1])
sage: from sage.rings.function_field.drinfeld_modules.finite_drinfeld_module import
     DrinfeldModule_finite
sage: isinstance(phi, DrinfeldModule)
True
sage: isinstance(phi, DrinfeldModule_finite)
True
```

When the user runs `phi = DrinfeldModule(A, [z, 1])`, SageMath bypasses the standard object creation process (which mainly involves calling a method nammed `__init__`), and instead enters in a specific method called `__classcall_private__`, redefined for our purpose. It is this method—which also checks the input (see § 3.3.2)—which decides what subclass of `DrinfeldModule` is to be used appropriate. This choice made, `__classcall_private__` prepares the input for the subclass, calls it, and returns the desired object. Notice that Drinfeld modules that do not fit `DrinfeldModule_finite` or `DrinfeldModule_charzero` (*i.e.* Drinfeld modules with positive $\mathbb{F}_q[T]$-characteristic whose ground field is infinite) are instances of `DrinfeldModule`, meaning the `__classcall_private__` method of `DrinfeldModule` can decide to choose `DrinfeldModule` directly.

Those mechanisms are rather ubiquitous in SageMath. They rely on the concept of *metaclass*, which are to classes what classes are to objects. In other words, a metaclass is a class whose objects are classes, which is thought as a "class factory". This concept is key to ensuring that different algorithms can be used to solve a same task in different situations. For example, when the user runs `FiniteField(q)`, `FiniteField` acts as a metaclass, and decide which implementation of finite fields to use, depending on the input `q`. This way, special implementations for characteristic two can be used.

```
sage: type(FiniteField(2))
<class 'sage.rings.finite_rings.finite_field_prime_modn.FiniteField_prime_modn_with_category'>
sage: type(FiniteField(3))
<class 'sage.rings.finite_rings.finite_field_prime_modn.FiniteField_prime_modn_with_category'>
sage: type(FiniteField(4))
<class 'sage.rings.finite_rings.finite_field_givaro.FiniteField_givaro_with_category'>
```

Furthermore, all Drinfeld module objects have *unique representation*: two Drinfeld modules that are equal are represented by the same SageMath object. This adds security and efficiency while limiting the amount of code, as mutability does not require any handling.

```
sage: drinfeld_modules = phi.category()
sage: psi = drinfeld_modules.object(phi(T))
sage: phi == psi
True
sage: phi is psi
True
```

Chapter 4
Computing characteristic polynomials of endomorphisms with Anderson motives

In this chapter, we compute characteristic polynomials of endomorphisms of Drinfeld modules. Our algorithms work for any endomorphism u, any function ring A, any rank r and any ground field K. When A is $\mathbb{F}_q[T]$, we provide thorough complexity analyses, and optimizations for function fields and the Frobenius endomorphism. Our method is based on the dual correspondence between Drinfeld modules and their Anderson motives.

Joint-work with Xavier Caruso. See Section 2 of [CL23].

4.1 Overview

We first let K be a finite extension of $\mathbb{F}_q$, of degree d. In that case, the $\mathbb{F}_q[T]$-characteristic of K is necessarily a prime ideal $\mathfrak{p}$, and we let p be the unique monic generator of $\mathfrak{p}$. Let now ϕ be a rank two Drinfeld $\mathbb{F}_q[T]$-module over K, accompanied by its Frobenius endomorphism π. By Lemma 2.1.28, there exists $t(T)$ in $\mathbb{F}_q[T]$ with degree $\leqslant d/2$ such that the bivariate polynomial defined by

$$\chi(\pi) = X^2 - t(T)X + (-1)^d \,\mathrm{N}_{K/\mathbb{F}_q}(\Delta)^{-1} p^{d/\deg(p)}$$

annihilates the Frobenius endomorphism:

$$\chi(\pi)(\pi) = \pi^2 - \phi_t \pi + (-1)^d \,\mathrm{N}_{K/\mathbb{F}_q}(\Delta)^{-1} \phi_{p^{d/\deg(p)}} = 0.$$

The polynomial $\chi(\pi)$ is the *characteristic polynomial* of π; it determines the isogeny class of ϕ (Theorem 2.1.26), and if ϕ is ordinary or supersingular (Proposition 2.1.25 and § 2.1.5). Because they fully determine $\chi(\pi)$, recall from § 2.1.4.2 that we call $-t$ the *Frobenius trace*, and that the constant coefficient of $\chi(\pi)$ is the *Frobenius norm*. Given that the Frobenius norm is expressed by a closed formula, computing $\chi(\pi)$ simply amounts to computing the Frobenius trace; this problem is the Drinfeld module equivalent of computing the number of $\mathbb{F}_q$-rational points of an elliptic curve over $\mathbb{F}_q$. In the Drinfeld module case, $\chi(\pi)$ can be computed using several methods inspired by elliptic curves (§ 6.4).

Remark 4.1.1. Notice, however, that while the Frobenius norm of an elliptic curve over $\mathbb{F}_q$ is always equal to q, for Drinfeld modules, it depends on d and Δ.

To define $\chi(\pi)$, one has to look for a classical free module with rank two. If $\mathfrak{q}$ is a prime ideal away from the characteristic, the $\mathfrak{q}$-adic Tate module $\mathbb{T}_\mathfrak{q}(\phi)$ (§ 2.1.3) is exactly that, and we define the characteristic

polynomial of π as that of $\mathbb{T}_{\mathfrak{q}}(\pi)$. Notice that many aspects of the definition can be generalized: first of all, π may be replaced by any endomorphism u, as the endomorphism $\mathbb{T}_{\mathfrak{q}}(u)$ is always well-defined. Second, if A is a function ring as in § 2.2, and ϕ is a Drinfeld A-module with rank r, then $\mathbb{T}_{\mathfrak{q}}(\phi)$ remains a free $A_{\mathfrak{q}}$-module with rank r, as long as $\mathfrak{q}$ is away from the A-characteristic. We thus define $\chi(u)$ as the characteristic polynomial of u. In particular, $\chi(u)$ is a degree r monic polynomial

$$\chi(u) = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in A[T]$$

that satisfies

$$u^r + \phi_{a_{r-1}}u^{r-1} + \cdots + \phi_{a_0} = 0.$$

The fact that χ has coefficients in $\mathbb{F}_q[T]$, that do not depend on $\mathfrak{q}$, is nothing but obvious [Gek91, Corollary 3.4]. Our work (Theorem 4.2.7) constitutes another proof of that fact, which is true for all base field K, function ring A, endomorphism u, and rank r.

Main results

We compute characteristic polynomials of endomorphisms for any endomorphism u, function ring A, rank r and ground field K. When A is $\mathbb{F}_q[T]$, we provide the following complexity analyses. Let $\boldsymbol{\Omega}$ be a feasible exponent for characteristic polynomial computation over a commutative ring, as in § 1.3.3. Let $\mathrm{SM}^{\geqslant 1}$ be as in § 1.3.4.

Theorem A (see Theorems 4.3.11 and 4.3.13; see also Theorem A of [CL23])**.** Let ϕ be a rank r Drinfeld $\mathbb{F}_q[T]$-module over K, and let u be an endomorphism of ϕ of τ-degree n. The characteristic polynomial of u can be deterministically computed for a cost of $O^{\sim}(n^2 + (n+r)r^{\boldsymbol{\Omega}-1})$ operations in K and $O(n^2 + r^2)$ applications of the Frobenius endomorphism of K.

Moreover, when K is a finite extension of $\mathbb{F}_q$ of degree d, the characteristic polynomial of u can be computed for an expected cost of

$$O^{\sim}(d\log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n,d) + ndr + (n+d)r^{\omega}\right)\log q\right)$$

bit operations, using a Las Vegas algorithm.

For the special case of the Frobenius endomorphism, we provide three optimized variants: `F-MFF` (*Frobenius Motive Finite Field*), `F-MKU` (*Frobenius Motive Kedlaya-Umans*) and `F-CSA` (*Frobenius Motive Central Simple Algebra*) respectively.

Theorem B (Theorem B of [CL23])**.** Assume K is a finite extension of $\mathbb{F}_q$ of degree d. Let ϕ be a rank r Drinfeld $\mathbb{F}_q[T]$-module of rank r over K. The characteristic polynomial of the Frobenius endomorphism of ϕ can be computed using one of the three following Las Vegas algorithms, for an expected cost in bit operations of:

— [`F-MFF`, see § 4.3.2.2] $O^{\sim}(d\log^2 q) + O^{\bullet}\left(O^{\sim}(d\log^2 q)(\mathrm{SM}^{\geqslant 1}(d,d) + d^2r + dr^{\omega})\log q\right)$, or

— [`F-MKU`, see § 4.3.2.3] $O^{\sim}(d\log^2 q) + O^{\bullet}\left((d^2r^{\omega-1} + dr^{\omega})\log q\right)$, or

— [`F-CSA`, see § 6.3.1] $O^{\sim}(d\log^2 q) + O^{\bullet}(rd^{\omega}\log q)$.

All these variants—except for `F-CSA`, which is presented in Chapter 6—are based on a correspondence between Drinfeld modules and Anderson motives (§ 2.1.1.4). The purpose of this chapter is to introduce these *motivic methods*, while Chapter 6 covers the description of the `F-CSA` algorithm. To our knowledge, the present work is the first to address the case of general function rings. When A is $\mathbb{F}_q[T]$, one may also use the algorithms of [MS23], which work for any endomorphism, rank, and base field. All algorithms of [MS23] and Chapter 4 are implemented in the SageMath implementation of Drinfeld modules (Chapter 3). Our comparison (§ 6.4) suggests that all these methods complete each other: in both practice and theory, each one of them performs as the best in at least one range of parameters.

Strategy

The definition of $\chi(u)$ as the characteristic polynomial of $\mathbb{T}_{\mathfrak{q}}(u)$ closely follows elliptic curves, but suffers one major drawback: it requires computing torsion elements, in possibly large extensions of K. But for Drinfeld modules, a better characterization is possible. In § 2.1.1, we have defined another linear object attached to ϕ: its *Anderson motive* $\mathbb{M}(\phi)$. It is defined as the $K\{\tau\} \otimes A$-module given by

$$\begin{array}{rcl} (K\{\tau\} \otimes A) \times K\{\tau\} & \to & K\{\tau\} \\ (\sum g_i \otimes a_i, f) & \mapsto & \sum g_i f \phi_{a_i}. \end{array}$$

Per Theorem 2.1.11, when A equals $\mathbb{F}_q[T]$, the Anderson motive is free with with rank r, with a basis given by

$$(1, \tau, \dots, \tau^{r-1}).$$

Coordinates of elements and matrices of endomorphisms can easily be computed using Euclidean Ore division (Algorithms 3 and 5), and most importantly, $\mathbb{M}$ is functorial: the endomorphism u of ϕ yields an endomorphism $\mathbb{M}(u)$ of $\mathbb{M}(\phi)$ defined by

$$\begin{array}{rccc} \mathbb{M}(u): & \mathbb{M}(\psi) & \to & \mathbb{M}(\phi) \\ & f & \mapsto & fu. \end{array}$$

The endomorphism $\mathbb{M}(u)$ can thus be represented by an r-by-r matrix with coefficients in $\mathbb{F}_q[T]$. Its characteristic polynomial is thus a monic degree r polynomial in $\mathbb{F}_q[T][X]$, which we prove in Theorem 4.2.7 to be equal to $\chi(u)$. The complexities announced earlier are obtained by computing $\chi(u)$ as the characteristic polynomial of $\mathbb{M}(u)$. In the general case, *i.e.* when A is not restricted to $\mathbb{F}_q[T]$, the Anderson motive is not free, but projective. Characteristic polynomials can still be defined in this context, and Theorem 4.2.7 holds.

The key idea to prove that $\chi(u)$ is the characteristic polynomial of $\mathbb{M}(u)$ is to use the duality between Ore polynomials of $K\{\tau\}$ and finite sub-$\mathbb{F}_q$-vector spaces of $\overline{K}$. The kernel of an Ore polynomial f is a finite sub-$\mathbb{F}_q$-vector space of $\overline{K}$, and any such space defines a unique monic separable Ore polynomial. The difference is that the Ore polynomial is encoded by information in K, while its kernel lives in an extension of K. In fact, when f is separable, the spaces $\mathrm{Ker}(f)$ and $K\{\tau\}/K\{\tau\}f$ can be seen as dual spaces of each other (after a scalar extension to $\overline{K}$) through the bilinear mapping

$$\begin{array}{rcl} \mathrm{Ker}(f) \times \left(K\{\tau\}/K\{\tau\}f\right) & \to & \overline{K} \\ (z, \overline{g}) & \mapsto & g(z). \end{array}$$

Our idea is to replace f by ϕ_a, $\overline{K}$ by $\mathbb{E}(\phi)$, and $K\{\tau\}$ by $\mathbb{M}(\phi)$. This strategy establishes a duality between the Tate module and the Anderson motive (§ 4.2.2), and is is in fact reminiscent of a common philosophy

in the theory of Drinfeld modules: Anderson motives (even though their category is larger) are the duals of Drinfeld modules, and encode all their linear properties. As of now, this approach cannot be applied to elliptic curves and abelian varieties.

4.2 Theoretical preliminaries

The goal of this section is to prove Theorem 4.2.7, which states that the characteristic polynomial (resp. the norm) of an endomorphism is the characteristic polynomial (resp. the determinant) of its action on the Anderson motive.

Let us first fix notations. We let $\mathbb{F}_q$, A, γ and K be as in § 2.2 and recall that unless specified otherwise, tensor products are taken over $\mathbb{F}_q$. If F is any extension of $\mathbb{F}_q$, we let A_F denote the scalar extension $F \otimes A$. Thanks to our assumptions on the curve C associated to A (introduction to § 2.2), A_F is a Dedekind domain. The *degree* of any ideal $\mathfrak{a}_F$ of A_F is the F-dimension of $A_F/\mathfrak{a}_F$. In most cases, we consider A_K and $A_{\overline{K}}$. It is convenient to write $\deg(a_F)$ for $\deg(\mathfrak{a}_F)$, when $a_F \in A_F$ is a generator of $\mathfrak{a}_F$. If $\mathfrak{q}$ is a prime ideal of A, the completion of A with respect to the $\mathfrak{q}$-adic valuation is denoted $A_\mathfrak{q}$; it is defined as the projective limit

$$A_\mathfrak{q} = \varprojlim A/\mathfrak{q}^n.$$

We fix ϕ and ψ, rank r Drinfeld A-modules over K. In what follows, u either refers to a morphism from ϕ to ψ or to an endomorphism of ϕ. We define

$$\mathbb{M}_\mathfrak{a}(\phi) = \mathbb{M}(\phi)/\mathfrak{a}\mathbb{M}(\phi).$$

As a set, we have $\mathbb{M}_\mathfrak{a}(\phi) = K\{\tau\}/K\{\tau\}\phi_a$. We then extend scalars to $\overline{K}$ on both $\mathbb{E}_\mathfrak{a}(\phi)$ and $\mathbb{M}_\mathfrak{a}(\phi)$, to define

$$\begin{cases} \overline{\mathbb{E}_\mathfrak{a}}(\phi) = \overline{K} \otimes_{\overline{K}} \mathbb{E}_\mathfrak{a}(\phi), \\ \overline{\mathbb{M}_\mathfrak{a}}(\phi) = \overline{K} \otimes \mathbb{M}_\mathfrak{a}(\phi). \end{cases}$$

These objects are equipped with endomorphisms $\mathbb{E}_\mathfrak{a}(u)$ and $\mathbb{M}_\mathfrak{a}(u)$. When $\mathfrak{a}$ is principal, generated by an element $a \in A$, we simply write $\mathbb{M}_a(\phi)$, etc. Finally, if R is a ring and, M_1 and M_2 are R-modules, we let $\mathrm{Hom}_R(M_1, M_2)$ denote the R-module of R-linear maps from M_1 to M_2.

4.2.1 Defining determinants and characteristic polynomials

Recall that as A is a projective module, so is A_K. Let M be a finitely generated projective A_K-module of projective rank r. As in [Lano2, § XIX.1], we let

$$\det M = \bigwedge^r M$$

denote the maximal exterior power of M. Any A_K-linear endomorphism

$$f : M \to M$$

induces a linear map

$$\begin{array}{rccc} \det f : & \det M & \to & \det M \\ & (x_1 \wedge \cdots \wedge x_r) & \mapsto & (f(x_1) \wedge \cdots \wedge f(x_r). \end{array}$$

The latter is the multiplication by some element of A_K, that we call the *determinant* of f and denote by $\det f$ in a slight abuse of notation. Similarly, we define the characteristic polynomial of f as the determinant of the $A_K[X]$-linear map $X-f$ acting on $A_K[X] \otimes_{A_K} M$.

4.2.2 Duality between torsion points and A-motives

Consider the map

$$\begin{aligned} \mathcal{B}(\phi): \quad \mathbb{E}(\phi) \times \mathbb{M}(\phi) &\to \overline{K} \\ (z, f) &\mapsto f(z). \end{aligned}$$

It is $\mathbb{F}_q$-linear with respect to the variable z and $\overline{K}$-linear with respect to the variable f. Let now $\mathfrak{a}$ be a nonzero ideal of A. If $\mathbb{E}(\phi)$ is restricted to the $\mathfrak{a}$-torsion $\mathbb{E}_\mathfrak{a}(\phi)$, then after a scalar extension to $\overline{K}$, $\mathcal{B}$ factorizes as

$$\overline{\mathcal{B}_\mathfrak{a}}(\phi): \quad \overline{\mathbb{E}_\mathfrak{a}}(\phi) \times \overline{\mathbb{M}_\mathfrak{a}}(\phi) \to \overline{K}.$$

Remark 4.2.1. The notations differ from [CL23]. In the original paper, $\overline{\mathbb{E}_\mathfrak{a}}(\phi)$ is rather denoted by $\mathbb{E}_\mathfrak{a}(\phi)_{\overline{K}}$, and $\overline{\mathbb{M}_\mathfrak{a}}(\phi)$ is rather denoted by $\mathbb{M}_\mathfrak{a}(\phi)_{\overline{K}}$. Accordingly, $\overline{\mathcal{B}_\mathfrak{a}}(\phi)$ was originally denoted by $\mathcal{B}_\mathfrak{a}(\phi)_{\overline{K}}$.

The goal of this section is to establish—through $\overline{\mathcal{B}_\mathfrak{a}}(\phi)$—a dual equivalence between $\overline{\mathbb{E}_\mathfrak{a}}(\phi)$ and $\overline{\mathbb{M}_\mathfrak{a}}(\phi)$ (Theorem 4.2.5). To do that, we first prove that $\overline{\mathcal{B}_\mathfrak{a}}(\phi)$ is a perfect pairing:

Proposition 4.2.2 (Proposition 2.1 of [CL23])**.** *The $\overline{K}$-bilinear form $\overline{\mathcal{B}_\mathfrak{a}}(\phi)$ is a perfect pairing.*

Proof. Recall that, since $\mathfrak{a}$ is away from the characteristic, $\mathbb{E}_\mathfrak{a}(\phi)$ is free with rank r over $A/\mathfrak{a}$. Therefore, $\dim_{\mathbb{F}_q} \mathbb{E}_\mathfrak{a}(\phi) = r \cdot \deg(\mathfrak{a}) = \dim_K \mathbb{M}_\mathfrak{a}(\phi)$, and we find that $\mathbb{E}_\mathfrak{a}(\phi)_{\overline{K}}$ and $\mathbb{M}_\mathfrak{a}(\phi)_{\overline{K}}$ have the same dimension over $\overline{K}$. It is then enough to prove that $\mathcal{B}_{\mathfrak{a},\overline{K}}$ is nondegenerate on the left, meaning that if $x \in \mathbb{E}_\mathfrak{a}(\phi)_{\overline{K}}$ satisfies $\mathcal{B}_{\mathfrak{a},\overline{K}}(x, y) = 0$ for all $y \in \mathbb{M}_\mathfrak{a}(\phi)_{\overline{K}}$, then x must vanish. More generally, we are going to prove that there is no nonzero $x \in \mathbb{E}_\mathfrak{a}(\phi)_{\overline{K}}$ having the following property: $\mathcal{B}_{\mathfrak{a},\overline{K}}(x, 1 \otimes \tau^j) = 0$ for all j large enough. We argue by contradiction and consider an element $x \in \mathbb{E}_\mathfrak{a}(\phi)_{\overline{K}}$ satisfying the above property. We write

$$x = \lambda_1 \otimes z_1 + \cdots + \lambda_n \otimes z_n.$$

with $\lambda_i \in \overline{K}$ and $z_i \in \mathbb{E}_\mathfrak{a}(\phi)$. Moreover, we assume that x is chosen in such a way that the number of terms n is minimal. This ensures in particular that the z_i's are linearly independent over $\mathbb{F}_q$. Writing that $\mathcal{B}_{\mathfrak{a},\overline{K}}(x, 1 \otimes \tau^j)$ vanishes, we obtain the relation

$$(E_j): \quad \lambda_1 z_1^{q^j} + \cdots + \lambda_n z_n^{q^j} = 0,$$

which, in turn, implies

$$(E'_j): \quad \lambda_1^q z_1^{q^{j+1}} + \cdots + \lambda_n^q z_n^{q^{j+1}} = 0.$$

Combining the relations (E_{j+1}) and (E'_j), we find

$$(\lambda_1^q - \lambda_n^{q-1}\lambda_1) \cdot z_1^{q^{j+1}} + \cdots + (\lambda_{n-1}^q - \lambda_n^{q-1}\lambda_{n-1}) \cdot z_{n-1}^{q^{j+1}} = 0.$$

In other words, the vector

$$y = (\lambda_1^q - \lambda_n^{q-1}\lambda_1) \otimes z_1^{q^{j+1}} + \cdots + (\lambda_{n-1}^q - \lambda_n^{q-1}\lambda_{n-1}) \otimes z_{n-1}^{q^{j+1}} \in \overline{\mathbb{E}_\mathfrak{a}}(\phi)$$

is a new solution to our problem.

This will contradict the minimality condition in the choice of x if we can prove that y does not vanish. To do this, we again argue by contradiction. Given that the z_i's are linearly independent over $\mathbb{F}_q$, the vanishing of y would imply $\lambda_i^q - \lambda_n^{q-1}\lambda_i = 0$ for all i, from which we would deduce that all the quotients $\frac{\lambda_i}{\lambda_n}$ lie in $\mathbb{F}_q$. Thanks to the relations (E_j), this again contradicts the linear independence of the z_i's over $\mathbb{F}_q$. □

Remark 4.2.3. Proposition 4.2.2 can be seen as a Drinfeld analogue of the classical pairing between the singular homology and the de Rham cohomology of a complex abelian variety: the space $\mathbb{E}_{\mathfrak{a}}(\phi)$ plays the role of the singular homology (*via* the étale viewpoint), while the space $\mathbb{M}_{\mathfrak{a}}(\phi)$ can be thought of as the incarnation of the de Rham cohomology (see [Ang94]).

4.2.3 Dual spaces

Proposition 4.2.2 gives a natural identification

$$\alpha_\phi : \quad \overline{\mathbb{E}_{\mathfrak{a}}}(\phi) \simeq \mathrm{Hom}_{\overline{K}}\left(\overline{\mathbb{M}_{\mathfrak{a}}}(\phi), \overline{K}\right) \simeq \mathrm{Hom}_K\left(\mathbb{M}_{\mathfrak{a}}(\phi), \overline{K}\right),$$

where $\mathrm{Hom}_{\overline{K}}$ (resp. Hom_K) refers to the space of $\overline{K}$-linear (resp. K-linear) morphisms. *A priori*, the isomorphism α_ϕ—which is provided by standard linear algebra results—is only $\overline{K}$-linear; we upgrade it and make it $A_{\overline{K}}$-linear.

If M is a module over A_K. We set

$$M^* = \mathrm{Hom}_K(M, K)$$

and equip M^* with the structure of A_K-module given by

$$\begin{array}{rcl} A_K \times M^* & \to & M^* \\ (a, \xi) & \mapsto & m \mapsto \xi(am). \end{array}$$

One checks that the construction $M \mapsto M^*$ is functorial, in the sense that if $g : M_1 \to M_2$ is a morphism of A_K-modules, then the dual map $g^* : M_2^* \to M_1^*$ is A_K-linear as well. We define

$$\overline{\mathbb{M}_{\mathfrak{a}}^*}(\phi) = \overline{K} \otimes_K \mathbb{M}_{\mathfrak{a}}(\phi)^*.$$

A direct adaptation of [Pap23, Lemma 3.6.2] using Noether's structure theorem for finitely generated modules over a Dedekind domain [Eis95, Theorem A3.2] gives the following lemma.

Lemma 4.2.4 (Lemma 2.4 of [CL23])**.** *Any torsion finitely generated A_K-module M is (noncanonically) isomorphic to its dual M^*.*

4.2.4 Correspondence

We may now state and prove Theorem 4.2.5:

Theorem 4.2.5 (Theorem 2.5 of [CL23]). *The perfect pairing $\overline{\mathcal{B}_{\mathfrak{a}}}(\phi)$ induces an $A_{\overline{K}}$-linear isomorphism:*

$$\alpha_\phi : \quad \overline{\mathbb{E}_{\mathfrak{a}}}(\phi) \quad \xrightarrow{\sim} \quad \overline{\mathbb{M}^*_{\mathfrak{a}}}(\phi).$$

Moreover, given a Drinfeld module morphism $u : \phi \to \psi$, the following diagram is commutative:

$$\begin{array}{ccc} \overline{\mathbb{E}_{\mathfrak{a}}}(\phi) & \xrightarrow{\mathrm{Id}\otimes\mathbb{E}_{\mathfrak{a}}(u)} & \overline{\mathbb{E}_{\mathfrak{a}}}(\psi) \\ \downarrow{\scriptstyle \alpha_\phi} & & \downarrow{\scriptstyle \alpha_\psi} \\ \overline{\mathbb{M}^*_{\mathfrak{a}}}(\phi) & \xrightarrow[\mathrm{Id}\otimes\mathbb{M}_{\mathfrak{a}}(u)^*]{} & \overline{\mathbb{M}^*_{\mathfrak{a}}}(\psi) \end{array}$$

Proof. For the first assertion, we already know that α_ϕ is a $\overline{K}$-linear isomorphism. It then only remains to verify that it is A-linear. Let $a \in A$ and $z \in \mathbb{E}_{\mathfrak{a}}(\phi)$. By definitions 2.1.8 and 2.1.9, we have $a{\cdot}z = \phi_a(z)$ and $a{\cdot}f = f\phi_a$, for $f \in \mathbb{M}(\phi)$. Hence $\alpha_\phi(a{\cdot}z)$ is the function $f \mapsto f\left(\phi_a(z)\right) = (f\phi_a)(z) = (a{\cdot}f)(z)$, which means that $\alpha_\phi(a{\cdot}z) = a{\cdot}\alpha_\phi(z)$ as desired. The second assertion is easily checked. □

Remark 4.2.6. Theorem 4.2.5 shows that $\overline{\mathbb{E}_{\mathfrak{a}}}(\phi)$ determines $\overline{\mathbb{M}_{\mathfrak{a}}}(\phi)$ and *vice versa*. There are multiple ways to state a correspondence between $\mathbb{E}_{\mathfrak{a}}(\phi)$ and $\mathbb{M}_{\mathfrak{a}}(\phi)$.

(i) One can actually do much better and obtain a direct correspondence between $\mathbb{E}_{\mathfrak{a}}(\phi)$ and $\mathbb{M}_{\mathfrak{a}}(\phi)$ without extending scalars to $\overline{K}$ (see, for instance, [Pap23, Equation (3.6.9)]). For this, we need to add more structures. On the one hand, on $\mathbb{M}_{\mathfrak{a}}(\phi)$, we retain the τ-action as defined in Definition 2.1.9. On the other hand, on $\mathbb{E}_{\mathfrak{a}}(\phi)$, we have a Galois action. Precisely let K^{sep} denote the separable closure of K inside $\overline{K}$. From the fact that $\mathfrak{a}$ is away from the characteristic, we deduce that $\mathbb{E}_{\mathfrak{a}}(\phi)$ lies in K^{sep}, and endow with an action of the Galois group $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. We now have the following identifications, refining these of Theorem 4.2.5:

$$\begin{aligned} \mathbb{E}_{\mathfrak{a}}(\phi) &\simeq \mathrm{Hom}_{K\{\tau\}}\left(\mathbb{M}_{\mathfrak{a}}(\phi), K^{\mathrm{sep}}\right) \\ \mathbb{M}_{\mathfrak{a}}(\phi) &\simeq \mathrm{Hom}_{\mathbb{F}_q[G_K]}\left(\mathbb{E}_{\mathfrak{a}}(\phi), K^{\mathrm{sep}}\right) \end{aligned}$$

where, in the first (resp. second) line, we consider K-linear morphisms commuting with the τ-action (resp. $\mathbb{F}_q$-linear morphisms commutating with the Galois action). In other words, the Galois representation $\mathbb{E}_{\mathfrak{a}}(\phi)$ and the τ-module $\mathbb{M}_{\mathfrak{a}}(\phi)$ correspond one to the other under Katz' anti-equivalence of categories [Kat73, Proposition 4.1.1].

(ii) Another possibility is to follow [Hei04]. There is a canonical A-linear isomorphism:

$$\mathbb{E}_{\mathfrak{a}}(\phi) \simeq \mathrm{Hom}_{A/\mathfrak{a}}\left(\mathbb{M}_{\mathfrak{a}}(\phi)^\tau, \Omega_A/\mathfrak{a}\Omega_A\right)$$

where $\mathbb{M}_{\mathfrak{a}}(\phi)^\tau$ denotes the subset of fixed points of $\mathbb{M}_{\mathfrak{a}}(\phi)$ by the τ-action and Ω_A is the module of Kähler differential forms of A over $\mathbb{F}_q$ (see Proposition 4.3 of *loc. cit.*). However, the formulation of Theorem 4.2.5 is better suited for the applications we shall develop in this chapter.

A classical consequence of Theorem 4.2.5 is the following.

Theorem 4.2.7 (Theorem 2.8 of [CL23]). *Let ϕ be a Drinfeld A-module over K, and let $u : \phi \to \phi$ be an endomorphism. Let $\mathfrak{q}$ be a maximal ideal of A away from the characteristic. Then, $\mathbb{T}_{\mathfrak{q}}(u)$ and $\mathbb{M}(u)$ are have same characteristic polynomials. In particular, $\mathfrak{n}(u)$ is the principal ideal generated by* $\det(\mathbb{M}(u))$.

Proof. Let $n \in \mathbb{Z}_{\geqslant 0}$. Applying Theorem 4.2.5 with $\mathfrak{a} = \mathfrak{q}^n$, we find

$$\chi\left(\mathbb{E}_{\mathfrak{q}^n}(u)\right) = \chi\left(\overline{\mathbb{E}_{\mathfrak{q}^n}(u)}\right) = \chi\left(\overline{\mathbb{M}_{\mathfrak{q}^n}(u)}\right) = \chi\left(\mathbb{M}_{\mathfrak{q}^n}(u)\right),$$

the second equality being a consequence of Theorem 4.2.5 and the fact that two dual morphisms have the same determinant (in suitable bases, their matrices are transposed one to the other). Thus we obtain $\chi(\mathbb{T}_{\mathfrak{q}}(u)) \equiv \chi(\mathbb{M}(u)) \pmod{\mathfrak{q}^n}$. Since this holds for all positive integer n, we conclude that $\chi(\mathbb{T}_{\mathfrak{q}}(u)) = \chi(\mathbb{M}(u))$. The last statement now follows from [Gek91, Lemma 3.10]. □

Remark 4.2.8. Our approach is reminiscent of a standard principle in the theory of Drinfeld modules, which states that Anderson motives and Drinfeld modules (or more generally, *abelian A-modules*; see for instance [Gos96, § 5.4, § 5.6] or [Pap23, § 3.6]) are dual objects. Theorem 4.2.5 is a concrete incarnation of this yoga, establishing a duality between the functors $\mathbb{E}_{\mathfrak{a}}$ and $\mathbb{M}_{\mathfrak{a}}$. Our presentation is rather elementary, and does not need the introduction of so-called abelian A-modules. As such, we include all proofs, hoping they will be of interest for some readers.

4.3 Algorithms

We now turn to algorithms to compute $\chi(u)$, the characteristic polynomial of u. We first assume that A is $\mathbb{F}_q[T]$. The main algorithm—Algorithm 6—is a direct consequence of Theorem 4.2.7. We provide thorough complexity analyses, and give optimizations when K is a finite field (§ 4.3.2.2) or when u is the Frobenius endomorphism (§ 4.3.2.3). When A is not assumed to be $\mathbb{F}_q[T]$, we describe an algorithm without giving a complexity analysis (§ 4.3.3).

4.3.1 Further algorithm prerequisites

First, it is necessary to build on § 1.3 and to introduce new algorithmic primitives.

4.3.1.1 Further algorithms for polynomial matrices

When M is a square matrix, we let $\chi(M)$ denote its characteristic polynomial. In this chapter, we compute characteristic polynomials of Drinfeld module endomorphisms as classical characteristic polynomials of polynomial matrices. Those matrices turn out to verify strict and known degree bounds (Lemma 4.3.6). With this insight, we provide the two following lemmas. The first is used to compute norms and characteristic polynomials using motivic techniques (Theorems 4.3.13, 4.3.16, and 5.3.1); the second is used to compute the characteristic polynomial of the Frobenius endomorphism using simple central algebras (Chapter 6).

Lemma 4.3.1 (Lemma 1.14 of [CL23])**.** *Assume that K is a finite extension of $\mathbb{F}_q$ of degree d, and let M be a polynomial matrix with size s and coefficients in $K[T]$. Let n be a uniform upper bound on the degree of the coefficients of $\chi(M)$. There exists a Las Vegas algorithm that computes $\chi(M)$ for an expected cost of $O^{\bullet}(n/d) + O^{\sim}((n+d)s^{\omega})$ operations in $\mathbb{F}_q$.*

Proof. Let K' be an extension of K of degree $\lceil n/d \rceil$. Such an extension, altogether with a generator α of K' over $\mathbb{F}_q$, can be found out using Couveignes and Lercier's Las Vegas algorithm for an expected cost of $O^{\bullet}(\frac{n}{d})$ operations in $\mathbb{F}_q$ [CL13]. The degree of the extension $K'/\mathbb{F}_q$ is then in the range $[n, n+d]$. Let

$M(\alpha)$ denote the matrix obtained from M by evaluating its coefficients at α, and write its characteristic polynomial—in $\mathbb{F}_q[T]$—as follows:

$$\chi(M(\alpha)) = \sum_{i=0}^{s} \sum_{j=0}^{n} a_{i,j} \alpha^i X^i,$$

the coefficients $a_{i,j}$ being in $\mathbb{F}_q$. Then

$$\chi(M) = \sum_{i=0}^{s} \sum_{j=0}^{n} a_{i,j} T^i X^i.$$

The generator α being known, computing $\chi(M(\alpha))$ costs $O^{\sim}(s^\omega)$ operations in K', which corresponds to $O^{\sim}((n+d)s^\omega)$ operations in $\mathbb{F}_q$. □

Lemma 4.3.2 (Lemma 1.15 of [CL23]). *Let M be a polynomial matrix with size s and coefficients in $\mathbb{F}_q[T]$. Let n be a a uniform upper bound on the degrees of the coefficients of M, and assume that the coefficients of $\chi(M)$ are in $\mathbb{F}_q[T^s]$. There exists a Las Vegas algorithm that computes $\chi(M)$ with probability of success at least $1/2$ for an expected cost of $O^{\sim}(ns^\omega)$ operations in $\mathbb{F}_q$.*

Proof. Assume for now that $\mathbb{F}_q$ is large enough for an integer n and distinct elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ such that $\alpha_i^s \neq \alpha_j^s$ whenever $i \neq j$ to exist. We compute the matrices $M(\alpha_1), \dots, M(\alpha_n)$ and their characteristic polynomials $\chi(M(\alpha_1)), \dots, \chi(M(\alpha_n))$ for a total cost of $O^{\sim}(ns^\omega)$ operations in $\mathbb{F}_q$. Thanks to our assumption, $\chi(M)$ can be seen as having s polynomial coefficients of degree at most n in T^s. Using fast interpolation algorithms [GG13, §II.10], $\chi(M)$ can be recovered from the $\chi(M(\alpha_i))$'s for a cost of $O^{\sim}(ns)$ operations in $\mathbb{F}_q$. We end up with a total cost of $O^{\sim}(ns^\omega)$ operations in $\mathbb{F}_q$.

Note that this procedure only works if $\mathbb{F}_q$ is large enough to pick elements $\alpha_1, \dots, \alpha_n$ as above. Let $\rho = \gcd(q-1, s)/(q-1)$ be the proportion of elements in ${\mathbb{F}_q}^\times$ that are d-th roots of unity. A family $(\alpha_1, \dots, \alpha_n) \in ({\mathbb{F}_q}^\times)^n$ has probability $p_n = (1-\rho)(1-2\rho)\cdots(1-n\rho)$ to suit our needs. As p_n is greater than $1 - (n(n+1)\rho)/2$, $\mathbb{F}_q$ is large enough with a chance of success greater than $1/2$ as soon as $q > 1 + sn(n+1)$. If that is not the case, we do all computations in a finite extension of $\mathbb{F}_q$. With these estimations, we conclude that it is enough to work in an extension whose degree has order of magnitude $\log_q(sn^2)$. Construction of and computations in this extension do not affect the announced complexity. □

4.3.1.2 Further algorithms for Ore polynomials

We follow up on § 1.3.4 and explicitly write variations of Euclid's algorithm for Ore polynomials, as well as complexity analyses. With Algorithm 1, one computes Ore right-Euclidean divisions.

Lemma 4.3.3 (Lemma 3.4 of [LS24]). *Assuming $\deg(f) > \deg(g)$, Algorithm 1 computes (deterministic procedure) the Euclidean division of f by g for a cost of $O(\deg(g)(\deg(f) - \deg(g)))$ operations in K and as many applications of the Frobenius endomorphism.*

Proof. The proof of the correction of Algorithm 1 follows its classical analogue. For the complexity, notice that in the worst-case scenario, the algorithm computes $\tau^{\deg(\beta)-\deg(g)} \cdot 1/c_\beta$ and $\tau^{\deg(\beta)-\deg(g)} \cdot 1/c_\beta \cdot b$ with $\deg(\beta)$ ranging from $\deg(g)$ to $\deg(f)$. This can be computed for a cost of $O(\deg(g)(\deg(f) - \deg(g)))$ operations in K and as many applications of the Frobenius endomorphism. Then, at each step of the loop, computing ε and $\alpha + \varepsilon$ costs a constant number of operations, and computing β costs $O(\deg(g))$ operations, hence the conclusion. □

Algorithm 1. OreEuclideanDivision (Algorithm 2 of [LS24])

Input: Two Ore polynomials $f, g \in K\{\tau\}$.
Output: Ore polynomials $\alpha, \beta \in K\{\tau\}$ such that $f = \alpha g + \beta$ and $\deg(\beta) < \deg(g)$.

Set $\alpha = 0$ and $\beta = f$;
while $\deg(g) \leqslant \deg(\beta)$ do
  Let c_g and c_β be the leading coefficients of g and β ;
  Set $\varepsilon = c_\beta \cdot \tau^{\deg(\beta)-\deg(g)} \cdot 1/c_g$;
  Set $\alpha = \alpha + \varepsilon$;
  Set $\beta = \beta - \varepsilon \cdot g$;
end
return (α, β).

Algorithm 1 naturally leads to a primitive to compute Ore right-greatest common divisors (rgcd'):

Algorithm 2. OreEuclidRgcd (Algorithm 3 of [LS24])

Input: Two Ore polynomials $f, g \in K\{\tau\}$ such that $g \neq 0$.
Output: The rgcd of f and g.

if $g = 0$ then
  return f.
end
if $\deg(g) > \deg(f)$ then
  return OreEuclidRgcd(g, f).
end
Compute (q, r) = OreEuclideanDivision(a, b);
return OreEuclidRgcd(r, b).

Lemma 4.3.4 (Lemma 3.6 of [LS24])**.** *Algorithm 2 computes (deterministic procedure) the rgcd of f and g for a cost of $O(\deg(f)\deg(g))$ operations in K and as many applications of the Frobenius endomorphism.*

Proof. As for Algorithm 1, the correction of Algorithm 2 is proved following the proof of the classical case. The same is true for the complexity: we follow [GG13, Theorem 3.11] with Lemma 4.3.3. □

4.3.1.3 Algorithms for the motivic canonical basis

Let K be an extension of $\mathbb{F}_q$, and let ϕ be a rank r Drinfeld $\mathbb{F}_q[T]$-module over K. We now enquire the computation of vectors and matrices in the canonical basis

$$(1, \tau, \dots, \tau^{r-1})$$

of $\mathbb{M}(\phi)$, as defined in Theorem 2.1.11.

We first design an algorithm to compute the coordinates $(f_0, \dots, f_{r-1})$ of an Ore polynomial f. This only involves Ore right-Euclidean divisions. Indeed, notice that if $f = a\phi_T + b$ is the Ore right-Euclidean division of f by ϕ_T, then the coordinates of f are that of b, plus "T times" that of a. This gives a recursive method:

Algorithm 3. MotiveCoordinates (Algorithm 1 of [CL23])

Input: An element $f \in \mathbb{M}(\phi)$
Output: The coordinates $(f_0, \dots, f_{r-1})$ of f

```
if deg f < r then
    return the vector defined by the coefficients of f ;
else
    Set m = max(1, ⌊deg_τ(f)/2r⌋) ;
    Write f = a · φ_T^m + b with deg(b) < rm (right Euclidean division);
    return T^m · MotiveCoordinates(a) + MotiveCoordinates(b) ;
end
```

Lemma 4.3.5 (Lemma 2.9 of [CL23]). *For an input $f \in \mathbb{M}(\phi)$ of τ-degree n, Algorithm 3 computes (deterministic procedure) the coordinates of f for a cost $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K.*

Proof. The first step of the algorithm consists in computing ϕ_T^m. Using fast exponentiation, this costs $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K. The Euclidean division requires $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K as well. Let $\mathrm{C}(s)$ be the cost of running the algorithm on an entry with degree s. By what precedes, $\mathrm{C}(s)$ is less than $\mathrm{C}(\lceil \frac{s}{2} \rceil)$, plus $O(s^2)$ operations in K and $O(s^2)$ applications of the Frobenius endomorphism. We conclude using the *Master Theorem* [Cor+22, Theorem 4.1]. □

An important consequence of Algorithm 3 is the following bounds on the degrees of the coefficients $(f_0, \dots, f_{r-1})$ of f.

Lemma 4.3.6 (Lemma 2.10 of [CL23]). *Let $f \in \mathbb{M}(\phi)$ have coordinates*

$$f = (f_0, \dots, f_{r-1})$$

with respect to the canonical basis $(1, \tau, \dots, \tau^{r-1})$. Seen as an Ore polynomial, f has τ-degree denoted by $\deg_\tau(f)$. Then, for every $0 \leqslant i < r$, either $\deg_\tau(f) < i$ and $f_i = 0$, or $\deg_\tau(f) \geqslant i$, in which case we have

$$\deg_T(f_i) \leqslant \frac{\deg_\tau(f) - i}{r}.$$

Proof. The is a consequence of Algorithm 3. □

Corollary 4.3.7 (Corollary 2.11 of [CL23]). *Let $(\mathbb{M}(u)_{i,j})_{0 \leqslant i,j < r}$ be the matrix of $\mathbb{M}(u)$ in the canonical bases. That is, $\mathbb{M}(u)_{i,j}$ is the coefficient on the i-th row and j-th column. Then, for every $0 \leqslant i, j \leqslant r-1$, either $\deg_\tau(u) + j < i$ and $\mathbb{M}(u)_{i,j} = 0$, or $\deg_\tau(u) + j \geqslant i$, in which case we have*

$$\deg(\mathbb{M}(u)_{i,j}) \leqslant \frac{(\deg(u) + j) - i}{r}.$$

Proof. By definition, $\mathbb{M}(u)_{i,j}$ is the coefficient in front of τ^i in the decomposition of $\tau^j u$ in the canonical basis. The corollary then follows from Lemma 4.3.6. □

Remark 4.3.8. As a byproduct of this corollary, we get a new—simpler—proof of Lemma 2.1.28. By Theorem 4.2.7, we know that $\chi(\pi)$ is the classical characteristic polynomial of the matrix of $\mathbb{M}(\tau^d)$. Therefore, for every $0 \leqslant i \leqslant r$, a_i is the trace of $\bigwedge^i \mathbb{M}(\tau^d)$, which is an alternated sum on the minors of the matrix of $\mathbb{M}(\tau^d)$ with size i. We conclude using Corollary 4.3.7.

One can then compute the matrix of an endomorphism by applying Algorithm 3 a total of r times. This is not the most efficient approach, as one can instead compute the coordinates of u (seen as an Ore polynomial), and "shift them" when they are right-multiplied by τ. To do that, let us write

$$\phi_T = g_0 + \cdots + g_r\tau^r,$$

with $g_r \neq 0$. Notice that the coordinates of τ^r are given by a closed and simple formula, depending only on T and the g_i's:

$$\tau^r = \left(\frac{T-g_0}{g_r}, -\frac{g_1}{g_r}, \cdots, -\frac{g_{r-1}}{g_r}\right),$$

More generally, if the coordinates $(f_0, \ldots, f_{r-1})$ of any f in $\mathbb{M}(\phi)$ are known, one obtains the coordinates of τf using a companion matrix. For any polynomial $f_i \in K[T]$, we let f_i^τ denote the polynomial in $K[T]$ deduced from f_i by raising all its coefficients to the q-th power. Then the coordinates of τf are given by the following matrix-vector product:

$$\begin{pmatrix} 0 & & & & \frac{T-g_0}{g_r} \\ 1 & 0 & & & -\frac{g_1}{g_r} \\ & 1 & \ddots & & \\ & & \ddots & 0 & \\ & & & 1 & -\frac{g_{r-1}}{g_r} \end{pmatrix} \cdot \begin{pmatrix} f_0^\tau \\ f_1^\tau \\ \vdots \\ \vdots \\ f_{r-1}^\tau \end{pmatrix}. \tag{4.1}$$

This gives Algorithm 4:

Algorithm 4. MotiveTauAction (Algorithm 2 of [CL23])

Input: The coordinates $(f_0, \ldots, f_{r-1})$ of an element $f \in \mathbb{M}(\phi)$
Output: The coordinates of $\tau f \in \mathbb{M}(\phi)$

Compute $f_0^\tau, \ldots, f_{r-1}^\tau$;
Compute $f_0' = \frac{T-g_0}{g_r} f_{r-1}^\tau$;
for $1 \leqslant i \leqslant r-1$ do
  Compute $f_i' = f_i^\tau - \frac{g_{i+1}}{g_r} f_{r-1}^\tau$;
end
return $(f_0', \ldots, f_{r-1}')$;

Lemma 4.3.9 (Lemma 2.13 of [CL23]). *For an input $f \in \mathbb{M}(\phi)$ of τ-degree n, Algorithm 4 computes (deterministic procedure) the coordinates of τf for a cost of $O(n)$ applications of the Frobenius endomorphism and $O(n)$ operations in K.*

Proof. By Lemma 4.3.6, the polynomial $f_i \in K[T]$ has degree at most $\frac{n-i}{r}$. As a consequence, computing f_i^τ requires at most $\left\lfloor \frac{n-i}{r} \right\rfloor + 1$ applications of the Frobenius endomorphism, and the pre-computation on line 1 costs

$$\sum_{i=0}^{r-1} \left(\left\lfloor \frac{n-i}{r} \right\rfloor + 1 \right) = n + 1$$

such applications. The remaining steps can be done in $O(n)$ arithmetic operations in K. □

We finally describe an algorithm to compute the matrix in $\mathbb{M}(\phi)$ of the endomorphism $\mathbb{M}(u)$. As mentioned, computing each column of the matrix with Algorithm 3 is doable but costly. Instead, we rely on Algorithm 4, which implements the companion matrix-vector product of Equation 4.1, to use Algorithm 3 for the sole computation of the first column. This way, only one Ore euclidean division is performed.

Algorithm 5. MotiveMatrix (Algorithm 3 of [CL23])

Input: An endomorphism $u : \phi \to \phi$ encoded by its defining Ore polynomial
Output: The matrix of $\mathbb{M}(u)$ with respect to the canonical bases
1 Compute $\mathbb{M}(u)_0$ = MotiveCoordinates(u, ϕ) ;
2 for $1 \leqslant i \leqslant r-1$ do
3 | Compute $\mathbb{M}(u)_i$ = MotiveTauAction$(\mathbb{M}(u)_{i-1})$;
4 end
5 return the matrix with columns $(\mathbb{M}(u)_0, \ldots, \mathbb{M}(u)_{r-1})$;

Lemma 4.3.10 (Lemma 2.14 of [CL23])**.** *For an input u of τ-degree n, Algorithm 5 computes (deterministic procedure) the matrix of $\mathbb{M}(u)$ for a cost of $O(n^2 + r^2)$ applications of the Frobenius endomorphism, and $O(n^2 + r^2)$ operations in K.*

Proof. Computing $\mathbb{M}(u)_0$ requires $O(n^2)$ applications of the Frobenius endomorphism and $O(n^2)$ operations in K (Lemma 4.3.5). Then, knowing $\mathbb{M}(u)_i$ for some $1 \leqslant i \leqslant r-1$, the computation of $\mathbb{M}(u)_{i+1}$ requires at most $O(n+i)$ applications of the Frobenius and $O(n+i)$ operations in K by Lemma 4.3.9. Summing all the contributions, we end up with the announced complexity. □

4.3.2 Algorithms for $A = \mathbb{F}_q[T]$

Having all the algorithmic primitives we need, we can now give the most important algorithm of the chapter (Algorithm 6) and its corollaries.

4.3.2.1 Algorithms for generic ground fields

We first begin by providing an algorithm that works or any ground field K. We recall from § 1.3.3 that Ω is a feasible exponent for characteristic polynomial computation.

Theorem 4.3.11 (Theorem 2.15 of [CL23])**.** *Recall ϕ is a Drinfeld $\mathbb{F}_q[T]$-module of rank r over K. Let u be an endomorphism of ϕ with τ-degree n. Using Algorithm 6, the characteristic polynomial of u can be computed (deterministic algorithm) for a cost of $O(n^2 + r^2)$ applications of the Frobenius and $O^{\sim}(n^2 + (n+r)r^{\Omega-1})$ operations in K.*

Algorithm 6. EndomorphismCharacteristicPolynomial (Algorithm 4 of [CL23])

Input: An endomorphism u of ϕ encoded by its defining Ore polynomial
Output: The characteristic polynomial of u
1 Compute $M = \text{MotiveMatrix}(u)$;
2 return the characteristic polynomial of M ;

Proof. The cost of computing the matrix of $\mathbb{M}(u)$ is $O(n^2 + r^2)$ applications of the Frobenius endomorphism, and $O(n^2 + r^2)$ operations in K. The matrix has size r and, thanks to Corollary 4.3.7, we know that all its entries have degree less than $1 + \frac{n}{r}$. Its characteristic polynomial can then be computed within $O^{\sim}((n+r)r^{\Omega-1})$ operations in K (see § 4.3.1.1). The theorem follows. □

Algorithm 6 is rather generic, and we now discuss several ways to optimize it.

4.3.2.2 Algorithms for finite ground fields

If K is a finite field, computations can be sped up using specific algorithmic primitives to compute characteristic polynomial of polynomial matrices (Lemma 4.3.1) on the one hand, and to compute Ore Euclidean divisions (§ 1.3.4) on the other hand. Both these families of primitives provide Las Vegas algorithms, which makes our algorithms Las Vegas as well. First, we speed up the matrix computation. Even though we—in this Section—only work with endomorphisms, the following lemma is valid for general isogenies, and will be reused in Chapter 5.

Lemma 4.3.12. *Recall ϕ is a Drinfeld $\mathbb{F}_q[T]$-module of rank r over K. Let u be an isogeny of ϕ with τ-degree n. Assume K is a finite extension of $\mathbb{F}_q$, with degree d over $\mathbb{F}_q$. Using Algorithm 5, and the primitives of § 1.3, the matrix of $\mathbb{M}(u)$ can be computed (Las Vegas procedure) for an expected cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + dr(n + r)\right) \log q\right)$$

bit operations.

Proof. The complexity analysis is similar to that of Theorem 4.3.11, except that the Ore Euclidean division of Algorithm 3 now costs $O^{\sim}(d \log^2 q) + O^{\bullet}(\mathrm{SM}^{\geqslant 1}(n, d) \log q)$ bit operations (see § 1.3.4). The announced complexity follows. □

We can now state and prove Theorem 4.3.13:

Theorem 4.3.13 (Theorem 2.16 of [CL23])**.** *Recall ϕ is a Drinfeld $\mathbb{F}_q[T]$-module of rank r over K. Let u be an endomorphism u of ϕ with τ-degree n. Assume K is a finite extension of $\mathbb{F}_q$, with degree d over $\mathbb{F}_q$. Using Algorithm 6, and Lemma 4.3.1, the characteristic polynomial of u can be computed (Las Vegas procedure) for an expected cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + ndr + nr^{\omega} + dr^{\omega}\right) \log q\right)$$

bit operations.

Proof. By lemma 4.3.12, the computation of the matrix of $\mathbb{M}(u)$ requires an initial computation costing $O^{\sim}(d \log^2 q)$ bit operations, followed by $O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + dr(n + r)\right) \log q\right)$ bit operations. Finally, it remains to compute the characteristic polynomial of the matrix. For this, we first notice that all its coefficients have degree at most n (Corollary 4.3.7). Therefore, using Lemma 4.3.1, the computation of the characteristic polynomial costs $O^{\bullet}((n+d)r^{\omega})$ operations in $\mathbb{F}_q$. The theorem follows. □

Remark 4.3.14. Comparing with the algorithms of [MS23], we find that Algorithm 6 exhibits a better theoretical complexity, except when the degree of $\gamma(T)$ is close to d and the rank r is very small compared to d and n; in this case, the algorithm of [MS23, Theorem 2(1)] has quadratic complexity in $\max(n, d)$, beating the term $\mathrm{SM}^{\geqslant 1}(n, d)$.

When u is the Frobenius endomorphism, Algorithm 6 leads to the algorithm `F-MFF` discussed in § 4.1, whose complexity is given by Corollary 4.3.15.

Corollary 4.3.15 (Variant `F-MFF`; see also Corollary 2.18 of [CL23])**.** *Recall ϕ is a Drinfeld $\mathbb{F}_q[T]$-module of rank r over K. Assume K is a finite extension of $\mathbb{F}_q$, with degree d over $\mathbb{F}_q$. Using Algorithm 6, and the primitives of § 1.3, the characteristic polynomial of the Frobenius endomorphism of ϕ can be computed (Las Vegas procedure) for an expected cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(d, d) + d^2 r + d r^{\omega}\right) \log q\right)$$

expected bit operations.

Proof. This is a direct application of Theorem 4.3.13 with $n = d$. □

4.3.2.3 Optimizations for the Frobenius endomorphism

Below, we present another method to compute the characteristic polynomial of the Frobenius endomorphism π. This leads to the algorithm `F-MKU`, as mentioned in § 4.1, which performs better for some ranges of parameters (at least theoretically). It is based on the two following remarks:

(i) As the Ore polynomial τ^d is central in $K\{\tau\}$, and its action on the motive can unambiguously be defined as a left or right multiplication.

(ii) The left multiplication by τ on $\mathbb{M}(\phi)$ is a semi-linear application, whose matrix is the companion matrix appearing in Equation (4.1), which is easy to compute.

More precisely, for a nonnegative integer s, let m_s be the $K[T]$-semi-linear endomorphism of $\mathbb{M}(\phi)$ defined by $f \mapsto \tau^s f$. We denote its matrix by M_s. In other words, M_s is the matrix whose j-th column contains the coefficients of $\tau^{j+s} \in \mathbb{M}(\phi)$ in the canonical basis. The matrix M_1 is the companion matrix of Equation (4.1) and, by definition, the matrix of $\mathbb{M}(\pi)$ is M_d.

For a polynomial $P \in \mathbb{F}_q[T]$, we let P^{τ^s} be the polynomial obtained by raising each coefficient of P to power q^s. Similarly, given a matrix M with entries in $\mathbb{F}_q[T]$, we write M^{τ^s} for the matrix obtained from M by applying $P \mapsto P^{\tau^s}$ to each of its entry. A calculation shows that

$$M_s = M_1 \cdot M_1^{\tau} \cdots M_1^{\tau^{s-1}}.$$

This equation leads to the following *square and multiply*-like formulas:

$$M_{2s} = M_s \cdot M_s^{\tau^s}, \tag{4.2}$$

$$M_{2s+1} = M_1 \cdot M_s^{\tau} \cdot M_s^{\tau^{s+1}}. \tag{4.3}$$

Let α be a generator of K over $\mathbb{F}_q$. Elements of K are classically represented as polynomials in α with coefficients in $\mathbb{F}_q$ and degree $d - 1$. Applying τ^s to an element $\sum_{i=0}^{r-1} a_i \alpha^i \in K$ amounts to applying the substitution $\alpha \mapsto \tau^s(\alpha)$. Thus, this can be efficiently computed using Kedlaya-Umans' algorithm for modular composition [KU11] for a cost of $O^{\bullet}(d \log q)$ bit operations. As mentioned in § 1.3.1, an initial precomputation of α^q must be performed once and for all, for a cost of $O^{\sim}(d \log^2 q)$ bit operations.

Theorem 4.3.16 (Variant F–MKU; Theorem 2.19 of [CL23]). *Recall ϕ is a Drinfeld $\mathbb{F}_q[T]$-module of rank r over K. Assume K is a finite extension of $\mathbb{F}_q$, with degree d over $\mathbb{F}_q$. Using Algorithm 6, and Kedlaya and Umans' algorithm, the characteristic polynomial of the Frobenius endomorphism of ϕ can be computed (Las Vegas procedure) for an expected cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left((d^2 r^{\omega-1} + dr^{\omega}) \log q\right)$$

expected bit operations.

Proof. Let $\mathrm{C}(s)$ be the cost, counted in bit operations, of computing the pair $\mathcal{P}_s = (M_s, \tau^s(\alpha))$. To compute $\mathcal{P}_{2s}$ and $\mathcal{P}_{2s+1}$, one uses the recurrence relations (4.2) and (4.3). As M_s has r^2 polynomial coefficients of degree at most s/r (Lemma 4.3.6), computing $\tau^s(M)$ requires $O(sr)$ modular compositions of degree d. As previously mentioned, we use Kedlaya-Umans' algorithm [KU11] for this task, leading to a total cost of $O^{\bullet}(nrd \cdot \log q)$ bit operations. Similarly $\tau^{2s}(\alpha)$ can be computed by composing $\tau^s(\alpha)$ with itself; using again Kedlaya-Umans' algorithm, this can be done within $O^{\bullet}(d \cdot \log q)$ bit operations. Moreover, the matrix product $M_s \cdot \tau^s(M)$ requires $O^{\sim}(dsr^{\omega-1})$ extra operations in $\mathbb{F}_q$. Given that one operation in $\mathbb{F}_q$ corresponds to $O^{\sim}(\log q) \subset O^{\bullet}(\log q)$ bit operations, we conclude that

$$\mathrm{C}(2s) \leqslant \mathrm{C}(s) + O^{\bullet}(dsr^{\omega-1} \log q).$$

A similar analysis provides a similar bound for $\mathrm{C}(2s+1)$. Solving the recurrence, we obtain $\mathrm{C}(s)$ to be in $O^{\bullet}(dsr^{\omega-1} \log q)$. Therefore, the computation of $\mathbb{M}(u)$ can be done within $O^{\bullet}(d^2 r^{\omega-1} \log q)$ bit operations.

Finally, the characteristic polynomial of the matrix of $\mathbb{M}(u)$ is computed, as previously, using Lemma 4.3.1, for a cost of $O^{\sim}(dr^{\omega})$ operations in $\mathbb{F}_q$, which is no more than $O^{\bullet}(dr^{\omega} \cdot \log q)$ bit operations. Adding both contributions and taking into account the precomputation of α^q, we obtain the corollary. □

4.3.3 Algorithms for generic A

We now drop the assumption that $A = \mathbb{F}_q[T]$. In full generality, it is not true that the motive $\mathbb{M}(\phi)$ is free over A_K, and the matrix of $\mathbb{M}(u)$ is not defined. One can nevertheless easily work around this difficulty, by extending scalars to the fraction field of A_K, denoted by $\mathrm{Frac}(A_K)$. Indeed, $\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$ is obviously free over $\mathrm{Frac}(A_K)$ given that the latter is a field. It is also clear that the determinants of $\mathbb{M}(u)$ and $\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(u)$ are equal.

Our first need is to design an algorithm for computing a basis of $\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$. For this, we will rely on the case of $\mathbb{F}_q[T]$, previously treated. We consider an element $T \in A$, $T \notin \mathbb{F}_q$. Since the underlying curve C is absolutely irreducible, T must be transcendental over $\mathbb{F}_q$. This gives an embedding $\mathbb{F}_q[T] \to A$, which extends to an inclusion of fields $K(T) \to \mathrm{Frac}(A_K)$. The resulting extension is finite of degree $t = \deg(T)$. Let $(b_1, \ldots, b_t)$ be a basis of $\mathrm{Frac}(A_K)$ over $K(T)$.

In what follows, T and $(b_1, \ldots, b_t)$ are assumed to be known. Finding them depends on the way C is given, but we believe that our hypothesis is reasonable. For instance, if C is presented as a plane smooth curve, *i.e.* if A is given as

$$A = \mathbb{F}_q[X, Y]/P(X, Y) \quad \text{with} \quad P \in \mathbb{F}_q[X, Y]$$

one may choose $T = X$, $t = \deg_Y P$ and $b_i = Y^{i-1}$ for $1 \leqslant j \leqslant t$.

Remark 4.3.17. Let g be the genus of C, the curve associated to A. The Riemann-Roch theorem indicates that the Riemann-Roch space $\mathcal{L}\left((g+1)\cdot[\infty]\right)$ has dimension at least 2. Hence it must contain a transcendental function, which shows that there always exists T for which $t \leqslant g+1$. In practice, T can be computed through various different algorithms (see [LS20; ACL22] and the references therein).

Now given a Drinfeld module $\phi : A \to K\{\tau\}$ over A, we restrict it to $\mathbb{F}_q[T]$ *via* the embedding $\mathbb{F}_q[T] \to A$, obtaining a second Drinfeld module $\phi' : \mathbb{F}_q[T] \to K\{\tau\}$ (see §2.2.1.3). Then, as $K[T]$-modules, one has $\mathbb{M}(\phi') = \mathbb{M}(\phi)$. Moreover, if ϕ has rank r, we have

$$\deg \phi'_T = \deg \phi_T = r \cdot \deg(T) = rt$$

showing that ϕ' has rank rt. The family $(1, \tau, \dots, \tau^{rt-1})$ is a basis of $\mathbb{M}(\phi)$ over $K[T]$, and we can use Algorithm 3 to compute the coordinates of any element of $\mathbb{M}(\phi)$ with respect to this basis. Let $\Gamma : \mathbb{M}(\phi) \to K[T]^{rt}$ be the map taking an element of $\mathbb{M}(\phi)$ to the column vector representing its coordinates in the above basis. Both Γ and Γ^{-1} are efficiently computable.

Let e_1 be an arbitrary nonzero element of $\mathbb{M}(\phi)$, *e.g.* $e_1 = 1$. A $K(T)$-basis of the $\mathrm{Frac}(A_K)$-line generated by e_1 is explicitly given by the family $e_1\phi_{b_1}, \dots, e_1\phi_{b_t}$. For $1 \leqslant j \leqslant t$, we set $C_{1,j} = \Gamma(e_1\phi_{b_j})$ and we form the following matrix, with rt rows and t columns:

$$M_1 = \begin{pmatrix} C_{1,1} & \cdots & C_{1,t} \end{pmatrix}.$$

We now consider a column vector E_2 outside the image of M_1 and define $e_2 = \Gamma^{-1}(E_2)$; e_2 is not $\mathrm{Frac}(A_K)$-collinear to e_1, and we have constructed a free family of cardinality 2. We then continue the same process, by setting $C_{2,j} = \Gamma(e_2\phi_{b,j})$ and considering the $rt \times 2t$ matrix

$$M_2 = \begin{pmatrix} C_{1,1} & \cdots & C_{1,t} & C_{2,1} & \cdots & C_{2,t} \end{pmatrix}.$$

We pick a column vector E_3 outside the image of M_2 and define $e_3 = \Gamma^{-1}(E_3)$, as well as M_3. We repeat this construction until we reach e_r. The vectors $e_1, \dots, e_r$ being linearly independent over $\mathrm{Frac}(A_K)$, they form a $\mathrm{Frac}(A_K)$-basis of $\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$. The matrix M_r is nothing but the change-of-basis matrix from the canonical $K[T]$-basis of $\mathbb{M}(\phi)$ to the newly computed basis $\mathcal{B} = (e_1\phi_{b_1}, \dots, e_1\phi_{b_t}, \dots, e_r\phi_{b_1}, \dots, e_r\phi_{b_t})$. If $f \in \mathbb{M}(\phi)$, the product $M_r^{-1} \cdot \Gamma^{-1}(f)$ gives the coordinates of f in $\mathcal{B}$. From this, we eventually read the coordinates of f in the $\mathrm{Frac}(A_K)$-basis $(e_1, \dots, e_r)$.

To summarize, we have constructed a $\mathrm{Frac}(A_K)$-basis of $\mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$ and designed an algorithm to compute coordinates in this basis. Using these inputs as primitives, it is now straightforward to extend the results of § 4.3.2 to the case of a general curve.

4.4 Discussion

We now discuss the theoretical and practical performances of our algorithms, and compare them with the state of the art. We consider Drinfeld $\mathbb{F}_q[T]$-modules ϕ over a field K. The rank is denoted by r, and the τ-degree of an endomorphism is denoted by n. We let ω be a feasible exponent for matrix multiplication, and Ω be a feasible exponent for matrix characteristic polynomial computation. The algorithms are implemented in the SageMath implementation of Chapter 3.

4.4.1 Theoretical asymptotic performance

We review possible algorithms in two settings: when K is an arbitrary field (§ 4.4.1.1), and when K is finite (§ 4.4.1.2).

4.4.1.1 On general fields

Currently, the only algorithm explicitly designed to compute the characteristic polynomial of an endomorphism when K is arbitrary is Algorithm 6 (Theorem 4.3.11).

Table 4.1: Algorithms for characteristic polynomials of degree n endomorphisms, in any rank r, over a generic field

Algorithm	*Operations in the base field & Frobenius applications*	*Constraints*
Th. 4.3.11 [1]	$O^{\sim}(n^2 + (n+r)r^{\Omega-1})$ & $O(n^2 + r^2)$	*None*

[1] Probabilistic algorithm. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the motive of the Drinfeld module.

4.4.1.2 On finite fields

When K is a finite extension of $\mathbb{F}_q$ with degree d, we can optimize Algorithm 6 to obtain Theorem 4.3.13. In this setting, one may also use the algorithms of [MS23], for which the authors take into account another parameter: the degree m of $\mathfrak{p}$.

Table 4.2: Algorithms for characteristic polynomials of degree n endomorphisms, in any rank r, over a finite field of degree d over $\mathbb{F}_q$

Algorithm	*Bit complexity*	*Constraints*
[MS23, Th. 2(1)] [1]	$O^{\bullet}\left(\left(r^{\Omega} + \min(nr^2, (n+r)r^{\omega-1})\right)\frac{d(n+m)}{m}\log q\right) + O^{\sim}(d\log^2 q)$	*None*
[MS23, Th. 2(2)] [1]	$O^{\bullet}\left(\left(r^{\Omega}\frac{d(n+m)}{m} + r\mathrm{SM}^{\geqslant 1}(n+r,d)\right)\log q\right) + O^{\sim}(d\log^2 q)$	*None*
Th. 4.3.13, `F-MFF` [2]	$O^{\bullet}((\mathrm{SM}^{\geqslant 1}(n,d) + ndr + nr^{\omega} + dr^{\omega})\log q) + O^{\sim}(d\log^2 q)$	*None*

[1] Two deterministic algorithms by Musleh and Schost. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the crystalline cohomology of the Drinfeld module.

[2] Probabilistic algorithm. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the motive of the Drinfeld module.

Remark 4.4.1. In all the tables (see also § 5.4 and 6.4), the term $O^{\sim}(d\log^2 q)$ which appears in blue on many lines corresponds to the precompution of the image of a generator of $K/\mathbb{F}_q$ by the Frobenius endomorphism (see § 1.3.1).

For the special case of the Frobenius endomorphism, many more methods are available, and we refer to § 6.4.

4.4.2 Benchmarks

We present benchmarks for the computation of characteristic polynomials of endomorphisms over a finite field. Our benchmarking protocol is the following: to test the behavior with respect to one parameter x (either the extension degree r, the τ-degree n or the rank r), we fix the two others and let x grow.

We fix $\mathbb{F}_q = \mathbb{F}_5$, and only consider base fields K of the form $\mathbb{F}_q[T]/\mathfrak{p}$, where $\mathfrak{p}$ is an $\mathbb{F}_q[T]$-characteristic. That is, m equals d. We have fixed a random seed, and our tests were run on an *AMD EPYC 7282 16-Core Processor*. Our benchmarks measure the computation time of the SageMath implementation of Algorithm 6. The exact code is accessible with instructions at:

`https://github.com/kryzar/thesis`

Remark 4.4.2. The reader should interpret our benchmarks with caution, as we rely on SageMath generic—and likely—unoptimized primitives. In particular, the implementations we mention do not implement the state of the art presented in § 1.3.1, nor the optimizations mentioned in § 4.3.1.1.

We observe the following run times:

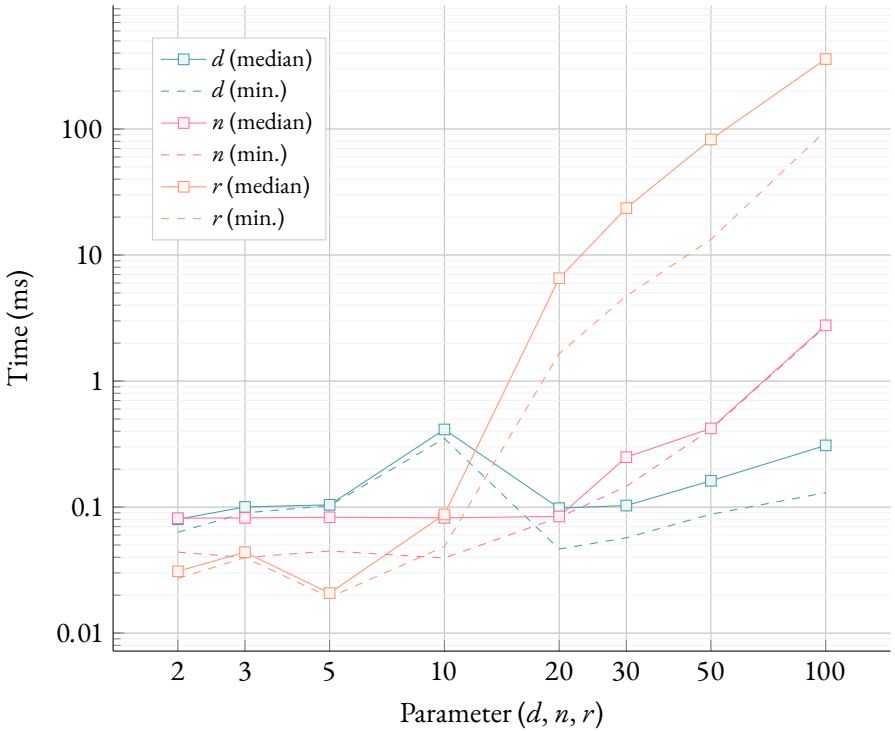


Figure 4.1: Computation of characteristic polynomial of endomorphisms of Drinfeld modules. We set $q = 5$, and make the extension degree d, the τ-degree n and the rank r vary. The default parameter values are $(d, n, r) = (15, 10, 10)$. Median computation time over ten samples, and minimum computation time among these samples.

Theoretically, the dependence in r is the most costly: it should behave as $O^\bullet(r^\omega)$, while the dependences to the two other parameters should be $O^\bullet(d)$ and $O^\bullet(n)$, respectively. We do observe that computation times with r growing and d, n fixed are the longest. However, more analysis is necessary to obtain a finer interpretation of the benchmarks.

Chapter 5
Computing norms of isogenies with Anderson motives

In this chapter, we adapt the results and algorithms of Chapter 4 to compute norms of isogenies.

Joint-work with Xavier Caruso. See Section 3 of [CL23].

5.1 Overview

In Theorem 4.2.7, we have seen that if u is an endomorphism of Drinfeld A-modules, then its characteristic polynomial is the characteristic polynomial of $\mathbb{M}(u)$, the action of u on the Anderson motive. If u is nonzero, the norm of u (as an isogeny) can also be obtained from the Anderson motive, by computing the determinant of $\mathbb{M}(u)$, as we had represented $\mathbb{M}(u)$ by a polynomial matrix. We build up on Chapter 4, and derive an algorithm to compute norms of general isogenies. In the case $A = \mathbb{F}_q[T]$, Step 2 of Algorithm 6 is replaced by the computation of a determinant, giving Algorithm 7, and the following complexity result:

Theorem C (see Theorems 5.3.1 and 5.3.2; see also Theorem C of [CL23])**.** Let ϕ and ψ be two rank r Drinfeld $\mathbb{F}_q[T]$-modules over K, and let u be an isogeny from ϕ to ψ of τ-degree n. The norm of u can be deterministically computed for a cost of $O^{\sim}(n^2 + nr^{\omega-1} + r^{\omega})$ operations in K and $O(n^2 + r^2)$ applications of the Frobenius.

Moreover, when K is a finite extension of $\mathbb{F}_q$ of degree d, the norm of u can be computed for an expected cost of

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + ndr + n \min(d, r) r^{\omega-1} + dr^{\omega}\right) \log q\right)$$

bit operations, using a Las Vegas algorithm.

While adapting Algorithm 6 to isogenies of isogenies of Drinfeld $\mathbb{F}_q[T]$-modules is rather straightforward, this is not the case for isogenies of Drinfeld A-modules. In that general context, the morphism $\mathbb{M}(u)$ is not represented by a matrix, and it appears we cannot compute $\mathfrak{n}(u)$ as the classical determinant of a polynomial matrix. Besides, $\mathbb{M}(u)$ is not *a priori* an endomorphism, so that the determinant of $\mathbb{M}(u)$ cannot be defined as in § 4.2.1. Our main task is thus to solve these theoretical problems. Working with finitely generated projective modules over a Dedekind domain, we begin by defining an appropriate notion of determinant. Once this is done, we describe this determinant in terms of Euler-Poincaré characteristics (§ 2.1.8.1), and the desired result follows by building on the duality between the functors $\mathbb{E}$ and $\mathbb{M}$, as in Chapter 4.

5.2 Theoretical preliminaries

In this section, we generalize Theorem 4.2.7 to general isogenies, by proving that the norm $\mathfrak{n}(u)$ of u is the determinant of $\mathbb{M}(u)$ (Theorem 5.2.3), for an appropriate notion of determinant in finitely generated projective modules over a Dedekind ring.

5.2.1 Defining determinants

Let R be a Dedekind domain. Let M, M' be two finitely generated projective R-modules of rank n. Let $f : M \to M'$ be an R-linear mapping. The morphism f gives rise to the R-linear map $\det f : \det M \to \det M'$ (§ 4.2.1.1). However, when f has different domain and codomain, *i.e.* $M \neq M'$, it no longer makes sense to interpret $\det f$ as the multiplication by some scalar. Instead, we define the "determinant" of f, denoted by $\mathfrak{det} f$, as

$$\mathfrak{det} f = (\det M' : \mathrm{Im}(\det f)) = \left\{a \in R : a \det M' \subset \mathrm{Im}(\det f)\right\}.$$

Equivalently $\mathfrak{det} f$ is the annihilator ideal of the cokernel of $\det f$.

Since R is a Dedekind domain, $\mathfrak{det} f$ can be decomposed as a product

$$\mathfrak{det} f = \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{det} f)},$$

where the product runs over all maximal ideals $\mathfrak{q}$ of R and the exponent $v_{\mathfrak{q}}(\mathfrak{det} f)$ is a nonnegative integer referred to as the $\mathfrak{q}$-*adic valuation* of $\mathfrak{det} f$. For the purpose of this thesis, it is fundamental to notice that $v_{\mathfrak{q}}(\mathfrak{det} f)$ can be found by computing the classical determinant of an actual matrix. Indeed, letting as before $R_{\mathfrak{q}}$ denote the completion of R at $\mathfrak{q}$, we define $M_{\mathfrak{q}} = R_{\mathfrak{q}} \otimes_R M$ and $M'_{\mathfrak{q}} = R_{\mathfrak{q}} \otimes_R M'$. The map f induces an $R_{\mathfrak{q}}$-linear morphism $f_{\mathfrak{q}} : M_{\mathfrak{q}} \to M'_{\mathfrak{q}}$. We deduce from the flatness of $R_{\mathfrak{q}}$ over R that

$$\mathfrak{det} f_{\mathfrak{q}} = R_{\mathfrak{q}} \otimes_R \mathfrak{det} f = (\mathfrak{q} \cdot R_{\mathfrak{q}})^{v_{\mathfrak{q}}(\mathfrak{det} f)}, \tag{5.1}$$

where $\mathfrak{det} f_{\mathfrak{q}}$ is defined, similarly to $\mathfrak{det} f$, as the annihilator ideal of the cokernel of $f_{\mathfrak{q}}$. On the other hand, we know that $R_{\mathfrak{q}}$ is a principal domain. Hence both $M_{\mathfrak{q}}$ and $M'_{\mathfrak{q}}$ are free of rank n over $R_{\mathfrak{q}}$. We choose bases $\mathcal{B}_{(\mathfrak{q})}$ and $\mathcal{B}'_{(\mathfrak{q})}$ of $M_{\mathfrak{q}}$ and $M'_{\mathfrak{q}}$ respectively, and let $F_{\mathfrak{q}}$ denote the matrix of $f_{\mathfrak{q}}$ in these bases. It follows from the definition that $\mathfrak{det} f_{\mathfrak{q}} = \det(F_{\mathfrak{q}})\, R_{\mathfrak{q}}$. Comparing with Equation (5.1), we finally conclude that

$$v_{\mathfrak{q}}(\mathfrak{det} f) = v_{\mathfrak{q}}(\det F_{\mathfrak{q}}).$$

We notice in particular that, although the determinant itself depends on the choices of $\mathcal{B}_{(\mathfrak{q})}$ and $\mathcal{B}'_{(\mathfrak{q})}$, its $\mathfrak{q}$-adic valuation does not. Indeed, changing $\mathcal{B}_{(\mathfrak{q})}$ (resp. $\mathcal{B}'_{(\mathfrak{q})}$) boils down to multiplying $F_{\mathfrak{q}}$ by an invertible matrix on the left (resp. on the right), which only multiplies the determinant by a unit, and as such, does not affect its $\mathfrak{q}$-adic valuation.

Remark 5.2.1. When studying projective modules, it is more common to consider the localization $R_{(\mathfrak{q})}$ instead of the completion $R_{\mathfrak{q}}$. Although the first setting is simpler, the second better suits our needs.

In a similar fashion, one can relate $\mathfrak{det} f$ to the Euler-Poincaré characteristic (§ 2.1.8.1) of the cokernel of f, which is essential to establish Theorem 5.2.3.

Proposition 5.2.2 (Proposition 3.1 of [CL23])**.** *We have*

$$\mathfrak{det} f = \xi_R(\mathrm{Coker} f).$$

Proof. As we have seen, the Euler-Poincaré characteristic commutes with completion. Therefore, it is enough to prove that $\mathfrak{det} f_\mathfrak{q} = \xi_{R_\mathfrak{q}}(\mathrm{Coker} f_\mathfrak{q})$ for each maximal ideal $\mathfrak{q}$ of R. Let then $\mathfrak{q}$ be a maximal ideal of R. It follows from the structure theorem of finitely generated modules over principal domains that there exist bases $\mathcal{B}_\mathfrak{q}$ and $\mathcal{B}'_\mathfrak{q}$ in which the matrix $F_\mathfrak{q}$ of $f_\mathfrak{q}$ is diagonal. If $\delta_1, \dots, \delta_r$ denote its diagonal coefficients, we have

$$\mathrm{Coker} f_\mathfrak{q} \simeq \left(R_\mathfrak{q}/\delta_1 R_\mathfrak{q}\right) \times \cdots \times \left(R_\mathfrak{q}/\delta_r R_\mathfrak{q}\right).$$

Hence

$$\xi_{R_\mathfrak{q}}(\mathrm{Coker} f_\mathfrak{q}) = \delta_1 \cdots \delta_r \cdot R_\mathfrak{q} = (\det F_\mathfrak{q}) \cdot R_\mathfrak{q} = \mathfrak{det} f_\mathfrak{q},$$

which is what we wanted to prove. □

5.2.2 Main result

Having defined an appropriate notion of determinant for our setting, we can state and prove Theorem 5.2.3:

Theorem 5.2.3 (Theorem 3.2 of [CL23])**.** *Let ϕ and ψ be two Drinfeld A-modules over K, and let u be an isogeny from ϕ to ψ. We have*

$$\mathfrak{n}(u) = \mathfrak{det}\, \mathbb{M}(u).$$

Proof. Writing u as the product of a purely inseparable isogeny with a separable isogeny, and noticing that (1) $\mathfrak{det}$ is multiplicative and (2) $\mathbb{M}$ is functorial, we are reduced to proving the theorem when $u = \tau^{\deg(\mathfrak{p})}$ on the one hand and when u is separable on the other hand.

Purely inseparable case. We assume that $u = \tau^{\deg(\mathfrak{p})}$. We follow Gekeler's idea for proving the multiplicativity of the norm [Gek91, Lemma 3.10]. Let $\mathfrak{q} \subset A_K$ be a maximal ideal away from the characteristic. Note that the map $\mathbb{E}_\mathfrak{q}(u) : \mathbb{E}_\mathfrak{q}(\phi) \to \mathbb{E}_\mathfrak{q}(\psi)$ is an isomorphism because τ is coprime with the right gcd of ϕ_q for q varying in $\mathfrak{q}$. By Theorem 4.2.5, we conclude that $\mathbb{M}_\mathfrak{q}(u) : \mathbb{M}_\mathfrak{q}(\psi) \to \mathbb{M}_\mathfrak{q}(\phi)$ is an isomorphism as well, showing that $\mathfrak{q}$ is coprime with $\xi_{A_K}(\mathrm{Coker}\, \mathbb{M}(u))$. Since this holds for any $\mathfrak{q}$, $\mathfrak{det}\, \mathbb{M}(u)$ is a power of $\mathfrak{p}$. On the other hand, observe that, by definition,

$$\deg_\tau(u) = \dim_K(\mathrm{Coker}\, \mathbb{M}(u)) = \deg(\xi_{A_K}(\mathbb{M}(u))).$$

Proposition 5.2.2 then implies that $\deg(\mathfrak{det}\, \mathbb{M}(u)) = \deg_\tau(u) = \deg(\mathfrak{p})$. Putting all together, we conclude that $\mathfrak{det}\, \mathbb{M}(u) = \mathfrak{p} = \mathfrak{n}(u)$.

Separable case. Given that u is nonzero, the kernel of the A-linear map $\mathbb{E}(u)$ is a torsion A-module. Let $a \in A$ such that $a \cdot \ker \mathbb{E}(u) = 0$. For all elements $z \in \overline{K}$, we then have the following implication: if $u(z) = 0$, then $\phi_a(z) = 0$. Since u is separable, this implies that u right-divides ϕ_a, from which we deduce that a annihilates $\mathrm{Coker}\, \mathbb{M}(u)$ as well. Applying successively the right exact functor $- \otimes_A A/aA$ and the left exact functor $\mathrm{Hom}_K(-, \overline{K})$ to the exact sequence of A_K-modules

$$0 \to \mathbb{M}(\psi) \to \mathbb{M}(\phi) \to \mathrm{Coker}\, \mathbb{M}(u) \to 0,$$

we get the following exact sequence of $A_{\overline{K}}$-modules

$$0 \to (\operatorname{Coker} \mathbb{M}(u))^* \otimes_K \overline{K} \to \mathbb{M}_a(\phi)^* \otimes_K \overline{K} \to \mathbb{M}_a(\psi)^* \otimes_K \overline{K}.$$

This shows that

$$(\operatorname{Coker} \mathbb{M}(u))^* \otimes_K \overline{K} \simeq \ker\left(\mathbb{M}_a(u)^*\right) \otimes_K \overline{K} \simeq \ker\left(\mathbb{M}_a(u)^* \otimes_K \mathrm{Id}_{\overline{K}}\right).$$

From Theorem 4.2.5, we then derive the following isomorphisms of $A_{\overline{K}}$-modules:

$$\begin{aligned}(\operatorname{Coker} \mathbb{M}(u))^* \otimes_K \overline{K} &\simeq \operatorname{Ker}\left(\mathbb{E}_a(u) \otimes_{\mathbb{F}_q} \overline{K}\right)\\ &= \operatorname{Ker}\left(\mathbb{E}(u) \otimes_{\mathbb{F}_q} \overline{K}\right)\\ &\simeq \operatorname{Ker} \mathbb{E}(u) \otimes_{\mathbb{F}_q} \overline{K}.\end{aligned}$$

Consequently, u being separable, we find that

$$\mathfrak{n}(u) = \xi_A\left(\operatorname{Ker} \mathbb{E}(u)\right) = \xi_{A_K}\left((\operatorname{Coker} \mathbb{M}(u))^*\right).$$

Using finally Lemma 4.2.4, we end up with $\mathfrak{n}(u) = \xi_{A_K}(\operatorname{Coker} \mathbb{M}(u)) = \mathfrak{det}\, \mathbb{M}(u)$, proving the theorem. □

An interesting consequence of Theorem 5.2.3 is a compatibility result between norms of isogenies and restrictions of Drinfeld modules (see §2.2.1.3), which will be particularly useful to us when Drinfeld A-modules are restricted to $A' = \mathbb{F}_q[T]$.

Corollary 5.2.4 (Corollary 3.3 of [CL23])**.** *Let $\gamma' : A' \to K$ be a second base for Drinfeld modules satisfying the assumptions of § 2.2, coming together with an injective homomorphism of rings $f : A' \to A$ such that $\gamma' = \gamma \circ f$. Let also ϕ and ψ be two Drinfeld A-modules over K, with a morphism u from ϕ to ψ. Then*

$$\mathfrak{n}\left(f^* u\right) = N_{A/A'}\left(\mathfrak{n}(u)\right),$$

where $N_{A/A'} : A \to A'$ is the norm map from A to A' via *f.*

Proof. Let $\mathfrak{p}'$ be a prime ideal of A'_K, and let $A'_{K,\mathfrak{p}'}$ be the completion of A'_K at $\mathfrak{p}'$. Write $A_{K,\mathfrak{p}'} = A'_{K,\mathfrak{p}'} \otimes_{A'_K} A_K$, $\mathbb{M}(\phi)_{\mathfrak{p}'} = A'_{K,\mathfrak{p}'} \otimes_{A'_K} \mathbb{M}(\phi)$, and $\mathbb{M}(\psi)_{\mathfrak{p}'} = A'_{K,\mathfrak{p}'} \otimes_{A'_K} \mathbb{M}(\psi)$. Since $A_{K,\mathfrak{p}'}$ is a product of local rings, the module $\mathbb{M}(\phi)_{\mathfrak{p}'}$ is free over $A_{K,\mathfrak{p}'}$. We pick a basis $\mathcal{B}_\phi = (e_{\phi,i})_{1\leqslant i\leqslant r}$ of it, together with a basis $\mathcal{B} = (a_m)_{1\leqslant m\leqslant n}$ of $A_{K,\mathfrak{p}'}$ over $A'_{K,\mathfrak{p}'}$. Note that the family $\mathcal{B}'_\phi = (a_m \cdot e_{\phi,i})_{1\leqslant i\leqslant r, 1\leqslant m\leqslant n}$ is a $A'_{K,\mathfrak{p}'}$-basis of $\mathbb{M}(\phi)'_{\mathfrak{p}} = \mathbb{M}(f^*\phi)'_{\mathfrak{p}'}$. We define similarly $\mathcal{B}_\psi$ and $\mathcal{B}'_\psi$. Let $C = (c_{ij})_{1\leqslant i,j\leqslant r}$ be the matrix of $\mathbb{M}(u)$ with respect to the bases $\mathcal{B}_\psi$ and $\mathcal{B}_\phi$ and, for $a \in A'_{K,\mathfrak{p}'}$, let $M(a) \in (A'_{K,\mathfrak{p}'})^{n\times n}$ be the matrix of the multiplication by a over $A_{K,\mathfrak{p}'}$. The matrix of f^*u in the bases $\mathcal{B}'_\psi$ and $\mathcal{B}'_\phi$ is the block matrix

$$D = \begin{pmatrix} M(c_{1,1}) & \cdots & M(c_{1,r}) \\ \vdots & & \vdots \\ M(c_{r,1}) & \cdots & M(c_{r,r}) \end{pmatrix}$$

The main result of [Siloo] implies that $\det D = N_{A_{K,\mathfrak{p}'}/A'_{K,\mathfrak{p}'}}(\det C)$. The proposition then follows from Theorem 5.2.3. □

5.3 Algorithms

We now turn to algorithms to compute $\mathfrak{n}(u)$, the norm of the isogeny u.

5.3.1 Algorithms for $A = \mathbb{F}_q[T]$

As in § 4.3.2, we now assume that A is $\mathbb{F}_q[T]$. Theorem 5.2.3 readily translates to an algorithm for computing the norm of an isogeny between Drinfeld modules: Algorithm 7.

Algorithm 7. IsogenyNorm (Algorithm 5 of [CL23])

Input: An isogeny u from ϕ to ψ encoded by its defining Ore polynomial
Output: The norm of u
1 Compute $M = \mathrm{MotiveMatrix}(u)$;
2 return the ideal generated by determinant of M

Theorem 5.3.1 (Theorem 3.4 of [CL23]). *Recall ϕ and ψ are two Drinfeld $\mathbb{F}_q[T]$-modules of rank r over K. Let u be an endomorphism of ϕ with τ-degree n. Using Algorithm 7, the norm of u can be computed (deterministic algorithm) for a cost of $O(n^2 + r^2)$ applications of the Frobenius endomorphism of K and $O^{\sim}(n^2 + nr^{\omega-1} + r^{\omega})$ operations in K.*

Proof. Per Lemma 4.3.10, the cost of computing the matrix of $\mathbb{M}(u)$ is $O(n^2+r^2)$ applications of the Frobenius endomorphism, and $O(n^2+r^2)$ operations in K. Besides, this matrix has size r and its entries have degrees all less than $1 + \frac{n}{r}$ (Corollary 4.3.7, which is also valid for isogenies). Therefore, using the algorithmic primitives of § 4.3.1.1, computing its determinant requires $O^{\sim}((n+r)r^{\omega-1})$ operations in K. □

When K is a finite field, one can speed up Algorithm 7 using the optimized primitives of § 1.3.4 for manipulating Ore polynomials, as for the endomorphism case. Precisely, we have the following.

Theorem 5.3.2 (Theorem 3.5 of [CL23]). *Recall ϕ and ψ are two Drinfeld $\mathbb{F}_q[T]$-modules of rank r over K. Let u be an endomorphism of ϕ with τ-degree n. Assume K is a finite extension of $\mathbb{F}_q$, with degree d over $\mathbb{F}_q$. Using Algorithm 5, and the primitives of § 1.3, the norm of u can be computed (Las Vegas algorithm) for an expected cost of*

$$O^{\sim}(d \log^2 q) + O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + ndr + n \min(d, r) r^{\omega-1} + dr^{\omega}\right) \log q\right)$$

bit operations.

Proof. By lemma 4.3.12, the computation of the matrix of $\mathbb{M}(u)$ requires an initial computation costing $O^{\sim}(d \log^2 q)$ bit operations, followed by $O^{\bullet}\left(\left(\mathrm{SM}^{\geqslant 1}(n, d) + dr(n + r)\right) \log q\right)$ bit operations. Then, for the computation of the determinant, we distinguish between two cases. If $d \leqslant r$, we keep on using the algorithms of [GJV03; JV06], for a cost of $O^{\sim}(nr^{\omega-1} + r^{\omega})$ operations in K, that is $O^{\sim}(ndr^{\omega-1} + dr^{\omega})$ operations in $\mathbb{F}_q$. On the contrary, when $d \geqslant r$, we use Lemma 4.3.1, performing then $O^{\bullet}(nr^{\omega} + dr^{\omega})$ operations in $\mathbb{F}_q$. Putting all together, and remembering that an operation in $\mathbb{F}_q$ corresponds to $O^{\sim}(\log q)$ bit operations, we get the theorem. □

Remark 5.3.3. When u is an endomorphism, the norm can be computed as the constant coefficient of the characteristic polynomial of u, up to a sign. We notice that the algorithms of the present subsection in some cases run faster than these of § 4.3.2. This is because we compute the determinant of the matrix of $\mathbb{M}(u)$ instead of its whole characteristic polynomial. However, we stress that the asymptotic costs of computing the characteristic polynomial and the norm of an endomorphism may be equal. This owes to the fact that in some cases, computing the characteristic polynomial of a matrix, or computing its determinant, both reduce to matrix multiplication.

Remark 5.3.4. In the special case where $u = \pi$ is the Frobenius endomorphism, the norm is given by a simple closed formula (see [Geko8, Theorem 2.11] and [Pap23, Theorem 2.4.7]), namely

$$\mathfrak{n}(\pi) = (-1)^{rd-r-d} N_{K/\mathbb{F}_q}(\Delta)^{-1} \mathfrak{p}^{\frac{d}{\deg(\mathfrak{p})}}, \tag{5.2}$$

where Δ is the leading coefficient of ϕ_T. Computing the Frobenius norm using Equation (5.2) costs $O^{\sim}(d \log^2 q) + O^{\bullet}(d \log q)$ bit operations [MS19, Proposition 3]. Noticing that the *Frobenius norm* is a degree d polynomial in $\mathbb{F}_q[T]$, this complexity is essentially optimal with respect to d, and asymptotically better than other algorithms mentioned in this thesis (see also discussions in § 4.4, § 5.4, and § 6.4).

5.3.2 Algorithms for generic A

When A is arbitrary, determining the norm of an isogeny u from ϕ to ψ becomes more complex due to the nonfreeness of the motives $\mathbb{M}(\phi)$ and $\mathbb{M}(\psi)$ in general. This necessitates working with arbitrary torsion-free modules over Dedekind domains. While this approach appears viable, we will follow an alternative strategy that simplifies the general scenario by reducing the computation to the previously addressed case of $\mathbb{F}_q[T]$.

From now on, we assume for simplicity that A is presented as

$$A = \mathbb{F}_q[X, Y]/P(X, Y)$$

and that $\deg(x) > \deg(y)$, where x and y denote the images in A of X and Y respectively. Let ϕ and ψ be two rank r Drinfeld A-modules over K, and let $u : \phi \to \psi$ be an isogeny between them. We consider a new variable Λ and form the polynomial rings $K[\Lambda]$ and $A_K[\Lambda]$. We set

$$\mathbb{M}(\phi)[\Lambda] = A_K[\Lambda] \otimes_{A_K} \mathbb{M}(\phi)$$

and endow it with the structure of $K[T, \Lambda]$-module inherited from its structure of $A_K[\Lambda]$-module through the ring homomorphism

$$\begin{array}{rccc} f: & K[T,\Lambda] & \to & A_K[\Lambda] \\ & P(T,\Lambda) & \mapsto & P(x+\Lambda y, \Lambda). \end{array}$$

Similarly, we define $\mathbb{M}(\psi)[\Lambda]$ and endow it with a structure of $K[T, \Lambda]$-module.

The assumption $\deg(x) > \deg(y)$ ensures that $\phi_x + \Lambda \cdot \phi_y$ is an Ore polynomial of degree $r \cdot \deg(x)$ with leading coefficient lying in K. Writing $s = r \cdot \deg(x)$, we deduce that the family $(1, \tau, \dots, \tau^{s-1})$ is a $K[T, \Lambda]$-basis of both $\mathbb{M}(\phi)[\Lambda]$ and $\mathbb{M}(\psi)[\Lambda]$. On the other hand, we observe that, after extending scalars to $A_K[\Lambda]$, the morphism $\mathbb{M}(u) : \mathbb{M}(\psi) \to \mathbb{M}(\phi)$ induces a $K[T, \Lambda]$-linear map $\mathbb{M}(u)[\Lambda] : \mathbb{M}(\psi)[\Lambda] \to \mathbb{M}(\phi)[\Lambda]$. Its determinant in the aforementioned distinguished bases is a bivariate polynomial, that we call $\delta(T, \Lambda)$. Evaluating it at $T = x + \Lambda y$, we obtain a univariate polynomial in Λ with coefficients in A_K.

Theorem 5.3.5 (Theorem 3.8 of [CL23]). *With the above notation and hypothesis, the leading coefficient of $\delta(T, \Lambda)$ with respect to T is a nonzero constant $c \in K^\times$. Moreover, if we write*

$$\delta(x+\Lambda y, \Lambda) = \delta_0 + \delta_1 \cdot \Lambda + \cdots + \delta_n \cdot \Lambda^n \qquad (n \in \mathbb{Z}_{\geqslant 0},\ \delta_i \in A_K),$$

then $c^{-1}\delta_0, \ldots, c^{-1}\delta_n$ all lie in A and generate $\mathfrak{n}(u)$.

Proof. For any fixed element $\lambda \in \overline{K}$, notice that the degree of the univariate polynomial $\delta(T, \lambda)$ is equal to the τ-degree of u. Since the latter remains constant when λ varies in $\overline{K}$, so does the former. The first assertion of the theorem follows.

Set $I = \overline{K} \otimes_{\mathbb{F}_q} \mathfrak{n}(u)$, which is an ideal of $A_{\overline{K}}$. Recall that the maximal ideals of $A_{\overline{K}}$ are all of the form

$$\mathfrak{m}_{(x_0,y_0)} = (x - x_0)A_{\overline{K}} + (y - y_0)A_{\overline{K}}$$

with $x_0, y_0 \in \overline{K}$. We write the decomposition of I into a product of prime ideals:

$$I = \mathfrak{m}_{(x_1,y_1)} \cdot \mathfrak{m}_{(x_2,y_2)} \cdots \mathfrak{m}_{(x_\ell,y_\ell)} \tag{5.3}$$

where ℓ is a nonnegative integer and $x_i, y_i \in \overline{K}$ for all i between 1 and ℓ.

We fix an element $\lambda \in \overline{K}$ and consider the ring homomorphism $f_\lambda : \overline{K}[T] \to A_{\overline{K}}$ defined by $T \mapsto x + \lambda y$. The map f_λ is the specialization of f at λ, and a finite morphism whose degree does not depend on λ. Let $N_\lambda : A_{\overline{K}} \to \overline{K}[T]$ denote the norm map with respect to f_λ. It follows from the decomposition (5.3) that $N_\lambda(I)$ is the ideal of $\overline{K}[T]$ generated by the polynomial

$$P_\lambda(T) = (T - x_1 - \lambda y_1) \cdots (T - x_\ell - \lambda y_\ell).$$

On the other hand, repeating the proof of Corollary 5.2.4, we find that $N_\lambda(I)$ is also the ideal generated by $\delta(T, \lambda)$. Therefore $\delta(T, \lambda) = c \cdot P_\lambda(T)$. Since this equality holds for any $\lambda \in \overline{K}$, it is safe to replace λ by the formal variable Λ. Specializing at $T = x + \Lambda y$, we obtain

$$\delta(x + \Lambda y, \Lambda) = c \cdot \prod_{i=1}^{\ell} \big((x - x_i) + \Lambda \cdot (y - y_i)\big)$$

Expanding the latter product and comparing with the definition of I, we find that I is the ideal of $A_{\overline{K}}$ generated by $\delta_0, \ldots, \delta_n$. Finally, the fact that I is defined over A implies that the pairs (x_i, y_i) are conjugated under the Galois action, which eventually shows that the $c^{-1} \cdot \delta_i$'s are in A. The theorem follows. □

Theorem 5.3.5 readily translates to an algorithm for computing the norm $\mathfrak{n}(u)$, namely:

(i) Compute the matrix of $\mathbb{M}(u)[\Lambda]$ using Algorithm 5 (treating Λ as a formal parameter).

(ii) Compute the determinant $\delta(T, \Lambda)$ of this matrix and let $c \in K^\times$ be its leading coefficient with respect to T,

(iii) Write

$$c^{-1} \cdot \delta(x+\Lambda y, \Lambda) = \delta'_0 + \delta'_1 \cdot \Lambda + \cdots + \delta'_n \cdot \Lambda^n \qquad (\delta'_i \in A_K).$$

(iv) Return the ideal of A generated by $\delta'_0, \ldots, \delta'_n$.

It follows from the proof of Theorem 5.3.5 that the degree n of $\partial(x+\Lambda y, \Lambda)$ is equal to ℓ, on the one hand, and to the τ-degree of the isogeny u, on the other hand. Unfortunately, this quantity may be large, especially when we compare it with the minimal number of generators of $\mathfrak{n}(u)$, which is at most 2 because A is a Dedekind domain.

To overcome this issue, an option could be to compute the δ'_i's one by one by using relaxed arithmetics [Hei04]: each time a new δ'_i is computed, we form the ideal I_i generated by $\delta'_0, \ldots, \delta'_i$ and stop the process when I_i has degree n; we then have the guarantee that $\mathfrak{n}(u) = I_i$ and that we have computed the ideal we were looking for. When $x_1, \ldots, x_\ell$ are pairwise disjoint (which is the most favorable case), we already have $\mathfrak{n}(u) = I_1$, so that the above procedure stops very rapidly. Another option consists in picking random elements $\lambda \in K$ and computing the evaluations $\partial(T, \lambda)$ and $c^{-1}\cdot\partial(x+\lambda y, y)$. Doing so, we obtain elements in $\mathfrak{n}(u)$ and we can hope, as above, that only a few number of them will generate the ideal. Again, this can be checked by looking at the degree of the candidate ideals.

5.4 Discussion

We now discuss the theoretical and practical performances of our algorithms, and compare them with the state of the art, as in § 4.4. We reuse the notations of § 4.4.2, and recall Remark 4.4.2 about the interpretation of run times.

5.4.1 Theoretical asymptotic performance

To compute the norm of an isogeny of Drinfeld modules, it currently seems that the only algorithm explicitly designed to do so is Algorithm 7 (Theorem 5.3.1). However, we believe that the algorithms of [MS23] could be adapted to that setting, and we mention that any algorithm computing the characteristic polynomial of an endomorphism computes its norm as a byproduct. We review possible algorithms in two settings: when K is an arbitrary field (§ 5.4.1.1), and when K is finite (§ 5.4.1.2).

5.4.1.1 On general fields

On arbitrary fields, we have:

Table 5.1: Algorithms for computing norms of degree n isogenies, in any rank r, over a generic field

Algorithm	*Operations in the base field & Frobenius applications*	*Constraints*
Th. 5.3.1 [1]	$O^{\sim}(n^2 + (n+r)r^{\omega-1})$ & $O(n^2 + r^2)$	*None*

[1] Probabilistic algorithm. The norm of any isogeny is the determinant of the motivic application associated to the isogeny.

5.4.1.2 On finite fields

On finite fields, Algorithm 7 is optimized and gives Theorem 5.3.2:

Table 5.2: Algorithms for computing norms of degree n isogenies, in any rank r, over a finite field of degree d over $\mathbb{F}_q$

Algorithm	*Bit complexity*	*Constraints*
Th. 5.3.2 [1]	$O^{\bullet}\big((\mathrm{SM}^{\geqslant 1}(n,d) + ndr + n\min(d,r)r^{\omega-1} + dr^{\omega})\log q\big)$ $+ O^{\sim}(d\log^2 q)$	*None*

[1] Probabilistic algorithm. The norm of any isogeny is the determinant of the motivic application associated to the isogeny.

Remark 5.4.1. Furthermore, the Frobenius norm can be computed in $O^{\sim}(d\log^2 q) + O^{\bullet}(d\log q)$ bit operations (see Remark 5.3.4), which is strictly better than any other algorithm mentioned in this paper.

5.4.2 Benchmarks

As for its counterpart in Chapter 4, we provide benchmark for the implementation of Algorithm 7. The methodology is the same as that of § 4.4.2.

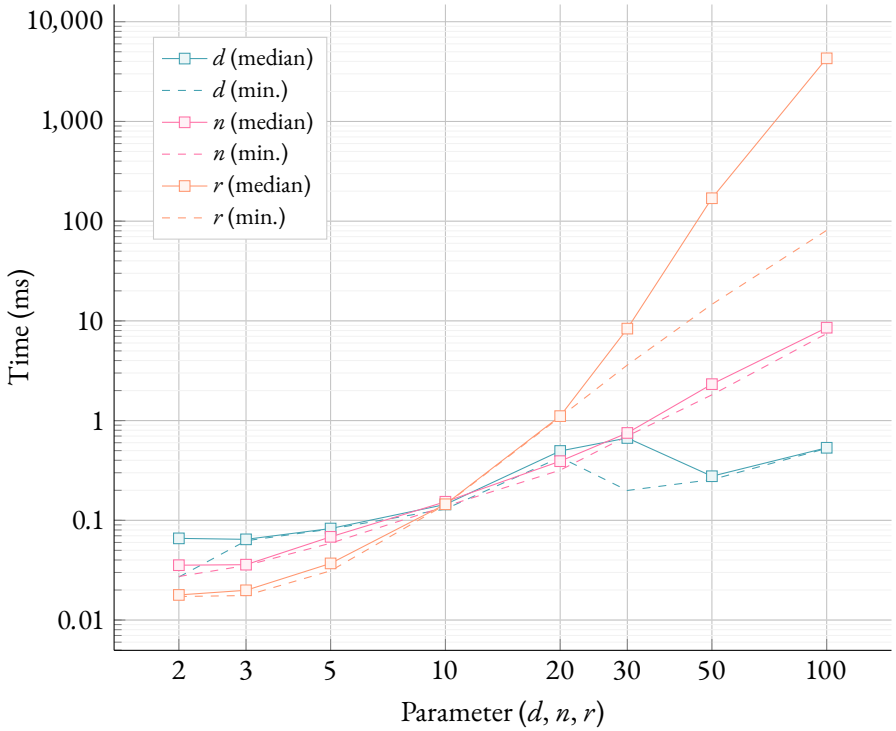


Figure 5.1: Computation of norms of isogenies of Drinfeld modules. We set $q = 5$, and make the extension degree d, the τ-degree n and the rank r vary. The default parameter values are $(d, n, r) = (15, 10, 10)$. Median computation time over ten samples, and minimum computation time among these samples.

The benchmarks interpretation is similar as that of § 4.4.2.

Chapter 6

Computing the Frobenius characteristic polynomial as a reduced norm

We present another algorithm to compute the characteristic polynomial of a Drinfeld module defined over a finite field; namely the `F-CSA` item of Theorem B. This approach, different than that of Chapter 4, relies on the computation of a reduced norm in a central simple algebra. While the methods of Chapter 4 work best when the rank is low with respect to the extension degree d, the method presented here is competitive in the opposite situation.

Joint-work with Xavier Caruso. See Section 4 of [CL23].

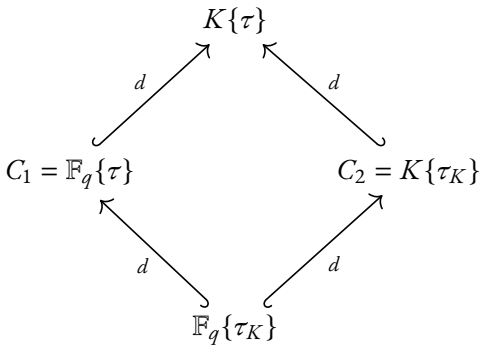
6.1 Overview

In Chapter 4, we have seen that the characteristic polynomial of the Frobenius endomorphism can be efficiently computed as the characteristic polynomial of an r-by-r matrix with coefficients in $K[T]$, where r is the rank of the Drinfeld $\mathbb{F}_q[T]$-module ϕ over K, a degree d extension of $\mathbb{F}_q$. We now look at another way to produce a polynomial matrix whose characteristic polynomial is that of the Frobenius endomorphism.

Recall that for any rank r Drinfeld module ϕ over K, the Frobenius endomorphism is defined by the Ore polynomial $\tau_K = \tau^d$ of $K\{\tau\}$. Independently of Drinfeld modules, τ_K is an important invariant: the center of $K\{\tau\}$ is $\mathbb{F}_q\{\tau_K\}$. However, $\mathbb{F}_q\{\tau_K\}$ is not the only commutative subalgebra of $K\{\tau\}$; for example, $C_1 = \mathbb{F}_q\{\tau\}$ and $C_2 = K\{\tau_K\}$ are commutative and maximal. Let C_i be either C_1 or C_2. We see $K\{\tau\}$ as a C_i-algebra through left-multiplication:

$$\begin{array}{rcl} C_i \times K\{\tau\} & \to & K\{\tau\} \\ (\lambda, f) & \mapsto & \lambda f. \end{array}$$

With that definition, $\mathbb{F}_q\{\tau\}$ and $K\{\tau_K\}$ both have rank d over $\mathbb{F}_q\{\tau^d\}$, and $K\{\tau\}$ has degree d over both of them. Indeed, if $(e_1, \dots, e_d)$ is a basis of K over $\mathbb{F}_q$, then it is also a basis of $K\{\tau\}$ over $\mathbb{F}_q\{\tau\}$, while a basis of $K\{\tau\}$ over $K\{\tau_K\}$ is given by $(1, \tau, \dots, \tau^{d-1})$.



We can then look at the C_i-linear application

$$\begin{array}{rccc} \mathrm{m}_{\phi_T}: & K\{\tau\} & \to & K\{\tau\} \\ & f & \mapsto & f\phi_T. \end{array}$$

Through m_{ϕ_T}, we can define the norm $\mathrm{N}_{K\{\tau\}/C_1}(\phi_T)$ (resp. $\mathrm{N}_{K\{\tau\}/C_2}(\phi_T)$) of ϕ_T with respect to C_1 (resp. C_2), and we can also define characteristic polynomials.

Example 6.1.1. Let us look at a concrete example. Fix $\mathbb{F}_q = \mathbb{F}_2$, $K = \mathbb{F}_4 = \{0, 1, i, i+1\}$, and let ϕ be defined by $\phi_T = i + \tau$. We compute the matrices M_1 and M_2 of m_{ϕ_T}, respectively with respect to the bases C_1 and C_2, respectively.

(i) Over C_1, a basis of $\mathbb{F}_4\{\tau\}$ over $\mathbb{F}_2\{\tau\}$ is given by $(1, i)$. We have

$$\begin{cases} \mathrm{m}_{\phi_T}(1) = 1(i+\tau) = (\tau, 1)^\intercal, \\ \mathrm{m}_{\phi_T}(i) = i(i+\tau) = i + 1 + i\tau = i + 1 + \tau(i+1) = i + 1 + \tau i + \tau = (1+\tau, 1+\tau)^\intercal. \end{cases}$$

We get

$$M_1 = \begin{pmatrix} \tau & 1+\tau \\ 1 & 1+\tau \end{pmatrix}.$$

(ii) Over C_2, a basis of $\mathbb{F}_4\{\tau\}$ over $\mathbb{F}_4\{\tau^2\}$ is given by $(1, \tau)$. We have

$$\begin{cases} \mathrm{m}_{\phi_T}(1) = 1(i+\tau) = (i, 1)^\intercal, \\ \mathrm{m}_{\phi_T}(i) = \tau(i+\tau) = (1+i)\tau + \tau^2 = (\tau^2, 1+i)^\intercal. \end{cases}$$

We get

$$M_2 = \begin{pmatrix} i & \tau^2 \\ 1 & 1+i \end{pmatrix}.$$

We then compute $\chi(M_1)$ and $\chi(M_2)$, obtaining

$$\chi(M_1)(x) = \chi(M_2)(x) = x^2 + x + \tau^2 + 1.$$

In the meantime, one can use Algorithm 6 to compute $\chi(\pi)$, the characteristic polynomial of the Frobenius endomorphism π of ϕ. We obtain, as a degree one polynomial of $\mathbb{F}_q[T][X]$,

$$\chi(\pi) = X + T^2 + T + 1.$$

The key is to notice that $\chi(\pi)$ is obtained from $\chi(M_1)$ by substituting T for x and X for τ^2.

Picking other values for $\mathbb{F}_q$, K, and ϕ, inevitably leads to the same observation: the characteristic polynomials of M_1 and M_2 are equal, they have coefficients in $\mathbb{F}_q\{\tau_K\}$—which is isomorphic to a classical univariate polynomial ring—and we obtain $\chi(\pi)$ by substituting T for x and X for τ_K. The purpose of this chapter is to properly state and prove this observation (Theorem 6.2.3), turning it into an efficient algorithm to compute the characteristic polynomial of the Frobenius endomorphism (Algorithm 9 and Theorem 6.3.2).

6.2 Theoretical preliminaries

We let K be a finite extension of $\mathbb{F}_q$; its degree over $\mathbb{F}_q$ is denoted d. The ring A is as in § 2.2. We fix ϕ, a Drinfeld A-module over K of rank r, whose Frobenius endomorphism is denoted π. By definition, π is defined by the Ore polynomial $\tau_K = \tau^d$ of $K\{\tau\}$. We go on to prove Theorem 6.2.3, which expresses $\chi(\pi)$ as a reduced norm in a central simple algebra. Doing that requires a preliminary introduction on general Ore polynomials and reduced norms: we refer to § 1.1.2.

We begin by defining the main objects of study. Recall § 1.1.2, and notice that $K\{\tau\}$ can be alternatively depicted as the ring

$$K[t; \mathrm{Frob}] \simeq K\{\tau\},$$

where $\mathrm{Frob} : K \to K$ is the Frobenius endomorphism taking x to x^q. Recall that we have set $A_K = K \otimes_{\mathbb{F}_q} A$, and define

$$\theta = \mathrm{Frob} \otimes \mathrm{id}_A : \quad A_K \quad \to \quad A_K,$$

which is a ring endomorphism of A_K of order d, with fixed subring A. We form the Ore algebra $A_K[t; \theta]$; it contains a subring isomorphic to $K[t; \theta] \simeq K\{\tau\}$. Therefore, elements of $K\{\tau\}$—in particular elements ϕ_a, $a \in A$—naturally sit in $A_K[t; \theta]$.

We now define the ideal

$$I(\phi) = \sum_{a \in A} A_K[t; \theta] \cdot (\phi_a - a).$$

In other words, $I(\phi)$ is the left ideal of $A_K[t; \theta]$ generated by the elements $\phi_a - a$ for a running over A.

Lemma 6.2.1 (Lemma 4.3 of [CL23]). *We assume that A is generated as a $\mathbb{F}_q$-algebra by the elements $a_1, \ldots, a_n$. Then $I(\phi)$ is generated as a left ideal of $A_K[t; \theta]$ by $\phi_{a_1} - a_1, \ldots, \phi_{a_n} - a_n$.*

Proof. Let I' be the left ideal of $A_K[t; \theta]$ generated by $\phi_{a_1} - a_1, \ldots, \phi_{a_n} - a_n$. We need to prove that $I' = I(\phi)$. The inclusion $I' \subset I(\phi)$ is obvious. For the reverse inclusion, consider $\lambda \in \mathbb{F}_q$ and $a, b \in A$ such that $\phi_a - a$, $\phi_b - b \in I'$. The equalities

$$\begin{aligned} \phi_{\lambda a} - \lambda a &= \lambda \cdot (\phi_a - a) \\ \phi_{a+b} - (a+b) &= (\phi_a - a) + (\phi_b - b) \\ \phi_{ab} - ab &= \phi_a \cdot (\phi_b - b) + b \cdot (\phi_a - a) \end{aligned}$$

(recall that b is central, so it commutes with ϕ_a) show that the three elements on the left hand side belong to I' as well. This stability property eventually ensures that I' contains all elements of the form $\phi_a - a$. Hence $I(\phi) \subset I'$ as desired. □

We recall from Definition 2.1.9 that the A-motive of ϕ, denoted by $\mathbb{M}(\phi)$, is isomorphic to $K\{\tau\}$ as a K-vector space. This gives a K-linear inclusion $\mathbb{M}(\phi) \to A_K[t;\theta]$ (mapping τ to t). We consider the composite

$$\zeta_\phi : \quad \mathbb{M}(\phi) \quad \to \quad A_K[t;\theta] \quad \to \quad A_K[t;\theta]/I(\phi).$$

Proposition 6.2.2 (Proposition 4.4 of [CL23]). *The map ζ_ϕ is an A_K-linear isomorphism.*

Proof. We first check linearity. Let $\lambda \in K$, $a \in A$ and $f \in \mathbb{M}(\phi)$. By definition, we have $(\lambda \otimes a)\cdot f = \lambda f \phi_a$. Hence

$$\zeta_\phi\left((\lambda \otimes a)\cdot f\right) = \lambda f \phi_a \equiv \lambda f a \pmod{I(\phi)}.$$

Moreover a is a central element in $A_K[t;\theta]$. We conclude that $\zeta_\phi\left((\lambda \otimes a)\cdot f\right) = \lambda a f$ and linearity follows.

In order to prove that ζ_ϕ is an isomorphism, we observe that $A_K[t;\theta] \simeq K\{\tau\} \otimes_{\mathbb{F}_q} A$ and we define the K-linear map $\beta_\phi : A_K[t;\theta] \to K\{\tau\}$ that takes $f \otimes a$ to $f\phi_a$ (for $f \in K\{\tau\}$ and $a \in A$). We claim that β_ϕ vanishes on $I(\phi)$. Indeed, for $a, b \in A$ and $g \in K\{\tau\}$, we have

$$\begin{aligned}\beta_\phi\left((g \otimes b)\cdot(\phi_a \otimes 1 - 1 \otimes a)\right) &= \beta_\phi(g\phi_a \otimes b - g \otimes ab)\\ &= g\phi_a\phi_b - g\phi_{ab} = 0.\end{aligned}$$

Consequently, β_ϕ induces a mapping $\bar{\beta}_\phi : A_K[t;\theta]/I(\phi) \to \mathbb{M}(\phi)$. It is now straightforward to check that $\bar{\beta}_\phi$ is a left and right inverse of ζ_ϕ, showing that ζ_ϕ is an isomorphism. □

We write $\mathrm{Frac}(A_K)$ for the field of fractions of A_K. The morphism θ extends to a ring endomorphism of $\mathrm{Frac}(A_K)$ that, in a slight abuse of notation, we continue to denote by θ. On $\mathrm{Frac}(A_K)$, θ has order d and its fixed subfield is $\mathrm{Frac}(A)$. We consider the Ore polynomial ring $\mathrm{Frac}(A_K)[t;\theta]$. By what we have seen previously, its center is $\mathrm{Frac}(A)[t^d]$ and there is a reduced norm map

$$N_{\mathrm{rd}} : \quad \mathrm{Frac}(A_K)[t;\theta] \quad \to \quad \mathrm{Frac}(A)[t^d].$$

Theorem 6.2.3 (Theorem 4.5 of [CL23]). *We have*

$$\chi(\pi)(t^d) = N_{\mathrm{rd}}\left(g(\phi)\right).$$

Proof. To prove the theorem, we use the framework of Proposition 6.2.2, which is the cornerstone of the proof. We define

$$\mathbb{M}_0(\phi) = \mathrm{Frac}(A_K) \otimes_{A_K} \mathbb{M}(\phi)$$

and

$$I_0(\phi) = \mathrm{Frac}(A_K) \otimes_{A_K} I(\phi),$$

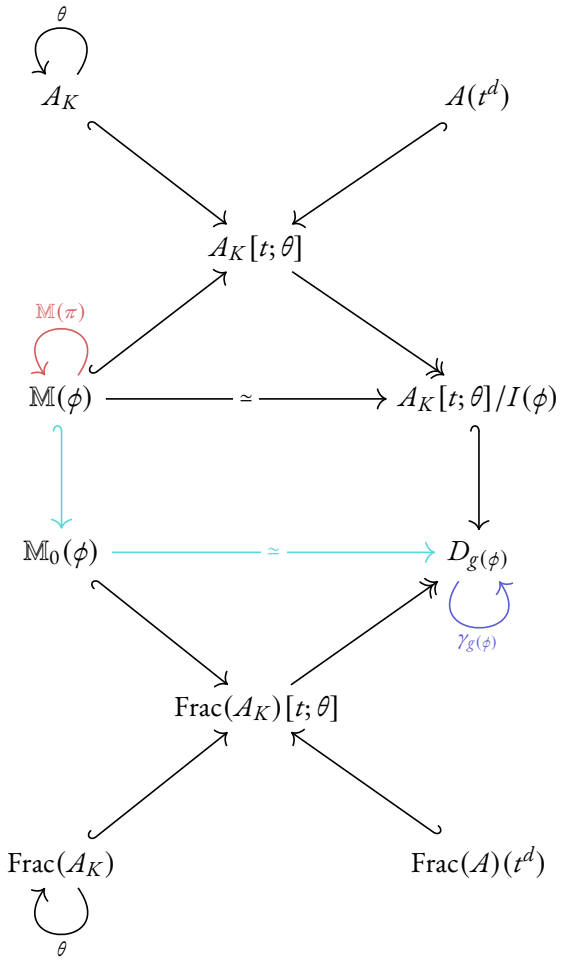
which is a left ideal of $\mathrm{Frac}(A_K)[t;\theta]$. Since the latter is a principal ideal domain, $I_0(\phi)$ is generated by a unique element $g(\phi)$, which we assume to be monic. Concretely $g(\phi)$ is the right gcd of the elements $(\phi_a - a)$ when a varies in A; after Lemma 6.2.1, we even have $g(\phi) = \textsc{rgcd}\left(\phi_{a_1} - a_1, \ldots, \phi_{a_n} - a_n\right)$ as soon as $a_1, \ldots, a_n$ generate A as an $\mathbb{F}_q$-algebra. We may then form the space

$$D_{g(\phi)} = \mathrm{Frac}(A_K)[t;\theta]\,/\,I_0(\phi) = \mathrm{Frac}(A_K)[t;\theta]\,/\,\mathrm{Frac}(A_K)[t;\theta]\cdot g(\phi),$$

which is a $\mathrm{Frac}(A_K)$-vector space. It then follows from Proposition 6.2.2 that ζ_ϕ induces an isomorphism

$$\mathbb{M}_0(\phi) \simeq D_{g(\phi)}.$$

Crucially, it is important to notice that $\mathbb{M}(\pi)$ corresponds (by injection) to an endomorphism of $\mathbb{M}_0(\phi)$, which in turns corresponds to the endomorphism $\gamma_{g(\phi)}$ of multiplication by τ^d (see § 1.1.2) on $D_{\gamma_{g(\phi)}}$. Since extending an endomorphism to the fraction field of A_K does not change its characteristic polynomial, $\chi(\pi)$ is the characteristic polynomial of $\gamma_{g(\phi)}$, which is a polynomial $\chi(\gamma_{g(\phi)})$. The following diagram summarizes the situation:



It then suffices to apply Proposition 1.1.6, which asserts—as $g(\phi)$ is monic—that

$$N_{\mathrm{rd}}(g(\phi)) = \chi(\gamma_{g(\phi)})(t^d).$$

This gives the theorem. □

Remark 6.2.4. When A is $\mathbb{F}_q[T]$, we recover a result given in [Pap23] (see Lemma 4.3.1, Theorems 4.2.2 and 1.7.16, and Equation (4.1.3)). It follows from Lemma 6.2.1 that $g(\phi)$ is $K(T)$-collinear to $\phi_T - T$. Therefore, the reduced norm of $\phi_T - T$ corresponds to the reduced characteristic polynomial of ϕ_T. Let $\chi_{\mathrm{rd}_{\phi_T}}(\tau_K, x) \in \mathbb{F}_q\{\tau_K\}[x]$ be this characteristic polynomial. Then we have shown the polynomials $\chi(\pi)(T, X)$ and $\chi_{\mathrm{rd}_{\phi_T}}(X, T)$ are equal up to a nonzero element in $\mathbb{F}_q$.

6.3 Algorithms

6.3.1 Algorithms for $A = \mathbb{F}_q[T]$

By Theorem 6.2.3, the computation of the characteristic polynomial of π reduces to the computation of a reduced norm. On the other hand, it is a classical fact that the reduced norm of a polynomial $P \in A_K[t;\theta]$ can be computed as a usual norm. Precisely, we consider the subalgebra $A[t]$ of $A_K[t;\theta]$; it is commutative. Moreover $A_K[t;\theta]$ appears as a free left module of rank d over $A[t]$. Thus, there exists a norm map $N_{A_K[t;\theta]/A[t]}$ which takes a polynomial P to the determinant of the $A[t]$-linear endomorphism of

$$\begin{array}{rccc} \mathrm{m}_P : & A_K[t;\theta] & \to & A_K[t;\theta] \\ & Q & \mapsto & QP. \end{array}$$

With this notation, we can define

$$N_{\mathrm{rd}}(P) = N_{A_K[t;\theta]/A[t]}(P) \in A[t].$$

We now assume that A is $\mathbb{F}_q[T]$ and fix a Drinfeld module $\phi : \mathbb{F}_q[T] \to K\{\tau\}$. In that setting, $A_K[t;\theta]$ is isomorphic, as an A_K-algebra, to $K[T]\{\tau\}$, where $\tau\lambda = \lambda^q\tau$ for all λ in K and $\tau T = T\tau$. It follows from Lemma 6.2.1 that $g(\phi)$ is $K(T)$-collinear to $\phi_T - T$. Fix a basis $\mathcal{B} = (e_1, \dots, e_d)$ of K over $\mathbb{F}_q$ and observe that $\mathcal{B}$ is an $\mathbb{F}_q[T]\{\tau\}$-basis of $K[T]\{\tau\}$ as well. Let M be the matrix of m_{ϕ_T} in $\mathcal{B}$. Its entries all lie in $\mathbb{F}_q[t]$ given that ϕ_T has coefficients in K. Observing moreover that $\mathrm{m}_{g(\phi)} = \mathrm{m}_{\phi_T} - \mathrm{m}_T = \mathrm{m}_{\phi_T} - T$, we conclude that

$$\chi(\pi)(t^d) = \chi(M)(T), \tag{6.1}$$

where $\chi(M)$ is the characteristic polynomial of M. We emphasize that the two variables t and T play different roles in the two sides of the Equality (6.1): in the left hand side, t appears in the variable at which the characteristic polynomial is evaluated whereas, in the right hand side, it is an internal variable appearing in the matrix M; and conversely for T.

In order to explicitly compute the matrix of m_P for a given Ore polynomial $P \in K[t;\theta]$, we can proceed as follows. We write $P = g_0 + g_1 t + \cdots + g_n t^n$ ($g_i \in K$) and notice that

$$\mathrm{m}_P = \mathrm{m}_{g_0} + \mathrm{m}_t \circ \mathrm{m}_{g_1} + \cdots + \mathrm{m}_t^n \circ \mathrm{m}_{g_n}.$$

Moreover the set of equalities $e_i t = t e_i^{1/q}$ for $1 \leqslant i \leqslant d$ shows that the matrix of m_t is $t \cdot F^{-1}$ where F is the matrix of the Frobenius endomorphism acting on K (which is $\mathbb{F}_q$-linear). These observations readily lead to Algorithm 8.

Algorithm 8. Matrix-CSA (Algorithm 6 of [CL23])

Input: An Ore polynomial $P = \sum_{i=0}^n g_i \tau^i$ in $K\{\tau\}$, a basis $\mathcal{B} = (e_1, \dots, e_d)$ of K over $\mathbb{F}_q$
Output: The matrix of m_P in the basis $\mathcal{B}$

```
Compute the matrix F ∈ F_q^{d×d} of the Frobenius endomorphism of K, in the basis B;
for 0 ⩽ i ⩽ n do
    Compute the matrix G_i ∈ F_q^{d×d} of the map K → K, x ↦ g_i x in the basis B;
end
return Σ_{i=0}^n F^{-i} · G_i · τ^i ;
```

Lemma 6.3.1 (Lemma 4.7 of [CL23]). *The deterministic Algorithm 8 runs in d applications of the Frobenius endomorphism and $O^{\sim}(nd^{\omega})$ operations in $\mathbb{F}_q$.*

Proof. Since $\mathcal{B}$ is the working basis, writing the coordinates of an element of K in $\mathcal{B}$ costs nothing. Therefore, computing the matrix F amounts to computing each g_i^q for $1 \leqslant i \leqslant d$. This then requires d applications of the Frobenius endomorphism. Similarly computing each G_i requires d multiplications in K, corresponding to $O^{\sim}(d^2)$ operations in $\mathbb{F}_q$. Finally, the last computation requires one inversion and $O(n)$ multiplications of $r \times r$ matrices over $\mathbb{F}_q$. The cost of this computation is then $O^{\sim}(nd^{\omega})$ operations in $\mathbb{F}_q$. □

We now have everything we need to compute the characteristic polynomial of the Frobenius endomorphism: see Algorithm 9.

Algorithm 9. FrobeniusCharacteristicPolynomial-CSA (Algorithm 7 of [CL23])

Input: A Drinfeld $\mathbb{F}_q[T]$-module ϕ
Output: The characteristic polynomial of the Frobenius endomorphism of ϕ
1 Compute M = Matrix-CSA(ϕ_T) ;
2 Compute the characteristic polynomial of M and write it $\sum_{i=0}^{d}(\sum_{j=0}^{r}\lambda_{i,j}\tau^{jd})X^i$;
3 return $\sum_{j=0}^{r}(\sum_{i=0}^{d}\lambda_{i,j}T^j)X^i$;

Theorem 6.3.2 (Variant `F-CSA`; see also Theorem 4.8 of [CL23]). *Recall ϕ is a Drinfeld $\mathbb{F}_q[T]$-module of rank r over K. Assume K is a finite extension of $\mathbb{F}_q$, with degree d over $\mathbb{F}_q$. Using Algorithm 9, and Lemma 4.3.2, the characteristic polynomial of the Frobenius endomorphism of ϕ can be computed (Las Vegas procedure) for an expected cost of $O^{\sim}(d\log^2 q) + O^{\bullet}(rd^{\omega}\log q)$ bit operations.*

Proof. Per Lemma 6.3.1, computing the matrix of m_{ϕ_T} requires $O(d)$ applications of the Frobenius and $O^{\sim}(rd^{\omega})$ operations in $\mathbb{F}_q$. Using Lemma 4.3.2, computing its characteristic polynomial can be achieved for an extra cost of $O^{\sim}(rd^{\omega})$ operations in $\mathbb{F}_q$. All of this corresponds to $O^{\sim}(d\log^2 q) + O^{\bullet}(rd^{\omega}\log q)$ bit operations in our complexity model (see § 1.3). □

6.3.2 Algorithms for generic A

When A is associated to a more general curve than $\mathbb{P}^1(\mathbb{F}_q)$, it is possible to follow the same strategy as before. However several simplifications that were previously applicable cannot be implemented in this case. First of all, finding $g(\phi)$ requires some computation. By Lemma 6.2.1, however, $g(\phi)$ can be obtained as the right gcd of a finite number of Ore polynomials, as soon as we have a finite presentation of the ring A. Fortunately, such a right gcd can be computed using a noncommutative variant of the Euclidean algorithm (see Algorithms 1 and 2). Once $g(\phi)$ is known, one can compute its reduced norm using the method of § 6.3.1: we form the matrix of the $\mathrm{Frac}(A)[t]$-linear map $\mathrm{m}_{g(\phi)} : \mathrm{Frac}(A_K)[t;\theta] \to \mathrm{Frac}(A_K)[t;\theta]$, defined by $Q \mapsto Q{\cdot}g(\phi)$, and view $N_{\mathrm{rd}}(g(\phi))$ as the determinant of $\mathrm{m}_{g(\phi)}$.

This approach yields a working algorithm for computing $\chi(\pi)$. It has nevertheless two drawbacks. First, the computation of the right gcd may be costly and have an impact on the size of the coefficients in the base ring $\mathrm{Frac}(A_K)$, which is not finite. One may gain a certain level of control by using the theory of noncommutative subresultants introduced by Li in [Li98], but this requires additional caution. The second disadvantage is that the Ore polynomial $g(\phi)$ is in general not of the form $\phi_a - a$, implying that

the computation of its reduced norm no longer boils down to finding the characteristic polynomial of a matrix with entries in $\mathbb{F}_q$. Instead, we need to compute the determinant of a general matrix over $\mathrm{Frac}(A)[t]$, which can be a more costly operation.

It turns out that we can overcome these two issues by following the same strategy as in § 5.3.2 and reducing the problem to the case of $\mathbb{F}_q[T]$. For simplicity, we assume again that A is presented as

$$A = \mathbb{F}_q[X, Y]/P(X, Y) \quad \text{with} \quad P \in \mathbb{F}_q[X, Y]$$

and that $\deg(x) > \deg(y)$ where x and y denote the images in A of the variables X and Y. We introduce a new variable Λ and the Ore polynomial ring $K[T, \Lambda][t; \theta]$ where θ acts on K *via* the Frobenius map $x \mapsto x^q$ and acts trivially on T and Λ. In this setting, we have a reduced norm map

$$N_{\mathrm{rd}} : K[T, \Lambda][t; \theta] \to \mathbb{F}_q[T, \Lambda][t^d].$$

We consider the trivariate polynomial $\varpi(T, \Lambda, t^d) = N_{\mathrm{rd}}\left(\phi_x + \Lambda \cdot \phi_y - T\right)$ and write

$$\varpi(x + \Lambda y, \Lambda, t^d) = \varpi_0(t^d) + \varpi_1(t^d) \cdot \Lambda + \cdots + \varpi_n(t^d) \cdot \Lambda^n$$

where the ϖ_i's are univariate polynomials over $\mathrm{Frac}(A)$. This gives the following theorem, which is an analogue of Theorem 5.3.5 and whose proof is similar.

Theorem 6.3.3 (Theorem 4.9 of [CL23])**.** *We keep the previous notation and assumptions. Let π be the Frobenius endomorphism of ϕ and let $\chi(\pi)$ be its monic characteristic polynomial. Then $\chi(\pi)$ equals* $\gcd(\varpi_0, \varpi_1, \ldots, \varpi_n)$.

The formula of Theorem 6.3.3 readily provides an algorithm for computing $\chi(\pi)$. This strategy is not hindered by the two aforementioned disadvantages. Moreover, as mentioned in § 5.3.2, it may occur that $\chi(\pi)$ is already the gcd of the first polynomials $\varpi_0, \ldots, \varpi_i$, for some $i < n$. Therefore, it can be beneficial to compute the ϖ_i's one by one (using relaxed arithmetics), determining the corresponding gcd at each step, and stopping the computation as soon as the resulting polynomial reaches degree d. As also discussed in § 5.3.2, another option is to work with evaluations at random values $\lambda \in \overline{K}$ instead of working with the formal variable Λ.

6.4 Discussion

We now compare many algorithms to compute the characteristic polynomial of the Frobenius endomorphism.

6.4.1 Theoretical asymptotic performance

Contrary to § 4.4 and § 5.4, the base field can only be finite. Therefore, we rather compare algorithms with respect to the rank and the base field. We also distinguish two classes of algorithms: those available for general ranks (§ 6.4.1.1), and those available only in rank two (§ 6.4.1.2), which take inspiration from elliptic curves.

6.4.1.1 In general rank

In general rank, the main algorithms to compute the characteristic polynomial of the Frobenius endomorphisms are:

(i) The algorithms based on crystalline cohomology of [MS23].

(ii) Two variants of Algorithm 6, both based on Anderson motives:

  (a) The variant `F-MFU` (Theorem 4.3.16) uses the Kedlaya-Umans algorithm to compute Frobenius endomorphisms in K.

  (b) The variant `F-MFF` (Corollary 4.3.15) is a direct utilization of Theorem 4.3.13.

(iii) Algorithm 9, denoted `F-CSA`, which express the characteristic polynomial of the Frobenius endomorphism as a reduced norm in a central simple algebra (Theorem 6.3.2).

(iv) An algorithm of [Geko8], originally presented in the rank two case, but generalized and implemented by Musleh for the general case.

In Table 6.1, we observe that no algorithm performs uniformly better than the others: Algorithm 9 seems to be the fastest when $r \gg d$, whereas one should turn to the algorithms of Chapter 4 or [MS23] when $r < d$. As in Table 4.2, the degree m of $\mathfrak{p}$, is taken into account in the analysis of [MS23].

Table 6.1: Algorithms for the characteristic polynomial of the Frobenius endomorphism in any rank r

Algorithm	*Bit complexity*	*Constraints*
[GP20, § 5.1] [1]	$O^{\sim}(r^2 d^3 \log q)$	$m = d$
[MS23, Th. 1(1)] [2]	$O^{\bullet}(r^{\omega} d^{3/2} \log q) + O^{\sim}(d \log^2 q)$	$m = d$
[MS23, Th. 1(2)] [2]	$O^{\bullet}((\frac{r^{\Omega}}{m} + \frac{r^{\omega}}{\sqrt{m}}) d^2 \log q) + O^{\sim}(d \log^2 q)$	$m < d$
[MS23, Th. 2(1)] [♭]	$O^{\bullet}((r^{\Omega} + \min(dr^2, (d+r)r^{\omega-1}))\frac{d(d+m)}{m} \log q) + O^{\sim}(d \log^2 q)$	*None*
[MS23, Th. 2(2)] [♭]	$O^{\bullet}((r^{\Omega}\frac{d(d+m)}{m} + r \cdot \mathrm{SM}^{\geqslant 1}(d+r, d)) \log q) + O^{\sim}(d \log^2 q)$	*None*
Cor. 4.3.15, `F-MFF` [3]	$O^{\bullet}((\mathrm{SM}^{\geqslant 1}(d, d) + rd^2 + dr^{\omega}) \log q) + O^{\sim}(d \log^2 q)$	*None*
Th. 4.3.16, `F-MKU` [4]	$O^{\bullet}((d^2 r^{\omega-1} + dr^{\omega}) \log q) + O^{\sim}(d \log^2 q)$	*None*
Th. 6.3.2, `F-CSA` [5]	$O^{\bullet}(rd^{\omega} \log q) + O^{\sim}(d \log^2 q)$	*None*

[1] Deterministic algorithm by Garai and Papikian. With Proposition 2.1.28 and the hypothesis $m = d$, the coefficients of $\chi(\pi)$ are uniquely determined by their images under $\gamma : \mathbb{F}_q[T] \to K$. The Frobenius norm is computed using Equation (5.2) and the other coefficients are recursively computed.

[2] Two deterministic algorithms by Musleh and Schost. The characteristic polynomial of any endomorphism is the characteristic polynomial of its action on the crystaline cohomology. In the case of the Frobenius endomorphism, algorithmic speed-ups are possible using a *baby step-giant step* method.

[3] Probabilistic algorithm. The characteristic polynomial of the Frobenius endomorphism is the characteristic polynomial of its action on the motive.

[4] Probabilistic algorithm. The characteristic polynomial of the Frobenius endomorphism is the characteristic polynomial of its action on the motive. The corresponding matrix is recursively computed using a *square and multiply*-like procedure.

[5] Probabilistic algorithm. The characteristic polynomial of the Frobenius endomorphism is interpreted as the reduced characteristic polynomial of ϕ_T in the central simple $\mathbb{F}_q[\tau^d]$-algebra $K\{\tau\}$.

[♭] Algorithm described in Table 4.2.

We compare the algorithms of Table 6.1 in Figure 6.1:

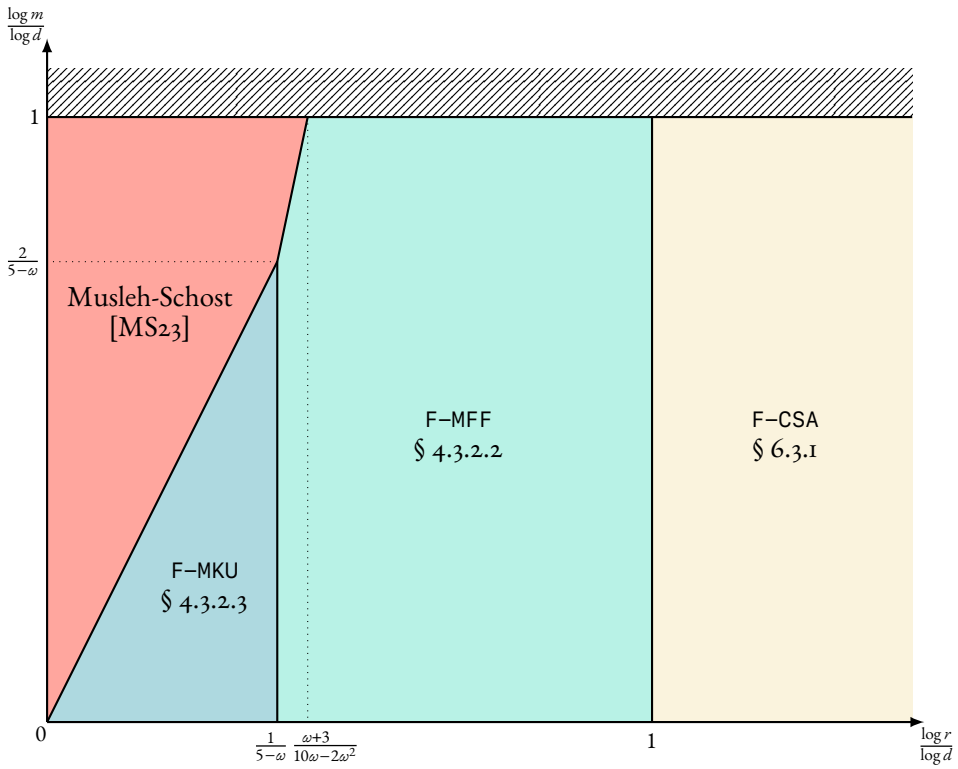


Figure 6.1: The best algorithm for computing the characteristic polynomial of the Frobenius endomorphism, depending on the size of r, d and m. Assumptions: $2 \leqslant \omega \leqslant 3$ and $\omega \leqslant \Omega \leqslant \omega + 1$.

6.4.1.2 In rank two

In the rank two case, a large selection of algorithms is available, due to the inspiration from elliptic curves. We review possible algorithms in Table 6.4.1.2, which is ordered chronologically. In this setting, the general algorithms of § 6.4.1.1 are not the most efficient.

Table 6.2: Algorithms for the characteristic polynomial of the Frobenius endomorphism in rank two

Algorithm	*Bit complexity*	*Constraints*
[Gek08] [1]	$O^\bullet(d^3 \log q) + O^\sim(d \log^2 q)$	*None*
[MS19, § 5] [2]	$O^\bullet(d^{1.885} \log q) + O^\sim(d \log^2 q)$	$m = d$
[MS19, § 7] [3]	$O^\bullet(d^2 \log^2 q)$	*None*
[MS19, § 6] [4]	$O^\bullet(d^2 \log q) + O^\sim(d \log^2 q)$	*None*
[GP20, § 5.1] ♯	$O^\sim(d^3 \log q)$	$m = d$
[DNS21, Th. 1] [5]	$O^\bullet(d^{1.5} \log q) + O^\sim(d \log^2 q)$	$m = d$
[MS23, Th. 1(1)] ♯	$O^\bullet(d^{1.5} \log q) + O^\sim(d \log^2 q)$	$m = d$
[MS23, Th. 1(2)] ♯	$O^\bullet(\frac{d^2}{\sqrt{m}} \log q) + O^\sim(d \log^2 q)$	$m < d$
[MS23, Th. 2(1)] ♭	$O^\bullet(d^2 \frac{d+m}{m} \log q) + O^\sim(d \log^2 q)$	*None*
[MS23, Th. 2(2)] ♭	$O^\bullet(\mathrm{SM}^{\geqslant 1}(d, d) \log q) + O^\sim(d \log^2 q)$	*None*
Cor. 4.3.15, `F-MFF` ♯	$O^\bullet(\mathrm{SM}^{\geqslant 1}(d, d) \log q) + O^\sim(d \log^2 q)$	*None*
Th. 4.3.16, `F-MKU` ♯	$O^\bullet(d^2 \log q) + O^\sim(d \log^2 q)$	*None*
Th. 6.3.2, `F-CSA` ♯	$O^\bullet(d^\omega \log q) + O^\sim(d \log^2 q)$	*None*

[1] Deterministic algorithm by Gekeler. The Frobenius norm is directly computed, and the Frobenius trace is computed as the solution of a linear system. See also [MS19, § 4.1].

[2] Monte-Carlo algorithm by Musleh and Schost. The algorithm is inspired by ideas from ideas of Narayanan in [Nar18, § 3.1], as well as Copersmith's block Wiedemann algorithm.

[3] Monte-Carlo algorithm by Musleh and Schost. The algorithm computes the Frobenius norm, and the minimal polynomial of ϕ_T using a Monte-Carlo algorithm. After, it recovers $\chi(\pi)$ by solving a Hankel system.

[4] Deterministic algorithm by Musleh and Schost. Drinfeld analogue of Schoof's algorithm for elliptic curves.

[5] Deterministic Algorithm by Doliskani, Narayanan and Schost, introduced to factorize polynomials in $\mathbb{F}_q[T]$. The algorithm actually computes the *Hasse invariant* of the Drinfeld module, from which the Frobenius trace is recovered thanks to the assumption that $m = d$. The algorithm gets inspiration from elliptic curve algorithms and computes the Hasse invariant as an element in a recursive sequence discovered by Gekeler. See [DNS21, § 2.1].

♯ Algorithm described in Table 6.1.

♭ Algorithm described in Table 4.2.

6.4.2 Benchmarks

All algorithms of § 6.4.1.1 are implemented. The benchmarks parameters are the same as that of § 4.4.2, and we recall Remark 4.4.2.

The rudimentary benchmarks of Figure 6.2 corroborate the comparison between the algorithms of Figure 6.1: when r is large, Algorithm `F-CSA` is the best, whereas when d is large, the algorithm of [MS23] is. For this reason, and as mentioned in § 3.2.3.4, the method `frobenius_charpoly` automatically picks the best algorithm, depending on the input.

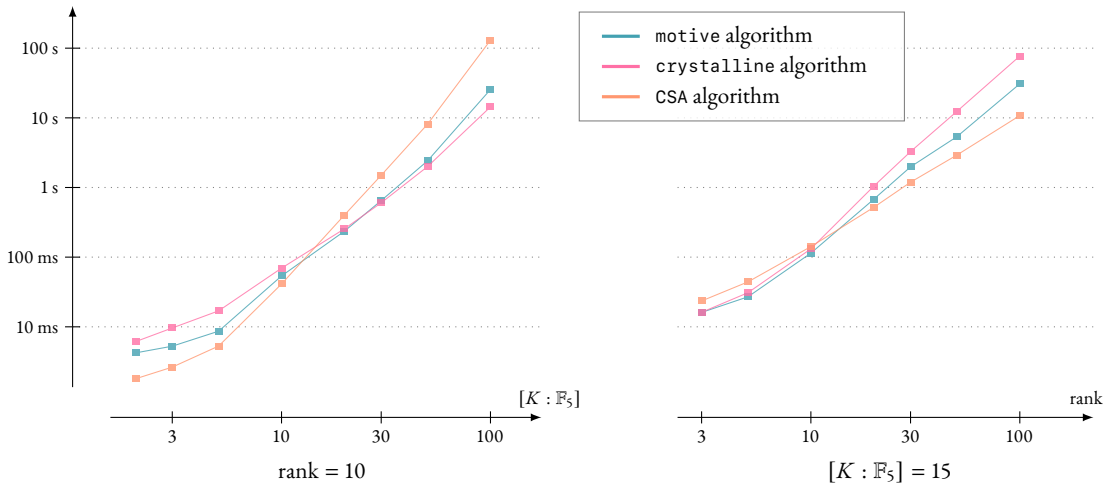


Figure 6.2: Timings for the computation of the characteristic polynomial of the Frobenius endomorphism. (Figure 1 of [Ayo+23]. CPU: Intel Core i5-8250U at 1.60GHz; OS: Ubuntu 22.04.1.)

Chapter 7
Computing a group action from class field theory

In this chapter, we efficiently compute a group action that appears in the class field theory of function fields. This group action is defined in terms of Drinfeld modules, and we focus on the case where the function field is hyperelliptic and imaginary, and the Drinfeld modules are ordinary with rank two. This group action is the function field analogue of the action used by Couveignes [Cou06] and Rostovtsev-Stolbunov [RS06] in the CRS cryptosystem. Our algorithm and its implementation lead to a much faster construction, but that is not secure.

Joint-work with Pierre-Jean Spaenlehauer. See [LS24].

7.1 Overview

In this chapter, we are interested in the efficient computation of an important group action from the class field theory of function fields. Let A and K be as in § 2.2, and consider a Drinfeld A-module ϕ over K. Elements of A correspond to endomorphisms of ϕ, by considering the injection

$$\begin{array}{ccc} A & \to & \mathrm{End}(\phi) \\ a & \mapsto & \phi_a. \end{array}$$

One of the aims of this chapter is to define isogenies that are not endomorphisms in terms of elements of A. Given than one element of A defines an endomorphism, we have to consider several elements, and turn to ideals $\mathfrak{a}$ of A. Consider the Ore polynomial $u_{\mathfrak{a}}$ of $K\{\tau\}$ defined by

$$u_{\mathfrak{a}} = \mathrm{RGCD}(\{\phi_a : a \in \mathfrak{a}\}),$$

which is proven to define an isogeny from ϕ, to a second Drinfeld A-module ψ over K. This Drinfeld module can easily be computed: if $a_1, \dots, a_\ell$ is a system of generators of A (as an $\mathbb{F}_q$-algebra), the generators $\psi_{a_1}, \dots, \psi_{a_\ell}$ of ψ are the remainders of the Ore right-Euclidean divisions of $u_{\mathfrak{a}}\phi_{a_i}$ by $u_{\mathfrak{a}}$, for all $1 \leqslant i \leqslant \ell$, respectively (see also Remark 7.1.1). We thus define the map $*_K$ by

$$\mathfrak{a} *_K \phi = \psi.$$

The map $*_K$ is a central object of our work. If $\mathfrak{a}$ is principal, then $u_{\mathfrak{a}}$ is an endomorphism generated, up to $\overline{K}$-isomorphism, by any generator of $\mathfrak{a}$, and ϕ equals ψ. For any nonzero d in A, $\frac{\mathfrak{a}}{d}$ is a fractional ideal, and we define

$$\frac{\mathfrak{a}}{d} *_K \phi = \mathfrak{a} *_K \phi,$$

We thus extend $*_K$ to a group action from the class group $\mathrm{Cl}(A)$ of A (recall that A is a Dedekind domain) to the set $\mathrm{Dr}_r^\circ(A, K)$ of $\overline{K}$-isomorphism classes of rank r Drinfeld A-modules over K:

$$*_K : \quad \mathrm{Cl}(A) \times \mathrm{Dr}_r^\circ(A, K) \quad \to \quad \mathrm{Dr}_r^\circ(A, K).$$

In a slight abuse of notation, this group action is still denoted $*_K$.

One can also consider the following definition. Here, we need to assume that $\mathrm{End}(\phi)$ is commutative, which will be the case in our work. Let ϕ be a Drinfeld A-module over K, of rank r. To an ideal $\mathfrak{a}$ of $\mathrm{End}(\phi)$, one associates—as previously—the Ore polynomial

$$u_{\mathfrak{a}} = \mathrm{RGCD}(\{\phi_a : a \in \mathfrak{a}\}),$$

which is also proven to define an isogeny. If $\mathfrak{a}$ is principal, $u_{\mathfrak{a}}$ is the endomorphism, also up to K-isomorphism, defined by any generator of $\mathfrak{a}$. Assuming $\mathrm{Cl}(\mathrm{End}(\phi))$ is a well-defined object (see Remark 7.1.3), we then proceed to define a group action from $\mathrm{Cl}(\mathrm{End}(\phi))$ to the sets of isomorphism classes of Drinfeld modules that are K-isogenous to ϕ. If K is a finite field, these are exactly the Drinfeld modules that have the same characteristic polynomial of the Frobenius endomorphism as ϕ (Theorem 2.1.26).

Remark 7.1.1. Notice that in both cases, $u_{\mathfrak{a}}$ is defined in terms of Ore polynomials, even though the group action can also be defined in terms of their kernels. If $\mathfrak{a}$ is in $\mathrm{End}(\phi)$, it is also possible to consider

$$R_{\mathfrak{a}} = \bigcap_{a \in \mathfrak{a}} \mathrm{Ker}(a),$$

the intersection of kernels of endomorphisms in A. It is a finite subspace of $\mathbb{E}(\phi)$, and the polynomial

$$\prod_{z \in R_{\mathfrak{a}}} (X - z) \in K[X]$$

is a q-polynomial that defines a monic Ore polynomial $u_{\mathfrak{a}}$ (Proposition 2.1.33). In virtue of Theorem 2.1.33, $u_{\mathfrak{a}}$ defines an isogeny on ϕ, which is exactly $u_{\mathfrak{a}}$ (Proposition 1.1.5). That being said, the equivalence between Ore polynomials of $K\{\tau\}$ and finite sub-$\mathbb{F}_q$-vector spaces of $\overline{K}$ allows to directly work with Ore polynomials, which completely bypasses the need to manipulate any kernel element. Indeed, provided that $\mathfrak{a}$ is given by a finite number of generators $a_1, \ldots, a_\ell$, computing the action then simply amounts to computing the images $\phi_{a_1}, \ldots, \phi_{a_\ell}$ and the Ore right-Euclidean divisions of $u_{\mathfrak{a}}\phi_{a_i}$ by $u_{\mathfrak{a}}$, for all $a_1, \ldots, a_\ell$. It is a fact of exceptional convenience that isogenies of Drinfeld modules live in an ambient space whose arithmetic is inherently compatible with the arithmetic of kernels of isogenies (see *e.g.* Proposition 1.1.5 or Lemma 7.3.4). It seems that no such space exists for isogenies of elliptic curves. In fact, a similar action exists for elliptic curves, and it is indeed defined in terms of kernels [Cou06; RS06]. Computation times are rather long; the bottleneck lies in the manipulation of torsion elements that live in possibly large extensions of the ground field [DKS18],

Remark 7.1.2. Following Remark 7.1.1, we draw our attention to the representation of ℓ-isogenies of elliptic curves (where ℓ is an integer), and then of Drinfeld modules (where ℓ is a polynomial).

(i) If ℓ is a positive integer, an ℓ-isogeny of $\mathbb{F}_q$-elliptic curves can be represented by a polynomial with $\frac{\ell-1}{2}$ coefficients, *i.e.* by $O(\ell)$ elements. If, for example, ℓ splits as $\ell = 2^m$, for some m, then the isogeny splits as a factor of m 2-isogenies; it can subsequently be rapidly evaluated using the Vélu formulae [Vél71; Ber+20]. However, if ℓ is a large prime, then the isogeny cannot be factored as a product of 2-isogenies, which makes its evaluation very challenging.

(ii) For Drinfeld modules, an isogeny with τ-degree n is represented by $n+1$ coefficients. But, while the τ-degree is an obvious candidate to measure the size of an isogeny, it may not be the most compelling one, as already discussed in § 2.1.8. In rank two, the norm of the isogeny, as in Definition 2.1.35, is generated by a polynomial $\ell \in \mathbb{F}_q[T]$, whose degree (in T) is exactly n. Going back to the setting of Drinfeld modules, we had endowed $\mathbb{F}_q(T)$ with its valuation at infinity. This valuation actually occupies a key place in the theory of Drinfeld modules, especially in the context of general function rings A, where definitions cannot be reduced to classical considerations on polynomials. Also, this valuation gives a norm $|\cdot|_\infty$, which is such that

$$|\ell|_\infty = q^n.$$

The τ-degree of an isogeny is thus logarithmic in the norm at infinity of its isogeny norm. So is thus the size of the representation of the isogeny. To conclude, depending on the metric, representation of ℓ-isogenies of Drinfeld modules are arguably—and relatively—more compact than their elliptic curve counterparts.

Remark 7.1.3. For this remark, let us assume that ϕ has rank two. If $\mathrm{End}(\phi)$ is a Dedekind domain, then its *class group*, denoted $\mathrm{Cl}(\mathrm{End}(\phi))$ is classically defined as the quotient of the nonzero fractional ideals of $\mathrm{End}(\phi)$ by the subgroup of nonzero principal fractional ideals. However, $\mathrm{End}(\phi)$ is a Dedekind domain if and only if it is the maximal order of its associated quadratic function field, as per § 2.1.5. If it is an order that is not maximal, one has to consider a subclass of ideals, called *proper ideals*. We refer to [Car18, § 3.4] for a precise construction.

If $\mathrm{End}(\phi)$ equals A, then $\mathrm{Cl}(\mathrm{End}(\phi))$ is well-defined and the actions of $\mathrm{Cl}(\mathrm{End}(\phi))$ and $\mathrm{Cl}(A)$ are the same, in which case, both are denoted $*_K$. As discussed, $\mathrm{End}(\phi)$ always contains a copy of A, but when K is finite and $A = \mathbb{F}_q[T]$, it is strictly larger than $\mathbb{F}_q[T]$, as it also contains the Frobenius endomorphism. Proposition 7.2.4 establishes an equivalence between two categories of Drinfeld modules that allows to work with both incarnations of $*_K$ at the same time.

It is also natural to ask whether the action $*_K$ is free and transitive, *i.e.* asking first if two Drinfeld modules ϕ and ψ, up to $\overline{K}$-isomorphisms, can be related by an ideal $\mathfrak{a}$ of A such that $\mathfrak{a} *_K \phi$ equals ψ, and second if the ideal $\mathfrak{a}$ is unique up to principal ideals. When A is $\mathbb{F}_q[T]$, the action is not transitive, as there are multiple isogeny classes (assuming that $K \neq \mathbb{F}_2$). Indeed: two Drinfeld $\mathbb{F}_q[T]$-modules are isogenous if and only if they have the same characteristic polynomial of the Frobenius endomorphism (Theorem 2.1.26), and the formula for a_0 in Lemma 2.1.28 implies that there are multiple polynomials of $\mathbb{F}_q[T][X]$ that appear as the characteristic polynomial of the Frobenius endomorphism of some Drinfeld module in $\mathrm{Dr}_r(\mathbb{F}_q[T], K)$. Does the action then become transitive when only considering $\overline{K}$-isomorphism classes of Drinfeld $\mathbb{F}_q[T]$-modules that are isogenous? In the setting that we later choose, yes. We also notice that to make the action transitive, one may restrict the number of isomorphism classes of Drinfeld modules. By focusing on rank one, and Drinfeld modules over a general function ring A, more constraints are added to the possible generators of ϕ: they ought to satisfy the equation that defines the curve behind A. This path leads to the following, fundamental result of the theory of Drinfeld modules:

Theorem 7.1.4 ([Hay11, Theorem 9.3])**.** *Let C be the $\mathbb{F}_q$-curve whose coordinate ring is $A_C = A$. Let ∞ be the distinguished point on C. Let $\mathbb{R}_C$ be the completion of $\mathbb{F}_q(C)$ with respect to the valuation at infinity, and let $\mathbb{C}_C$ be the completion of an algebraic closure of $\mathbb{R}_C$. Then the group action*

$$*_{\mathbb{C}_C} : \quad \mathrm{Cl}(A_C) \times \mathrm{Dr}_1^\circ(A_C, \mathbb{C}_C) \quad \to \quad \mathrm{Dr}_1^\circ(A_C, \mathbb{C}_C)$$

if free and transitive. We say that $\mathrm{Dr}_1^\circ(A_C, \mathbb{C}_C)$ *is a* principal homogeneous space *for* $\mathrm{Cl}(A_C)$*, meaning that the action is free and transitive.*

Multiple things have to be done in order to make this theorem—a function field analogue of [Sil94, Proposition 2.4, Lemma 2.5.1]—effective.

(i) Algorithmically, $\mathbb{C}_C$ is a very complicated object. In its simplest incarnation—when C is the projective line—$\mathbb{R}_\infty$ can be described as the ring $\mathbb{F}_q[[1/T]]$ of Laurent series in $1/T$, but no practical representations are known for elements in $\mathbb{C}_\infty$. We bypass this problem by considering a reduction of the action of Theorem 7.1.4 from $\mathbb{C}_C$ to a finite field K, using the reduction and lifting theory of Drinfeld modules. This is Theorem 7.2.9.

(ii) It is also not obvious how to describe $\mathrm{Cl}(A_C)$. For that, we consider the case where $C = \mathcal{H}$ is an imaginary hyperelliptic curve (§ 1.2.4), in which case $\mathrm{Cl}(A_C)$ can be represented with Mumford coordinates (§ 1.2.4.3).

(iii) A last problem is the manipulation of rank one Drinfeld A_C-modules, as opposed to Drinfeld $\mathbb{F}_q[T]$-modules. Recall that Drinfeld $\mathbb{F}_q[T]$-modules are simply determined by a single Ore polynomial, corresponding to the image of T. On the other hand, Drinfeld A_C-modules are usually described by multiple Ore polynomials which need to commute with one another, and, on top of that, which must verify the algebraic equation defining C. However, in the following situation, describing Drinfeld A_C-modules is easier: when a rank two Drinfeld $\mathbb{F}_q[T]$-module whose characteristic polynomial of the Frobenius endomorphism defines C, is known. In that case, C is a plane curve, A_C is generated as an $\mathbb{F}_q$-algebra by elements $\overline{X}$ and $\overline{Y}$, and the Ore polynomials $\psi_{\overline{T}} = \phi_T$ and $\psi_{\overline{X}} = \tau_K$ define a rank one Drinfeld $A_{\mathcal{H}}$-module. Proposition 7.2.4 establishes that this association leads to an equivalence of categories, provided that $C = \mathcal{H}$ is an imaginary hyperelliptic curve.

Those ideas, put together, lead to a concise and fast algorithm (see Algorithm 10, Proposition 7.3.1, and Proposition 7.3.2) to compute the group action, as defined by Theorem 7.2.9. The group action we consider is free and transitive, and we also provide algorithms that *invert* the action: given any two Drinfeld modules ϕ and ψ, we efficiently recover the ideal (up to principal ideals) $\mathfrak{a}$ of $A_{\mathcal{H}}$ such that $\mathfrak{a} *_K \phi$ equals ψ (Algorithm 12, Proposition 7.3.7, and Proposition 7.3.8). In § 7.4, we describe a practical implementation of Algorithm 10, that runs in milliseconds on inputs with cryptographic size.

Notations for the chapter

As usual, $\mathbb{F}_q$ is a finite field with q elements. We let d be an odd integer and m be a positive divisor of d. We let $p \in \mathbb{F}_q[T]$ be a monic and irreducible polynomial of degree d/m, and the ideal (p) is denoted by $\mathfrak{p}$. We fix K, an extension of $\mathbb{F}_q[T]/\mathfrak{p}$ with degree m, so that K has degree d over $\mathbb{F}_q$. We thus have a morphism

$$\gamma : \mathbb{F}_q[T] \to \mathbb{F}_q[T]/\mathfrak{p} \to K$$

from $\mathbb{F}_q[T]$ to K whose kernel is $\mathfrak{p}$.

We now let $\chi_{\mathcal{H}}$ be a polynomial in $\mathbb{F}_q[T][X]$ that has the following form:

$$\chi_{\mathcal{H}} = X^2 + h(T)X - f(T),$$

where f equals αp^m for some nonzero α in $\mathbb{F}_q$ and h is a polynomial with degree $\leqslant d/2$ that is not a multiple of p. The curve $\mathcal{H}$ defined by χ_H may have singularities, but if the discriminant of χ_H (with respect to X) is squarefree, then $\mathcal{H}$ is smooth in the affine plane, and as such, is an imaginary hyperelliptic curve over $\mathbb{F}_q$ (§ 1.2.4). Furthermore, Lemma 2.1.28 implies that the characteristic polynomial of the Frobenius endomorphism of an ordinary rank two Drinfeld $\mathbb{F}_q[T]$-module over K verifies the same degree bounds as $\chi_{\mathcal{H}}$.

We then let

$$A_{\mathcal{H}} = \mathbb{F}_q[T][X]/(\chi_{\mathcal{H}})$$

be the coordinate ring of $\mathcal{H}$, and $\mathbb{F}_q(\mathcal{H})$ be the function field of $\mathcal{H}$, which is isomorphic to the fraction field of $A_{\mathcal{H}}$. We now let $\mathfrak{p}_{\mathcal{H}}$ denote the ideal of $A_{\mathcal{H}}$ generated by the classes of p and X. This ideal is prime, and $\mathbb{F}_q[T]/\mathfrak{p}$ and $A_{\mathcal{H}}/\mathfrak{p}_{\mathcal{H}}$ are isomorphic $\mathbb{F}_q$-algebras. We thus equip K with a second structural morphism

$$\gamma_{\mathcal{H}} : A_{\mathcal{H}} \to A_{\mathcal{H}}/\mathfrak{p}_{\mathcal{H}} \to K,$$

whose kernel is exactly $\mathfrak{p}_{\mathcal{H}}$.

We then recall that $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$ is the category of rank one Drinfeld $A_{\mathcal{H}}$-modules over K, that $\mathrm{Dr}_2(\mathbb{F}_q[T], K)$ is the category of rank two Drinfeld $\mathbb{F}_q[T]$-modules over K, and that $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$ is the subcategory in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)$ whose objects have a characteristic polynomial of the Frobenius endomorphism equal to $\chi_{\mathcal{H}}$. It is implicit that $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$ is defined with respect to $\gamma_{\mathcal{H}}$ and that $\mathrm{Dr}_2(\mathbb{F}_q[T], K)$ and $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$ are defined with respect to γ. We stress that $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$ may be empty, meaning that no Drinfeld module in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)$ has $\chi_{\mathcal{H}}$ as characteristic polynomial of the Frobenius endomorphism. We therefore have to assume that $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_H}$ is nonempty.

Remark 7.1.5. A rank two Drinfeld $\mathbb{F}_q[T]$-module over K, whose characteristic polynomial of the Frobenius endomorphism is $\chi_{\mathcal{H}}$, may not be supersingular. This is guaranteed by our hypothesis on h, which would contradict Proposition 2.1.25.

Remark 7.1.6. In § 2.2.1.1, we impose the base curve of a Drinfeld module to be smooth. However, an imaginary hyperelliptic curve over $\mathbb{F}_q$ is not: its unique point at infinity is singular, and its unique singularity. This bears no consequence, as we have defined function fields with respect to affine curves (§ 1.2.1.3 and § 1.2.2.5), and that the affine part of $\mathcal{H}$ is smooth. If $\mathcal{H}$ were to be real hyperelliptic, it would still have a unique place at infinity, which would desingularize to two distinct points, which would both be singular; adapting the definition of Drinfeld modules for this curve would likely be significantly more technical.

7.2 Theoretical preliminaries

We prove all necessary results to compute the group action. First of all, we describe the endomorphism ring of our Drinfeld modules as $A_{\mathcal{H}}$ (Proposition 7.2.1), and then establish a correspondence which allows to manipulate rank two Drinfeld $\mathbb{F}_q[T]$-modules rather than rank one Drinfeld $A_{\mathcal{H}}$-modules (Proposition 7.2.4). The question of data representation is investigated in § 7.2.4.

7.2.1 Description of the endomorphism ring

Having assumed that $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$ contains at least one object ϕ, it is legitimate to ask whether $\mathrm{End}(\phi)$ contains only $\mathbb{F}_q[T][\pi]$, where π is the Frobenius endomorphism of ϕ, or if it is strictly larger.

The ring $\mathbb{F}_q[T][\pi]$ is no other than $A_{\mathcal{H}}$. Indeed, as it has degree two, the characteristic polynomial $\chi_{\mathcal{H}} = \chi(\pi)$ of π is also its minimal polynomial (otherwise, π would equal ϕ_a for some a in $\mathbb{F}_q[T]$, as noticed in [Gek91, Lemma 3.3]). Therefore, the kernel of the map

$$\begin{array}{rcl} \mathbb{F}_q[T][X] & \to & \mathrm{End}(\phi) \\ P(T,X) & \mapsto & P(\phi_T, \pi) \end{array}$$

is exactly the ideal generated by $\chi_{\mathcal{H}}$. This leads to an injection

$$\begin{array}{rcl} A_{\mathcal{H}} & \to & \mathrm{End}(\phi) \\ \overline{P}(T,X) & \mapsto & P(\phi_T, \pi). \end{array}$$

By definition, the function field of $\mathcal{H}$—the fraction field of $A_{\mathcal{H}}$—is an imaginary hyperelliptic function field. As a consequence, all its $\mathbb{F}_q[T]$-orders are ordered for the inclusion relation; among them, only the maximal order is a Dedekind domain. As $\mathcal{H}$ is smooth in the affine plane, its coordinate ring $A_{\mathcal{H}}$ is a Dedekind domain, and it is therefore the integral closure of $\mathbb{F}_q[T]$ in $\mathbb{F}_q(\mathcal{H})$, and the maximal order of $\mathbb{F}_q(\mathcal{H})$ [Lor96, Chapter 5, Theorem 10.8]. On the other hand, $\mathrm{End}(\phi)$ is also an order in $\mathrm{End}^\circ(\phi)$, the algebra of endomorphisms of ϕ, which is an imaginary quadratic function field (see § 2.1.5). As $\mathrm{End}(\phi)$ contains a copy of $A_{\mathcal{H}}$, these quadratic function fields must be isomorphic, and therefore, $\mathrm{End}(\phi)$ and $A_{\mathcal{H}}$ are equal, up to isomorphism of $\mathbb{F}_q[T]$-algebras. This is formalized in the proof of Proposition 7.2.1. Recall that $\mathrm{End}_{\overline{K}}(\phi)$ is the ring of endomorphisms of ϕ that are defined over $\overline{K}$.

Proposition 7.2.1 (Proposition 2.2 of [LS24])**.** *The $\mathbb{F}_q[T]$-algebras $\mathrm{End}_{\overline{K}}(\phi)$, $\mathrm{End}(\phi)$ and $A_{\mathcal{H}}$ are isomorphic.*

Proof. We first prove that $A_{\mathcal{H}}$ is maximal. Let O be an order in $\mathbb{F}_q(\mathcal{H})$. Since the canonical field extension $\mathbb{F}_q(T) \to \mathbb{F}_q(\mathcal{H}) = \mathrm{Frac}(A_{\mathcal{H}})$ has degree 2, O must be a rank 2 $\mathbb{F}_q[T]$-module. Let $(1, \alpha)$ be an $\mathbb{F}_q[T]$-basis of O. Then, α^2 equals $a + b\alpha$, for some a and b in $\mathbb{F}_q[T]$, which implies that α belongs to $A_{\mathcal{H}}$, the integral closure of $\mathbb{F}_q[T]$ in $\mathbb{F}_q(\mathcal{H})$. This implies that O is in $A_{\mathcal{H}}$, and that $A_{\mathcal{H}}$ is maximal.

We now prove that $A_{\mathcal{H}}$ and $\mathrm{End}(\phi)$ are isomorphic. Since π is not in the image of the map $g \mapsto \phi_g$, $\mathbb{F}_q[\phi_T, \pi] \subset \mathrm{End}_K(\phi)$ is a rank two $\mathbb{F}_q[T]$-module in $\mathrm{End}^\circ(\phi) = \mathrm{End}_K(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T)$, the algebra of endomorphisms of ϕ (see § 2.1.5); $\mathrm{End}^\circ(\phi)$ is an imaginary quadratic function field containing $\mathrm{End}(\phi)$ as an order. Therefore, as $A_{\mathcal{H}}$ and $\mathrm{End}(\phi)$ are two orders in a quadratic imaginary function field and $\mathrm{End}(\phi)$ contains $A_{\mathcal{H}}$, these quadratic imaginary function fields are the same. As $A_{\mathcal{H}}$ is maximal, it is necessary that $A_{\mathcal{H}}$ equals $\mathrm{End}(\phi)$.

It remains to prove that $\mathrm{End}_{\overline{K}}(\phi)$ equals $\mathrm{End}(\phi)$. For any finite extension L of K, by [Car18, Theorem 6.4.2.(iii)], $\mathrm{End}(\phi)$ is a sub-order of $\mathrm{End}_L(\phi)$. As $\mathrm{End}(\phi)$ is maximal, $\mathrm{End}(\phi) = \mathrm{End}_L(\phi)$. □

7.2.1.1 Absolute isomorphisms and rational isogenies

The following lemma will be used later. We recall that two rank two Drinfeld $\mathbb{F}_q[T]$-modules are

(i) $\overline{K}$-isomorphic if and only if they have the same j-invariant,

(ii) K-isogenous if and only if they have the same characteristic polynomial of the Frobenius endomorphism.

Lemma 7.2.2 (proposition 2.3 of [LS24])**.** *Two ordinary rank two Drinfeld $\mathbb{F}_q[T]$-modules defined over K are K-isomorphic if and only if they are K-isogenous and $\overline{K}$-isomorphic.*

Proof. Let ϕ and ψ be two K-isogenous and $\overline{K}$-isomorphic Drinfeld modules. Let $\lambda : \phi \to \psi$ be a $\overline{K}$-isomorphism and $u : \phi \to \psi$ be a K-isogeny, then $\lambda^{-1}u$ is a $\overline{K}$-endomorphism of ϕ. By Proposition 7.2.1, $\mathrm{End}_{\overline{K}}(\phi)$ equals $\mathrm{End}_K(\phi)$. Therefore, $\lambda^{-1}u$ is in $K\{\tau\}$, and λ is in K. The reciprocal is staightforward: a K-isomorphism is both a K-isogeny and a $\overline{K}$-isomorphism. □

Remark 7.2.3. Lemma 7.2.2 is an analogue for Drinfeld modules of a classical property of endomorphism rings of ordinary elliptic curves defined over finite fields (see [Cox22, Proposition 4.19] or [Bab+20, Theorem 3.3]). We also notice that the representation of isogenies and isomorphisms as Ore polynomials makes the proof relatively easy.

Throughout this thesis and unless stated otherwise, isogenies are K-isogenies and Drinfeld modules are called isogenous if they are K-isogenous.

7.2.2 A correspondence of Drinfeld modules

As mentioned in § 7.1, our goal is now to prove the following correspondence:

Proposition 7.2.4 (Proposition 2.4 of [LS24])**.** *The categories* $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$ *and* $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$ *are equivalent under the following functor. For objects, we map:*

$$\begin{array}{rcl} \mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}} & \to & \mathrm{Dr}_1(A_{\mathcal{H}}, K) \\ \phi & \mapsto & \overline{a}(T, X) \mapsto a(\phi_T, \tau_K). \end{array}$$

And to a morphism of Drinfeld modules in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$*, we associate the morphism defined by the same Ore polynomial.*

Proposition 7.2.4 is key in proving Theorem 7.2.9. It also helps working with Drinfeld $\mathbb{F}_q[T]$-modules instead of Drinfeld A-modules. Its proof is postponed to the end of this section, as we first need to describe the objects in $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$.

Remark 7.2.5. Proposition 7.2.4 sheds light on another key difference between Drinfeld modules and elliptic curves. If ϕ is a Drinfeld $\mathbb{F}_q[T]$-module over K, then $\overline{K}$ is a module over $\mathbb{F}_q[T]$, which we have denoted by $\mathbb{E}(\phi)$ (Definition 2.1.8). Evidently, $\overline{K}$ can also be seen also a module over $\mathrm{End}(\phi)$ via

$$\begin{array}{rcl} \mathrm{End}(\phi) \times \overline{K} & \to & \overline{K} \\ (u, z) & \mapsto & u(z). \end{array}$$

This module is

$$\mathrm{End}(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{E}(\phi).$$

The question we ask now is: can $\mathrm{End}(\phi) \otimes_{\mathbb{F}_q[T]} \mathbb{E}(\phi)$ be described as $\mathbb{E}(\psi)$, for another Drinfeld module ψ? Proposition 7.2.4 affirms so, at least in our case. The key is that the definition of Drinfeld modules allows general function rings and arbitrary ranks. As $\mathrm{End}(\phi)$ is isomorphic to $A_{\mathcal{H}}$, we could consider rank one Drinfeld $A_{\mathcal{H}}$-modules in parallel with rank two Drinfeld $\mathbb{F}_q[T]$-modules, giving the desired interpretation.

This does not *a priori* occur with elliptic curves. If E is an elliptic curve over $\mathbb{F}_q$, one can consider $\mathrm{End}(E) \otimes E(\overline{\mathbb{F}_q})$. Here, $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, and is isomorphic to an order O in an imaginary quadratic field if E is ordinary. However, as E are only abelian groups, we cannot describe $\mathrm{End}(E) \otimes E(\overline{\mathbb{F}_q})$ as the "O-module associated to an O-elliptic curve".

Lemma 7.2.6 (Lemma 2.5 of [LS24]). *Any rank one Drinfeld $A_{\mathcal{H}}$-module ψ over K has the following form:*

$$\begin{cases} \psi_{\overline{T}} = \gamma_{\mathcal{H}}(\overline{T}) + g\tau + \Delta\tau^2, \\ \psi_{\overline{X}} = \beta\tau_K, \end{cases}$$

where $\Delta \in K^\times$, $g \in K$, and $\beta \in \mathbb{F}_q{}^\times$. Moreover, β is a nonzero square root of $\alpha\,\mathrm{N}_{K/\mathbb{F}_q}(\Delta)$, and β is uniquely determined by Δ and g. (Recall from § 7.1 that α is such that $\chi_{\mathcal{H}} = X^2 + h(T)X - f$ and $f = \alpha p^m$.)

Proof. Let ψ be a rank one Drinfeld $A_{\mathcal{H}}$-module over K. Since $\overline{T}$ has degree two in $A_{\mathcal{H}}$ and ψ has rank one, $\psi_{\overline{T}}$ must be an Ore polynomial of τ-degree two. Therefore, $\psi_{\overline{T}} = \gamma(\overline{T}) + g\tau + \Delta\tau^2$ for some $\Delta \in K^\times$, $g \in K$.

Next, we show that $\psi_{\overline{X}}$ equals $\beta\tau_K$ for some β in $\mathbb{F}_q{}^\times$. We start by noticing that since ψ has rank one and $\overline{X}$ has degree d, we must have $\deg_\tau(\psi_{\overline{X}}) = d$, by definition of the rank. As $\psi_{\overline{p}}$ has constant coefficient zero, *i.e.* is separable, Proposition 2.1.33 implies that $\tau^{d/m}$ right-divides $\psi_{\overline{p}}$. Therefore $\psi_{\overline{f}} = \alpha\psi_{\overline{p}}^m$ is right-divisible by $\tau^d = \tau_K$. Since $\overline{f}$ has degree $2d$ and ψ has rank 1, this implies that $\psi_{\overline{f}} = w\tau^d$ for some $w \in K\{\tau\}$ of τ-degree d, and consequently $\psi_{\overline{X}}\psi_{\overline{X}+\overline{h}} = \psi_{\overline{f}} = w\tau_K$. Since h is not divisible by p, $\overline{X} + \overline{h}$ is not in $\mathfrak{p}_{\mathcal{H}}$, and $\psi_{\overline{X}+\overline{h}}$ is separable. Consequently, $\psi_{\overline{X}+\overline{h}}$ equals w/β for some β in $K^\times$, and $\psi_{\overline{X}}$ equals $\beta\tau_K$.

By examining the coefficient of τ^{2d} in the equation $\psi_{\overline{X}}^2 + \psi_{\overline{X}}\psi_{\overline{h}} = \psi_{\overline{f}}$, we realize that β^2 equals $\alpha\Delta \cdot \Delta^{q^{d-1}}$, which equals $\alpha\Delta \cdot \Delta^{q^{d-1}}$, which is nothing but $\alpha\,\mathrm{N}_{K/\mathbb{F}_q}(\Delta)$: as d is odd, the $\mathbb{F}_q$-linear automorphism of K associated to τ^2 generates the Galois group of K over $\mathbb{F}_q$. There is no subfield of K of degree two over $\mathbb{F}_q$, and hence β is in $\mathbb{F}_q{}^\times$. We then prove that only one square root β of $\alpha\,\mathrm{N}_{K/\mathbb{F}_q}(\Delta)$ is suitable. If q is a power of 2, then there is only one square root. Therefore, we assume q to be odd, and let $\pm\delta$ be the two distinct square roots of $\alpha\,\mathrm{N}_{K/\mathbb{F}_q}(\Delta)$. By contradiction, assume that there exist rank one Drinfeld $A_{\mathcal{H}}$-modules ρ and ρ' over K such that

$$\begin{cases} \rho_{\overline{T}} = \rho'_{\overline{T}} = \gamma_{\mathcal{H}}(\overline{T}) + g\tau + \Delta\tau^2, \\ \rho_{\overline{X}} = \delta\tau_K, \\ \rho'_{\overline{X}} = -\delta\tau_K. \end{cases}$$

Then

$$0 = \rho_{\overline{X^2+hX-f}} - \rho'_{\overline{X^2+hX-f}} = 2\delta\rho'_{\overline{h}}\tau_K = 0.$$

This contradicts the fact that h is nonzero. □

Lemma 7.2.7 (Lemma 2.6 of [LS24]). *Any rank one Drinfeld module ψ' in $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$ is $\overline{K}$-isomorphic to a Drinfeld module ψ in $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$ such that $\psi_{\overline{X}}$ equals τ_K.*

Proof. By Lemma 7.2.6, $\psi'_{\overline{X}}$ equals $\beta\tau_K$ for some $\beta \in \mathbb{F}_q{}^\times$. Let x in $K^\times$ be an element such that $\mathrm{N}_{K/\mathbb{F}_q}(x)$ equals β, and let λ be a $(q-1)$th-root of x in $\overline{K}$. Then $\lambda^{q^d-1} = (\lambda^{q-1})^{1+q+q^2+\cdots+q^{d-1}} = \mathrm{N}_{K/\mathbb{F}_q}(x) = \beta$. Direct computations show that the Drinfeld module ψ in $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$ defined for all a in $A_{\mathcal{H}}$ by $\psi_a = x\psi'_a x^{-1}$ satisfies the desired property. □

We now have everything we need to prove the main result of the section.

Proof of Proposition 7.2.4. To an object ϕ in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$, we associate the Drinfeld module ψ in $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$ defined by $\psi_{\overline{T}} = \phi_T$ and $\psi_{\overline{X}} = \tau_K$. Let ϕ' be the rank two Drinfeld $\mathbb{F}_q[T]$-module over K

defined by $\phi'_T = \alpha\phi_T\alpha^{-1}$, so that ϕ' and ϕ are $\overline{K}$-isomorphic. Note that the characteristic polynomial of the Frobenius endomorphism of ϕ' need not be $\chi_{\mathcal{H}}$. We prove that ψ', defined by $\psi'_{\overline{T}} = \phi'_T$ and $\psi'_{\overline{X}} = \alpha\tau_K\alpha^{-1} = \alpha^{1-q^d}\tau_K$, is a well-defined rank one Drinfeld $A_{\mathcal{H}}$-module. Writing $\phi_T = \gamma(T) + g\tau + \Delta\tau^2$, we must have $g \neq 0$: otherwise ϕ would have zero j-invariant, and ϕ would be supersingular by [BK92, Lemma 3.2]. This would contradict the assumption that h is not divisible by p. Since the coefficient of τ in ϕ'_T is $\alpha^{q-1}g$ and is in K, we obviously obtain that $\alpha^{q-1} \in K$. Then, α^{1-q^d} is in K as a power of α^{q-1}. Therefore, ψ' is defined over K. Notice that if $\chi_{\mathcal{H}}(\phi'_T, \tau_K) = 0$, then $\alpha \in K$ (Lemma 7.2.2), so that $\alpha\tau_K\alpha^{-1} = \tau_K$. The Drinfeld modules ψ and ψ' are $\overline{K}$-isomorphic, and we extend our association to a well-defined map from the set $\overline{K}$-isomorphism classes of rank two Drinfeld $\mathbb{F}_q[T]$-modules whose characteristic polynomial of the Frobenius endomorphisms is $\chi_{\mathcal{H}}$, to the set of $\overline{K}$-isomorphism classes of rank one Drinfeld $A_{\mathcal{H}}$-modules. It remains to prove that this map is bijective. Injectivity comes easily and surjectivity is a direct consequence of Lemma 7.2.7. The last assertion is straightforward. □

Definition 7.2.8. Using Proposition 7.2.4 and working under its hypotheses, we can define the *j-invariant* of rank one Drinfeld $A_{\mathcal{H}}$-module as that of its associated rank two Drinfeld $\mathbb{F}_q[T]$-module.

7.2.3 The group action

Theorem 7.2.9 is the most important theoretical result of the chapter, as it defines the group action we want to compute (see Algorithm 10).

Theorem 7.2.9 (Theorem 2.7 of [LS24])**.** *As a nonempty set, $Dr_1^\circ(A_{\mathcal{H}}, K)$ is a* principal homogeneous space for $\mathrm{Cl}(A_{\mathcal{H}})$ *under the $*_K$ action, meaning that $*_K$ is free and transitive.*

The proof of Theorem 7.2.9 is postponed to § 7.2.3.2, as we first need to introduce background and the reduction and lifting of Drinfeld modules.

7.2.3.1 Reducing and lifting Drinfeld modules

Our strategy to prove Theore 7.2.9 is to use reduction and lifting properties of ordinary Drinfeld modules. As it is only relevant for the proof of Theorem 7.2.9, this framework was not introduced in Chapter 2; we refer to [Hay11, Section 11] or [BK92, Theorem 3.4] for an introduction. Let L be a finite extension of $\mathbb{F}_q(\mathcal{H})$. Let $v_{\mathfrak{P}_L}$ be a discrete valuation on L extending the $\mathfrak{p}_{\mathcal{H}}$-adic valuation of $A_{\mathcal{H}}$. It corresponds to a valuation ring $O_{\mathfrak{P}_L}$ contained in L, and a prime ideal $\mathfrak{P}_L$ of $O_{\mathfrak{P}_L}$, and we have a reduction morphism

$$\mathrm{red}_{\mathfrak{P}_L} : O_{\mathfrak{P}_L} \to O_{\mathfrak{P}_L}/\mathfrak{P}_L.$$

An Ore polynomial $f \in L\{\tau\}$ is said to be *defined over* $O_{\mathfrak{P}_L}$ if its coefficients lie in $O_{\mathfrak{P}_L}$ and its leading coefficient is invertible in $O_{\mathfrak{P}_L}$. A Drinfeld $A_{\mathcal{H}}$-module ϕ over L is said to be *defined over* $O_{\mathfrak{P}_L}$ if for all a in $A_{\mathcal{H}}$, the Ore polynomial ϕ_a is defined over $O_{\mathfrak{P}_L}$. The set of Drinfeld modules defined over $O_{\mathfrak{P}_L}$ is denoted by $\mathrm{Dr}_{r,\mathfrak{P}_L}(A_{\mathcal{H}}, L)$. By considering the morphism

$$\gamma : A_{\mathcal{H}} \to A_{\mathcal{H}}/\mathfrak{p} \to O_{\mathfrak{P}_L}/\mathfrak{P}_L,$$

the reduction map $\mathrm{red}_{\mathfrak{P}_L}$ canonically extends to a map

$$\mathrm{red}_{\mathfrak{P}_L} : \mathrm{Dr}_{r,\mathfrak{P}_L}(A_{\mathcal{H}}, L) \to \mathrm{Dr}_r(A_{\mathcal{H}}, O_{\mathfrak{P}_L}/\mathfrak{P}_L).$$

Lemma 7.2.10 (Lemma 2.9 of [LS24]). *For any Drinfeld module ϕ in $\mathrm{Dr}_{r,\mathfrak{P}_L}(A_{\mathcal{H}}, K)$ and any ideal $\mathfrak{a}$ of $A_{\mathcal{H}}$, the Drinfeld module $\mathfrak{a} *_K \phi$ is defined over $O_{\mathfrak{P}_L}$ and*

$$\mathrm{red}_{\mathfrak{P}_L}(\mathfrak{a} *_K \phi) = \mathfrak{a} *_{(O_{\mathfrak{P}_L}/\mathfrak{P}_L)} \mathrm{red}_{\mathfrak{P}_L}(\phi).$$

Proof. The definition of $\mathfrak{a} *_K \phi$ over $O_{\mathfrak{P}_L}$ is asserted in [Hay11, Proposition 11.2]. Hence, $\mathrm{red}_{\mathfrak{P}_L}(\mathfrak{a} *_K \phi)$ is well-defined. Let $u_{\mathfrak{a}}$ be the monic generator of the left-ideal of $K\{\tau\}$ generated by $\{\phi_g : g \in \mathfrak{a}\}$. Since ϕ is defined over $O_{\mathfrak{P}_L}$, then $u_{\mathfrak{a}}$ has coefficients in $O_{\mathfrak{P}_L}$, and the reduction of $u_{\mathfrak{a}}$, denoted $\mathrm{red}_{\mathfrak{P}_L}(u_{\mathfrak{a}})$, generates the left-ideal in $(O_{\mathfrak{P}_L}/\mathfrak{P}_L)\{\tau\}$ generated by $\{\mathrm{red}_{\mathfrak{P}_L}(\phi_g) : g \in \mathfrak{a}\}$. Consequently, $\mathrm{red}_{\mathfrak{P}_L}(u_{\mathfrak{a}})$ defines the isogeny associated to $\mathfrak{a} *_{(O_{\mathfrak{P}_L}/\mathfrak{P}_L)} \mathrm{red}_{\mathfrak{P}_L}(\phi)$, which concludes the proof. □

7.2.3.2 Proof of the theorem

Proof of Theorem 7.2.9. Throughout this proof, we fix a place $\overline{\mathfrak{p}}$ of $\overline{\mathbb{F}_q(T)}$ above $\mathfrak{p}$. Such a place defines compatible discrete valuation rings $O_{\mathfrak{P}_L}$ in all finite extensions L of $\mathbb{F}_q(T)$. Let us prove the transitivity of the action. Let $j_1, j_2 \in K$ be the j-invariants of two Drinfeld modules ϕ_1 and ϕ_2 in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$; ϕ_1 and ϕ_2 can be seen as objects in $\mathrm{Dr}_1(\mathbb{A}_{\mathcal{H}}, K)$ using Proposition 7.2.4. Since the ideal $(p(\overline{T}))$ of $A_{\mathcal{H}f}$ splits in $A_{\mathcal{H}}$ (it is the product of $(p(\overline{T}), \overline{X})$ and $(p(\overline{T}), \overline{X} + h(\overline{T}))$), Deuring's lifting theorems for Drinfeld modules [BK92, Theorem 3.4, Theorem 3.5] (see [Lan87, Chapter 13, § 4] for the elliptic curve analogue) imply that there exists a finite extension L of $\mathbb{F}_q(T)$ and two Drinfeld $\mathbb{F}_q[T]$-modules ϕ_1^L and ϕ_2^L of $\mathrm{Dr}_2(\mathbb{F}_q[T], L)$ such that

(i) ϕ_1^L and ϕ_2^L are isomorphic over $\mathbb{C}_\infty$;

(ii) their L-endomorphism rings are isomorphic to $A_{\mathcal{H}f}$;

(iii) their j-invariants are algebraic integers of $\mathbb{C}_\infty$ [Gek83, § (4.3)] which respectively reduce to j_1 and j_2 (elements of L) modulo $\mathfrak{P}_L$.

Therefore, ϕ_1^L and ϕ_2^L can be regarded as rank one Drinfeld $A_{\mathcal{H}}$-modules over K that are defined over $\mathfrak{P}_L$, *i.e.* objects of $\mathrm{Dr}_1(A_{\mathcal{H}}, L)_{\mathfrak{P}_L}$. Since $\mathrm{Cl}(A_{\mathcal{H}})$ acts on $\mathrm{Dr}_{1,\mathfrak{P}}(A_{\mathcal{H}}, L)$ via $*_L$ [Hay11, Proposition 11.2], and the group action $*_{\mathbb{C}_{\mathcal{H}}}$ is transitive (Theorem 7.1.4), there is an ideal $\mathfrak{a}$ of $A_{\mathcal{H}}$ such that $\mathfrak{a} *_L \phi_1^L$ is isomorphic to ϕ_2^L. Consequently, the j-invariants of $\mathfrak{a} *_L \phi_1^L$ and ϕ_2^L are equal, and so are their reductions modulo $\overline{\mathfrak{p}}$. Using Lemma 7.2.10, the j-invariant of $\mathfrak{a} *_L \phi_1^L$ reduces modulo $\mathfrak{P}_L$ to the j-invariant of $\mathfrak{a} *_{O_{\mathfrak{P}_L}/\mathfrak{P}_L} \phi_1$, which therefore also equals j_2. Hence $\mathfrak{a}$ sends the $\overline{K}$-isomorphism class of ϕ_1 to that of ϕ_2 via the $*_{\overline{K}}$ action (which is the same as the $*_K$-action on ϕ_1, since ϕ_1 is defined over K).

Finally, let us prove the freeness of the action. Let ϕ be a rank one Drinfeld $A_{\mathcal{H}f}$-module over K, and set $\psi = \mathfrak{a} *_K \phi$. Assume that ϕ and ψ are $\overline{K}$-isomorphic. Since ϕ and ψ are K-isogenous, by Lemma 7.2.2 they must be K-isomorphic. Let $\alpha \in K$ be such an isomorphism, *i.e.* $\alpha\phi_a\alpha^{-1} = \psi_a$ for any a in $A_{\mathcal{H}}$. Using [BK92, Theorem 3.4] as above, the lifting procedure provides us with a finite extension L of $\mathbb{F}_q(T)$, and with a Drinfeld module ϕ' in $\mathrm{Dr}_1(A_{\mathcal{H}}, L)_{\mathfrak{P}_L}$, which reduces to ϕ modulo $\mathfrak{P}_L$. Then, set $\psi' = \mathfrak{a} *_K \phi'$, and let $u_{\mathfrak{a}}$ be the associated isogeny. By the same argument as in the proof of Lemma 7.2.10, we realize that $u_{\mathfrak{a}}$ is defined over $O_{\mathfrak{P}_L}$ (and so its leading coefficient is 1) and that $\mathrm{red}_{\mathfrak{P}}(u_{\mathfrak{a}}) = \alpha$, which implies that $u_{\mathfrak{a}}$ is in K. Consequently, ϕ' and ψ' are K-isomorphic, $\mathfrak{a}$ is principal (Theorem 7.1.4), and the group action is free. □

7.2.4 Data representation

Before describing Algorithms 10 and 12, we need data structures to represent elements in $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$ and $\overline{K}$-isomorphism classes. Thanks to Proposition 7.2.4, we can use j-invariants—which are elements of K—to represent $\overline{K}$-isomorphism classes of Drinfeld modules in $\mathrm{Dr}_1(\mathbb{A}_{\mathcal{H}}, K)$. For representing elements in $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$, we use Mumford coordinates [Coh+12, Theorem 14.5]; in our case $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$ is isomorphic to $\mathrm{Pic}^0(\mathcal{H})$:

Lemma 7.2.11 (Lemma 3.1 of [LS24]). *The groups* $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$ *and* $\mathrm{Pic}^0(\mathcal{H})$ *are isomorphic.*

Proof. The isomorphism between $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$ and $\mathrm{Pic}^0(\mathcal{H})$ comes from the fact that there is a unique degree-1 place ∞ at infinity. Indeed, the group of affine divisors $\mathrm{Div}(\mathcal{A}_{\mathcal{H}})$ (i.e. the subgroup of divisors whose valuation at infinity is 0, see [Lor96, § 7]) is isomorphic to the group of degree-0 divisors in $\mathrm{Div}_0(\mathcal{H})$ via the map which sends a divisor D in $\mathrm{Div}(\mathcal{A}_{\mathcal{H}})$ to $D - \deg(D)\infty$. Next, we notice that D is principal in $\mathrm{Div}(\mathcal{A}_{\mathcal{H}})$ if and only if its image in $\mathrm{Div}_0(\mathcal{H})$ is principal. We conclude by using the isomorphism in [Lor96, Chapter 7, Proposition 7.1], which shows that the quotient of $\mathrm{Div}(\mathcal{A}_{\mathcal{H}})$ by principal divisors is isomorphic to $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$. □

Since $\mathcal{H}$ is an imaginary hyperelliptic curve and $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$—the group involved in the group action we want to compute—is isomorphic to $\mathrm{Pic}^0(\mathcal{H})$, we can use Mumford coordinates (§ 1.2.4.3) to represent elements in $\mathrm{Cl}(\mathcal{A}_{\mathcal{H}})$. The isomorphism classes of Drinfeld modules in $\mathrm{Dr}_1(\mathcal{A}_{\mathcal{H}}, K)$ are represented by j-invariants. Therefore, given a pair (ρ, σ) of Mumford coordinates and a j-invariant j, we let $(\rho, \sigma) *_K j$ denote the j-invariant obtained from Theorem 7.2.9.

7.3 Algorithms

We arrive to algorithms, the main goal of this chapter. In § 7.3.1, we describe and analyze Algorithm 10, with which the action of Theorem 7.2.9 is computed. After that, in § 7.3.2, we provide algorithms to recover an ideal class from an isogeny presented as an Ore polynomial.

7.3.1 From an ideal to an isogeny

We now describe Algorithm 10, the main algorithmic contribution of the chapter, which aims at efficiently computing the group action described in Theorem 7.2.9. We recall from § 1.2.4.3 and § 7.2.4 that elements of the degree zero Picard group can be represented by *Mumford coordinates*.

Proposition 7.3.1 (Proposition 3.2 of [LS24]). *Algorithm 10 (GroupAction) is correct.*

Proof. The Mumford coordinates (ρ, σ) represent the ideal $\mathfrak{a}$ of $\mathcal{A}_{\mathcal{H}}$ generated by $\rho(\overline{T})$ and $\overline{X} - \sigma(\overline{T})$. As j is nonzero ([BK92, Lemma 3.2]), the rank one Drinfeld $\mathcal{A}_{\mathcal{H}}$-module ϕ over K defined by $\phi_{\overline{T}} = \gamma(T) + \tau + j^{-1}\tau^2$ and $\phi_{\overline{X}} = \beta\tau_K$ has j-invariant j, where we have picked β in $\mathbb{F}_q{}^{\times}$ (see Lemma 7.2.6). We shall prove that $\mathfrak{a} *_K \phi$ is ψ, where $\psi \in \mathrm{Dr}_1(\mathcal{A}_{\mathcal{H}}, K)$ is the Drinfeld module such that $\psi_{\overline{T}} = \gamma(T) + \widehat{g}\tau + \widehat{\Delta}\tau^2$ and $\psi_{\overline{X}} = \beta\tau_K$.

The Ore polynomial u computed at Step 3 is $\mathrm{rgcd}(\phi_{\rho(\overline{T})}, \tau_K - \phi_{v(\overline{T})})$, which is by construction the monic Ore polynomial defining the isogeny. Since we need to invert the coefficient u_0 (at Step 5), we need to prove that u is separable. This is indeed true: u right-divides $\phi_{\rho(\overline{T})}$, which is separable because $\deg(\rho) < d$. Hence ρ cannot be a multiple of p, which is a generator of $\mathrm{Ker}(\gamma)$.

Algorithm 10. GroupAction (Algorithm 1 of [LS24])

Input: A pair (ρ, σ) of Mumford coordinates representing an element of $\mathrm{Cl}(A_{\mathcal{H}})$, and the j-invariant j in K of a Drinfeld module of $\mathrm{Dr}_1(A_{\mathcal{H}}, K)$

Output: The j-invariant $(\rho, \sigma) *_K j$, obtained from Theorem 7.2.9 and Lemma 7.2.11

1 Set $\widetilde{\rho} = \rho(\gamma(T) + \tau + j^{-1}\tau^2) \in K\{\tau\}$;
2 Set $\widetilde{\sigma} = \sigma(\gamma(T) + \tau + j^{-1}\tau^2) \in K\{\tau\}$;
3 Compute $u = \mathrm{rgcd}(\widetilde{\rho}, \tau_K - \widetilde{\sigma})$;
4 Let u_0, u_1 be the first two coefficients of u;
5 Compute $\widehat{g} = u_0^{-q}(u_0 + u_1(\gamma(T)^q - \gamma(T)))$;
6 Compute $\widehat{\Delta} = j^{-q^{\deg_\tau(\rho)}}$;
7 return $\widehat{g}^{q+1}/\widehat{\Delta}$.

Since u is an isogeny [Hay11, Corollary 5.10], there exists a rank one Drinfeld $A_{\mathcal{H}}$-module ψ over K such that $u \cdot \phi_{\overline{T}} = \psi_{\overline{T}} \cdot u$ where $\psi_{\overline{T}}$ has τ-degree 2. It remains to prove that $\psi_{\overline{T}}$ equals $\gamma(T) + \widehat{g} + \widehat{\Delta}\tau^2$. This is done by extracting—as in Equations (2.1) the coefficients of τ and $\tau^{\deg_\tau(u)+2}$ in the equality $u \cdot \phi_{\overline{T}} = \psi_{\overline{T}} \cdot u$, which provides us with:

$$\begin{cases} u_0\, g + u_1\, \gamma(T)^q &= \widehat{g}\, u_0^q + \gamma(T)\, u_1, \\ j^{-q^{\deg_\tau(u)}} &= \widehat{\Delta}. \end{cases}$$

There is only one pair $(\widehat{\Delta}, \widehat{g}) \in K^2$ which satisfies these two equalities, and the associated Drinfeld module has j-invariant $\widehat{g}^{q+1}/\widehat{\Delta}$. □

We finish this section by studying the asymptotic complexity of Algorithm 10. For Ore Euclidean division and right-greatest common divisor computation, we use Algorithms 1 and 2, respectively.

Proposition 7.3.2 (Proposition 3.7 of [LS24])**.** *The deterministic Algorithm 10 runs in $O(d^2)$ operations in K and $O(d^2)$ applications of the Frobenius endomorphism.*

Proof. Writing $\rho = \rho_n T^n + \cdots + \rho_0$ and $\phi_T = \gamma(T) + \tau + j^{-1}\tau^2$, we have $n \leqslant (d-1)/2$ and $\widetilde{\rho} = \rho_n \phi_T^n + \cdots + \rho_0$. In order to compute $\tilde{\rho}$, we can first compute $\phi_T^2, \ldots, \phi_T^n$ iteratively. Let $1 \leqslant m \leqslant n-1$ be an integer and write $\phi_T^m = \sum_{i=0}^{2m} a_i \tau^i$. Then

$$\phi_T \phi_T^m = \sum_{i=0}^{2m} \left(a_i \gamma(T) \tau^i + g a_i^q \tau^{i+1} + \Delta a_i^{q^2} \tau^{i+2} \right).$$

Knowing ϕ_T^m, the computation of ϕ_T^{m+1} requires $O(m)$ additions, multiplications, q-exponentiations and q^2-exponentiations, which is $O(m)$ operations in K and $O(m)$ applications of the Frobenius endomorphism of $K/\mathbb{F}_q$. Consequently, $O(d^2)$ operations in K and $O(d^2)$ applications of the Frobenius endomorphism are required to compute $\phi_T^2, \ldots, \phi_T^n$.

The last operation affecting the asymptotic complexity is the rgcd, which we perform using Algorithm 2. We have $\deg(\rho) = n$, $\deg(\sigma) < n$, so that $\tilde{\sigma}$ and $\tau_K - \tilde{\rho}$ respectively have τ-degree at most d. By Lemma 4.3.3, this algorithm runs in $O(d^2)$ operations in K and $O(d^2)$ applications of the Frobenius endomorphism. □

7.3.2 From an isogeny to an ideal

In this section, we make explicit the transitivity of the group action of Theorem 7.2.9. More explicitly, given two rank one Drinfeld $A_{\mathcal{H}}$-modules ϕ and ψ over K, we compute Mumford coordinates (ρ, σ) that represent the class $(\rho(\overline{T}), \overline{X} - \sigma(\overline{T}))$ in $\mathrm{Cl}(A_{\mathcal{H}})$ that associates the isomorphism class of ψ with that of ϕ, via $*_K$ in Theorem 7.2.9.

7.3.2.1 Idea of the algorithm

Using Proposition 7.2.4, ϕ and ψ can also be viewed as rank two Drinfeld $\mathbb{F}_q[T]$-modules over K, whose characteristic polynomial of the Frobenius endomorphism is $\chi_{\mathcal{H}}$. On the one hand, Wesolowski's algorithm can be used to obtain an isogeny u between ϕ and ψ (§ 2.1.6). On the other hand, computing the Mumford coordinates associated to a class of ideals of $A_{\mathcal{H}}$—provided that the ideal class is presented by one of its representatives, and that this representative has a finite number of known generators—can be done efficiently, as discussed in § 1.2.4.3. For these reasons, we focus on computing the generators of an ideal in $A_{\mathcal{H}}$, up to principal ideals, that corresponds to an isogeny u from ϕ to ψ, up to isomorphism. The isogeny u will be given by Wesolowski's algorithm. We proceed by first assuming that the isogeny norm of u is coprime to the $\mathbb{F}_q[T]$-characteristic p of K (Algorithm 11), before deriving an algorithm for the general case (Algorithm 12).

7.3.2.2 Correspondence between ideals and isogenies

We start by the following lemma, which establishes a correspondence between classes of ideals in $A_{\mathcal{H}}$ and isogenies. It establishes that the product of isogenies corresponds to the product of ideal classes, which complements Theorem 7.2.9.

Lemma 7.3.3 (Lemma 3.8 of [LS24]). *Let ϕ be an object in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_H}$. There is a one-to-one correspondence between monic isogenies whose domain is ϕ and nonzero ideals in $A_{\mathcal{H}}$. Moreover, for any three Drinfeld modules ϕ_1, ϕ_2, ϕ_3 in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$ accompanied by two isogenies $u_1 : \phi_1 \to \phi_2$, $u_2 : \phi_2 \to \phi_3$, the ideal associated to $u_2 \cdot u_1$ in $A_{\mathcal{H}}$ is the product of the ideals associated to u_1 and u_2.*

Proof. To any monic isogeny $u : \phi \to \psi$, we associate the nonzero left ideal $\mathrm{Hom}(\psi, \phi)u$ of $\mathrm{End}(\phi) \simeq A_{\mathcal{H}}$. As ψ is isogenous to ϕ, the characteristic polynomial of ψ is that of ϕ. Reciprocally, to any nonzero ideal $\mathfrak{a}$ of $A_{\mathcal{H}}$ corresponds the isogeny defined by $\mathrm{RGCD}(\{g(\phi_T, \tau_K) : g \in \mathfrak{a}\})$.

To prove the second statement, we start by letting u denote the isomorphism between $\mathrm{End}(\phi)$ and $\mathrm{End}(\psi)$ that sends $g(\phi_T, \tau_K)$ to $g(\psi_T, \tau_K)$ for any g in $A_{\mathcal{H}}$. Let $\widehat{u}$ be a ρ-dual isogeny for u, for some $\rho \in \mathbb{F}_q[T]$ such that u right-divides ϕ_u (see Definition 2.1.41). Notice that for all $g \in A_{\mathcal{H}}$, ϕ_ρ right-divides $g(\phi_T, \tau_K)\widehat{u}$ if and only if ψ_ρ left-divides $\widehat{u}g(\psi_T, \tau_K)$. Said otherwise, u sends the ideal $\mathrm{Hom}(\psi, \phi)u$ of $\mathrm{End}(\phi)$ to the ideal $u\,\mathrm{Hom}(\psi, \phi)$ of $\mathrm{End}(\psi)$ (keep in mind that both $\mathrm{End}(\phi)$ and $\mathrm{End}(\psi)$ are commutative). By considering the isomorphism $u_{1,2} : \mathrm{End}(\phi_1) \to \mathrm{End}(\phi_2)$ and by using the commutativity of $\mathrm{End}(\phi_2)$, we obtain

$$\begin{aligned}
\mathrm{Hom}(\phi_3, \phi_2)u_2 \cdot u_{1,2}(\mathrm{Hom}(\phi_2, \phi_1)u_1) &= (\mathrm{Hom}(\phi_3, \phi_2)u_2) \cdot (u_1\,\mathrm{Hom}(\phi_2, \phi_1)) \\
&= (u_1\,\mathrm{Hom}(\phi_2, \phi_1)) \cdot (\mathrm{Hom}(\phi_3, \phi_2)u_2) \\
&= u_{1,2}(\mathrm{Hom}(\phi_3, \phi_2)\,\mathrm{Hom}(\phi_2, \phi_1)u_2u_1) \\
&\subset u_{1,2}(\mathrm{Hom}(\phi_3, \phi_1)u_2u_1).
\end{aligned}$$

To conclude, we use the properties of the norm of isogenies: the norm is multiplicative and corresponds to the norm of the associated ideal in $A_{\mathcal{H}f}$ [Gek91, Lemma 3.10.(iv)]. Consequently, the norms on both sides of the inclusion are equal. This implies that the last inclusion is in fact an equality. □

7.3.2.3 The case of prime ideals

Our goal is to describe an algorithm which returns the ideal of $A_{\mathcal{H}f}$ (up to principal ideals) corresponding to a ρ-isogeny u (see Definition 2.1.41) between two Drinfeld modules of $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}f}}$. Before we work on the general case (Algorithm 12), let us first study the special case of prime ideals (Algorithm 11).

Algorithm 11. PrimeIsogenyToPrimeIdeal (Algorithm 4 of [LS24])

Input:
- An ordinary Drinfeld module $\phi \in \mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}f}}$,
- A monic prime $r \in \mathbb{F}_q[T]$ away from the $\mathbb{F}_q[T]$-characteristic $\mathfrak{p}$ of K,
- An r-isogeny $u : \phi \to \psi$ between $\phi, \psi \in \mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}f}}$.

Output: A polynomial σ in $\mathbb{F}_q[T]$ such that the left-ideal of $K\{\tau\}$ generated by ϕ_r and $\tau_K - \phi_\sigma$ is generated by u.

1 Compute y, remainder in the right-division of τ_K by u;
2 Write $u^{(0)} = 1$;
3 for $1 \leqslant n \leqslant \deg(r)$ do
4 | Compute $u^{(n+1)}$, the remainder in the right-division of $\phi_T u^{(n)}$ by u;
5 end
6 Find $(\sigma_0, \ldots, \sigma_{\deg(r)-1})$ in ${\mathbb{F}_q}^{\deg(r)}$ such that $y - (\sigma_0 u^{(0)} + \cdots + \sigma_{\deg(r)-1} u^{(\deg(r)-1)})$ is zero;
7 return $\sigma_0 + \sigma_1 T + \cdots + \sigma_{\deg(r)-1} T^{\deg(r)-1}$.

In what follows, ω is a feasible exponent for matrix multiplication in K, satisfying $2 \leqslant \omega \leqslant 3$, as in § 1.3.3. Before proving the correctness of Algorithm 11, we need the following technical lemma:

Lemma 7.3.4 (Lemma 3.9 of [LS24])**.** *Let A be a function ring as in § 2.2 and $\mathfrak{p}_A$ be the A-characteristic of K. Let ϕ and ψ be two Drinfeld A-modules over K. If there exists an isogeny between ϕ and ψ whose norm is coprime to $\mathfrak{p}_A$, then the* RGCD *of the Ore polynomials defining* $\mathrm{Hom}(\psi, \phi)$ *is* 1.

Proof. Let $f : \phi \to \psi$ be an r_A-isogeny, where r_A is an element of A away from $\mathfrak{p}_A$. Set

$$V = \bigcap_{u \in \mathrm{Hom}(\psi,\phi)} \mathrm{Ker}(u),$$

and let g be an isogeny in $\mathrm{Hom}(\psi, \phi)$. The sequence of A-modules

$$0 \to V \to \mathrm{Ker}(g) \to \mathrm{Ker}(g)/V \to 0$$

is exact, so that $\chi(V)$ divides $\chi(\mathrm{Ker}(g))$, where χ is the Euler-Poincaré characteristic with respect to A. Consequently, by definition of the Euler-Poincaré characteristic (see § 2.1.8.1), $\chi(V)\mathfrak{p}_A^{\mathrm{h}(g)/\deg(\mathfrak{p})}\mathfrak{n}(f)$ divides $\mathfrak{n}(fg)$. In particular, $\chi(V)\mathfrak{n}(f)$ divides $\mathfrak{n}(fg)$. By [Gek91, Lemma 3.10.(iv)], we have

$$\sum_{g \in \mathrm{Hom}(\psi,\phi)} \mathfrak{n}(fg) = \mathfrak{n}(f).$$

Since $\mathfrak{n}(f)$ is not the zero ideal, $\chi(V)$ must equal A and hence V is $\{0\}$. Then $\mathrm{Ker}(\textsc{rgcd}(\mathrm{Hom}(\psi,\phi))) = V$ is trivial, which implies that $\textsc{rgcd}(\mathrm{Hom}(\psi,\phi))$ divides $\tau^{\deg(\mathfrak{p})\ell}$ for some ℓ in $\mathbb{Z}_{\geqslant 0}$. Since r_A is away from $\mathfrak{p}_A$, the r_A-dual of f is separable (it has norm (r_A)), hence $\textsc{rgcd}\left(\mathrm{Hom}(\psi,\phi)\right) = 1$. □

Proposition 7.3.5 (Proposition 3.10 of [LS24]). *Algorithm 11 (PrimeIsogenyToPrimeIdeal) is correct.*

Proof. First, we notice that since r is prime, the norm of u must be the ideal (r) of $\mathbb{F}_q[T]$, and hence $\deg_\tau(u) = \deg(r)$. Since u is an r-isogeny, ϕ_r is in $\mathrm{Hom}(\psi,\phi)u$. Since $A_{\mathcal{H}f}$ is a Dedekind domain in a quadratic extension of $\mathbb{F}_q(T)$, the ideal $\mathrm{Hom}(\psi,\phi)u$—seen as an ideal in $A_{\mathcal{H}f}$ by Lemma 7.3.3—contains the prime r. Therefore, it can only be either the full ring $A_{\mathcal{H}f}$, the principal ideal (r), or a prime ideal of degree 1 above (r).

By Lemma 7.3.4, the left-ideal in $K\{\tau\}$ generated by elements in $\mathrm{Hom}(\psi,\phi)u$ equals $K\{\tau\}u$, which is neither the full ring $K\{\tau\}$, nor $K\{\tau\}\phi_r$, since $\deg_\tau(\phi_r) = 2\deg(r)$ is strictly greater than $\deg_\tau(u)$. Consequently, using the correspondence in Lemma 7.3.3, $\mathrm{Hom}(\psi,\phi)u$ must be a degree-1 prime ideal above the principal ideal associated to r. Said otherwise, the polynomial $X^2 + h(T)X - f(T)$ factors over $(\mathbb{F}_q[T]/(r))[X]$, and a prime ideal above (r) in $A_{\mathcal{H}f}$ has the form $(r(\overline{T}), X - \sigma(\overline{T}))$, where $\sigma \in \mathbb{F}_q[T]$ satisfies $\chi_{\mathcal{H}f}(\overline{T},\overline{\sigma}) = 0$ in $\mathbb{F}_q[T]/(r)$. Note that up to reducing σ modulo r, we can assume that $\deg(\sigma) < \deg(r)$; under this assumption, σ is uniquely defined.

We now prove that the coefficients of σ satisfy the equality in Step 6, so that it can indeed be computed via linear algebra. To this end, we need to prove that u right-divides $\tau_K - \phi_\sigma$. This is a direct consequence of the fact that the ideal $\mathrm{Hom}(\psi,\phi)u$ of $\mathrm{End}(\phi)$ corresponds to the ideal of $A_{\mathcal{H}f}$ generated by $r(\overline{T})$ and $X - \sigma(\overline{T})$. □

Proposition 7.3.6 (Proposition 3.10 of [LS24]). *Let m denote the degree of r. The deterministic Algorithm 11 runs in $O(dm^\omega)$ operations in K and $O(dm + m^2)$ applications of the Frobenius endomorphism.*

Proof. Computing the first remainder costs $O(dm)$ operations in K, and $O(dm)$ applications of the Frobenius endomorphism. The other remainders are computed recursively. Knowing $u^{(n)}$, computing $u^{(n+1)} = \phi_T \cdot u^{(n)}$ requires $O(m)$ operations in K, and the same number of Frobenius applications. This Ore polynomial has degree at most $\deg_\tau(u) + 1$. By Lemma 4.3.3, computing this remainder requires $O(\deg_\tau(u)) = O(m)$ operations in K, and as many applications of the Frobenius. Consequently, computing all elements in the loop requires $O(m^2)$ operations in K and $O(m^2)$ applications of the Frobenius endomorphism.

The last costly step is solving a linear system. More precisely, the algorithm finds a solution of an affine system over $\mathbb{F}_q$, whose associated matrix has less than dm rows, and m columns. Solving such a system requires $O(dm^\omega)$ operations in K. In total, we get $O(dm^\omega)$ operations in K, and $O(dm + m^2)$ applications of the Frobenius endomorphism. □

7.3.2.4 The general case

We now go from the prime case to the general case with Algorithm 12.

Proposition 7.3.7 (Proposition 3.11 of [LS24]). *Algorithm 12 (IsogenyToIdeal) terminates and is correct.*

Proof. The proof is done by induction on the degree of u, which strictly decreases at each recursion call, hence the termination of the algorithm. By Lemma 7.3.3, there is a uniquely defined ideal $\mathfrak{a}$ of $A_{\mathcal{H}f}$ corresponding to u. Since $A_{\mathcal{H}f}$ is a Dedekind domain (Lemma 7.2.11), $\mathfrak{a}$ factors as a product of prime ideals.

Algorithm 12. IsogenyToIdeal (Algorithm 5 of [LS24])

INPUT:

(i) A Drinfeld module ϕ in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$,

(ii) A (non-necessarily prime) monic polynomial ρ in $\mathbb{F}_q[T]$, away from $\mathfrak{p}$

(iii) A ρ-isogeny u from ϕ to some other Drinfeld module ψ in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$,

OUTPUT: A factorization of the ideal $\mathfrak{a}$ of $A_{\mathcal{H}}$ associated to u in Lemma 7.3.3.

```
if ρ equals 1 then
    return A_H.
end
Compute a nonconstant monic prime factor r of ρ;
Compute ũ = rgcd(u, φ_r);
if ũ equals 1 then
    return IsogenyToIdeal(φ, ρ/r^{v_r(ρ)}, u).
end
else if ũ equals λφ_r for some λ ∈ K^× then
    return (r(T̄)) · IsogenyToIdeal(φ, ρ/r, u · φ_r^{-1}).
end
else
    Compute σ = PrimeIsogenyToPrimeIdeal(φ, r, ũ);
    Compute φ̃, the codomain of ũ, using Equation (2.1);
    return (ρ(T̄), X̄ − σ(T̄)) · IsogenyToIdeal(φ̃, ρ/r, u · ũ^{-1}).
end
```

For r in $\mathbb{F}_q[T]$ an irreducible polynomial, we let $\mathfrak{a}_r$ denote the product of all primes in the factorization of $\mathfrak{a}$ which contain $\overline{r} \in A_{\mathcal{H}}$. Consequently, since $\overline{\rho}$ is in $\mathfrak{a}$, we have

$$\mathfrak{a} = \prod_{\substack{r \text{ prime} \\ r \text{ divides } \rho}} \mathfrak{a}_r.$$

Let r be a prime factor of ρ. Then there are three possible cases, depending on whether r is inert, splits, or ramifies in $A_{\mathcal{H}}$.

If r is inert, then $\mathfrak{a}_r$ equals $(\overline{r})^\ell$, for some $\ell \geqslant 0$. If ℓ is zero, then $\mathfrak{a}_r$ equals $A_{\mathcal{H}}$. In this case, if $\rho \neq 1$, then $\overline{r} \notin \mathfrak{a}$ and therefore $\textsc{rgcd}(u, \phi_r) = 1$. Consequently, $\overline{r}$ is invertible in $\mathfrak{a}$, and therefore $\overline{\rho}/\overline{r}^{v_r(\rho)}$ belongs to $\mathfrak{a}$ and we can apply our induction hypothesis. If $\ell > 0$, then $\overline{r}$ divides all elements in $\mathfrak{a}$. Therefore ϕ_r right-divides u and hence $\widetilde{u} = \lambda\phi_r$ for some $\lambda \in K^\times$. Since ϕ_r is an endomorphism of ϕ, $u \cdot \phi_r^{-1}$ is a well-defined isogeny between ϕ and ψ, and its corresponding ideal in $A_{\mathcal{H}}$ is $\{g : g \in A_{\mathcal{H}}, g \cdot \overline{r} \in \mathfrak{a}\}$. This ideal contains $\overline{\rho}/\overline{r}$, hence we can apply our induction hypothesis.

If r splits then the ideal $(\overline{r})$ of $A_{\mathcal{H}}$ factors as a product $\mathfrak{P}_1 \cdot \mathfrak{P}_2$ of two distinct prime ideals. Therefore, $\mathfrak{a}_r = \mathfrak{P}_1^m \cdot \mathfrak{P}_2^n$ for some $m, n \geqslant 0$. First, if both m and n are nonzero, then $\mathfrak{a}_r = (\overline{r}) \cdot \mathfrak{P}_1^{m-1}\mathfrak{P}_2^{\beta-1}$. Consequently, u is right-divisible by ϕ_r, $\widetilde{u} = \lambda\phi_r$ for some $\lambda \in K^\times$ and we can apply our induction hypothesis on the isogeny $u \cdot \phi_r^{-1}$. Now, we study the case where either m or n is zero. Without loss of generality, let us assume that β is zero. Then $\mathfrak{a}_r = \mathfrak{P}_1^m$. In this case, $\widetilde{u}$ cannot be right-divisible by ϕ_r: this would contradict the fact that $(\overline{r})$ does not divide $\mathfrak{a}$. On the other hand, $\widetilde{u}$ cannot equal one since for any element $g \in \mathfrak{P}_1$, $g(\phi_T, \tau_K)$ must right-divide both ϕ_r and u. Since u is an isogeny, $\mathrm{Ker}(u)$, *i.e.* $\mathrm{Ker}(\mathbb{E}(u))$, is an $\mathbb{F}_q[T]$-submodule of $\mathbb{E}(\phi)$, and so is $\ker(\widetilde{u}) = \mathrm{Ker}(\mathbb{E}(u)) \cap \mathbb{E}_r(\phi)$. Consequently, $\widetilde{u}$ is an isogeny from ϕ to some other Drinfeld module ϕ' in $\mathrm{Dr}_2(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}}$. The Drinfeld module ϕ' can be computed using Equation (2.1), and the ideal corresponding to this isogeny can be computed using Algorithm 11, which is correct by Proposition 7.3.5. To apply the induction hypothesis on ℓ, it remains to prove that $u' \coloneqq u \cdot \widetilde{u}^{-1}$ defines an isogeny $u' : \phi' \to \psi$ which right-divides $\phi'_{\rho/r}$. To this end, let $\hat{u}$ denote the dual ρ-isogeny of u, and let $\widehat{\widetilde{u}}$ be the dual r-isogeny of $\widetilde{u}$. We have

$$\begin{aligned} \phi'_\rho\phi'_r &= \widetilde{u} \cdot \widetilde{\hat{u}} \cdot \phi'_\rho = \widetilde{u} \cdot \phi_\rho \cdot \widehat{\widetilde{u}} = \widetilde{u} \cdot \hat{u} \cdot u \cdot \widehat{\widetilde{u}} \\ &= \widetilde{u} \cdot \hat{u} \cdot u' \cdot \widetilde{u} \cdot \widetilde{\hat{u}} = \widetilde{u} \cdot \hat{u} \cdot u' \cdot \phi'_r. \end{aligned}$$

By right-dividing by ϕ'_r, we obtain that u' divides ϕ_ρ and that it is the ρ-dual of the composed isogeny $\widetilde{u} \cdot \hat{u}$. This proves that u' is a well-defined isogeny. By using the second statement in Lemma 7.3.3, we obtain that the ideal associated to u' is

$$\mathfrak{P}_1^{m-1} \cdot \prod_{\substack{r' \text{ prime} \\ \phi_{r'} \text{ divides } u \\ r' \neq r}} \mathfrak{a}_{r'},$$

which contains $\overline{\rho}/\overline{r}$, so that we can apply our induction hypothesis.

Finally, the ramified case is proved similarly than the split case. The main difference is that $\mathfrak{P}_1 = \mathfrak{P}_2$, so that $\mathfrak{a}_r = (r)^\ell \cdot \mathfrak{P}_1^m$, for some $\ell \geqslant 0$ and $\rho \in \{0, 1\}$; this does not change the proof. □

Proposition 7.3.8 (Proposition 3.13 of [LS24])**.** *Let m denote the τ-degree of u. Using the Cantor-Zassenhaus algorithm for polynomial factorization, the Las Vegas Algorithm 12 runs in $O^\sim(dm^\omega + m^3 + m \log q)$ expected operations in K and $O(dm + m^3)$ expected applications of the Frobenius endomorphism.*

Proof. Step 4 is performed using the Cantor-Zassenhaus algorithm, with expected cost bounded by $O^{\sim}(m^2 + m \log q)$. Notice also that the initial factorization of ρ may be performed only once for this cost, at the first call of the algorithm. Then Step 5 performs an Ore Euclidean division, which costs $O(m^2)$ operations in K and $O(m^2)$ applications of the Frobenius endomorphism using Euclid's algorithm (Lemma 4.3.4).

If $\widetilde{u}$ is 1 or $\lambda\phi_r$, it is sufficient to compute a polynomial division, and $u \cdot \phi_r^{-1}$ in the latter case. These computations do not exceed the complexity of Step 5. No other computation is performed and the algorithm is recursively called on a smaller instance. If $\widetilde{u}$ is neither 1 or $\lambda\phi_r$, then Algorithm 11 is called. Let $\rho = r_1 \cdots \rho_\ell$ be a factorization of u, where the r_i' are not necessarily distinct primes with $k_i := \deg(r_i)$. We can assume that the prime factors are ordered as the algorithm processes them. Then, counting all the recursive calls of the algorithm, we get that the total expected cost is bounded above by

$$O^{\sim}(m^2 + m \log q) + \sum_{i=1}^{\ell} \left(O\left(\sum_{j=i}^{\ell} k_j^2 \right) + O(d\, k_i^{\omega}) \right)$$

operations in K and

$$\sum_{i=1}^{\ell} \left(O\left(\sum_{j=i}^{\ell} k_j^2 \right) + O(dk_i + k_i^2) \right)$$

applications of the Frobenius endomorphism. Since $\sum_{i=1}^{\ell} k_i = m$, we obtain that these formulas are bounded above by $O^{\sim}(dm^{\omega} + m^3 + m \log q)$ expected operations in K and $O(dm + m^3)$ expected applications of the Frobenius endomorphism. □

Remark 7.3.9. Algorithm 12 needs as input a polynomial $u \in \mathbb{F}_q[T]$ such that u right-divides ϕ_u. It can be found by looking for a non-trivial $\mathbb{F}_q$-linear relation between the remainders of $\phi_{T^0}, \phi_{T^1}, \ldots, \phi_{T^\ell}$ in the right-division by u. When $\ell \geqslant \deg_\tau(u)$, such a non-trivial linear combination exists. Algorithm 12 also involves the factorization of a polynomial u in $\mathbb{F}_q[T]$. We choose to use the Cantor-Zassenhaus algorithm [CZ81], a Las Vegas probabilistic algorithm with expected complexity bounded above by $O^{\sim}(\delta^2 + \delta \log q)$, where δ is the degree of the input. Another possibility is to use Berlekamp's algorithm, which is deterministic; its complexity involves a dependence in q, and its complexity is overall polynomial, if q is polynomial in δ. However, with a complexity dominated by δ^{ω}, its use would severely hinder the overall complexity of the algorithm. Finally, the complexities for Algorithms 11 and 12 will be expressed in terms of d, q, and the degree of the input polynomial r (resp. u). As u is an r-isogeny (resp. u), its degree is bounded by that of r (resp. u).

Remark 7.3.10. One could ask whether the complexities of Propositions 7.3.2, 7.3.6 and 7.3.8 may be enhanced by using more efficient algorithmic primitives for the arithmetic of Ore polynomials. In § 1.3.4, we mention the algorithms of [CL17a] and [CL17b] for Ore polynomial multiplication, Euclidean division and right-greatest common divisor; in many applications, these algorithms yield substantial speed-ups. We highlight that the authors work under the hypothesis that q is fixed and that operations in K as well as applications of the Frobenius and K cost $O^{\sim}(d)$ operations in $\mathbb{F}_q$.

Let us first ask ourselves if we can enhance Algorithm 10 by using asymptotically fast Ore Euclidean division at Step 3. Per [CL17b, Proposition 3.1], as we have seen, computing u would cost $O^{\sim}(\mathrm{SM}^{\geqslant 1}(d, d))$ operations in $\mathbb{F}_q$. Using the values given in § 1.3.4, we get $\mathrm{SM}^{\geqslant 1}(d, d) = d^{\frac{9-\omega}{5-\omega}}$. Even using the lower bound $\omega = 2$, we would get $\frac{9-\omega}{5-\omega} = \frac{7}{3}$, and the computation of u would then be outweighed by the

computations of $\tilde{u}$ and $\tilde{v}$, which both cost $O^{\sim}(d^3)$ operations in $\mathbb{F}_q$ in the complexity model of *loc. cit*. Therefore, using the algorithmic primitives of [CL17a] and [CL17b] does not at the moment improve the complexity bound in Proposition 7.3.2. To benefit from these, one would need to enough reduce the cost of computing $\tilde{u}$ and $\tilde{\sigma}$. Our attempts to do so were unsuccessful.

The situation for Algorithm 11 is quite similar. The first step requires computing the remainder in the Euclidean division of τ_K by u. As u has degree $O(m)$ and τ_K has degree d, the computation would require $O^{\sim}(\mathrm{SM}^{\geqslant 1}(d+m, d))$ operations in $\mathbb{F}_q$. With the formula for $\mathrm{SM}^{\geqslant 1}$, this is $O^{\sim}((d+m)d^{\frac{4}{5-\omega}})$ operations in $\mathbb{F}_q$. Adding to that the $O(d^2m^{\omega})$ operations in $\mathbb{F}_q$ required to solve the system, there is no benefit in using the algorithms of [CL17b]. In fact, doing so would actually worsen the asymptotic complexity with respect to the variable d. This is due to the fact that the bound is linear with respect to $d+m$ for fixed d, but it has a costly dependence with respect to d.

The complexity of Algorithm 12 depends on that of Algorithm 11, and our conclusion is the same.

7.4 Discussion

Although we believe that this computational problem is interesting on its own—especially considering the importance of this group action in class field theory—the original motivation was to apply it to cryptography [LS22]. We thus mention a practical implementation of Algorithm 10, which was targeted to cryptography. Then, we describe a key-exchange protocol inspired from the Couveignes-Rostovtsev-Stolbunov (CRS) cryptosystem (§ A.1.3.2). Using an algorithm of Wesolowski [Wes22], we then prove the insecurity of our protocol. See also Appendix A.

7.4.1 Implementation

To demonstrate the practical effectivity of Algorithm 10, we have implemented the group action for a hyperelliptic curve of genus 260 defined over $\mathbb{F}_2$. Our C++/NTL code is available at

`https://gitlab.inria.fr/pspaenle/crs-drinfeld-521`.

Set $K = \mathbb{F}_2[T]/\mathfrak{p}$, where $\mathfrak{p} = T^{521} + T^{32} + 1 \in \mathbb{F}_2[T]$. Polynomials of $\mathbb{F}_2[T]$ are encoded using the hexadecimal NTL notation: for instance, `0x4bc` refers to $T^2 + T^4 + T^5 + T^7 + T^{10} + T^{11}$. By extension, elements of K are also encoded with the NTL hexadecimal notation, implicitly using the reduction modulo the ideal $\mathfrak{p}$. Let us pick an isomorphim class of Drinfeld modules represented by the j-invariant

$$j = \begin{array}{l} \texttt{0xb985b4ce23bd9cf992f1176e17c27dab7ae67270131} \\ \texttt{12a2804cb64abccc7cce061e12786bb3248809922da} \\ \texttt{35d3b624d67d08087e07c260fcaa9807a420ca83fa95}. \end{array}$$

Let ϕ be the Drinfeld $\mathbb{F}_2[T]$-module over K defined by $\phi_T = \gamma(T) + \tau + j^{-1}\tau^2$. The characteristic polynomial of its Frobenius endomorphism is $X^2 + h(T)X - f(T)$, with

$$h = \texttt{0xb1ffea4ab7e58b96adf4e4972d7db9184821c1d64b375df52669c60973bb80dee}$$

and

$$f = T^{521} + T^{32} + 1.$$

The polynomial $X^2 + h(T)X - f(T)$ then defines a genus-260 hyperelliptic curve $\mathcal{H}$ over $\mathbb{F}_2$, whose Picard group $\mathrm{Pic}^0(\mathcal{H})$ is cyclic and has almost-prime order

$$2 \times 3154131824675456726041163164150477433504949628897448652594429436560240732956 89.$$

We ran our implementation of Algorithm 10, with the above parameters, on a laptop with Intel i5-8365U@1.60GHz CPU, 8 cores, 16 GB RAM. We chose an element of $\mathrm{Pic}^0(\mathcal{H})$ at random such that the u-polynomial in the Mumford coordinates is irreducible and has degree 35. The most costly step in practice is the first step of Euclid's algorithm: it starts by computing τ^{521} modulo ϕ_u, which has τ-degree 70. Unfortunately, in our non-commutative setting we cannot use binary exponentiation to speed-up this step: for f, f' and g in $K\{\tau\}$, $(f + K\{\tau\}g) \cdot (f' + K\{\tau\}g)$ may be different than $ff' + K\{\tau\}g$. Therefore, we implemented a parallelized subroutine specialized for this task. By using the 8 cores of the laptop, computing this group action takes 24 ms.

Remark 7.4.1. The group order was computed using the Magma implementation of the Denef-Kedlaya-Vercauteren algorithm [Ked01; DV06b]. This computation costs 53 hours on a Intel(R) Xeon(R) CPU E7-4850. This highly contrasts with the analog problem on elliptic curves; computing the class number of an imaginary quadratic number field may be a very challenging problem [BKV19].

7.4.2 Application to cryptography

As we explain in § A.1.3.1, it is possible to build cryptographic protocols using free and transitive group actions, as long as some problems are assumed computationally challenging. Such actions are called *hard homogeneous spaces*. The CRS cryptosystem is one of them, and makes the class group of an imaginary quadratic number field acting on a set of isomorphism classes of ordinary elliptic curves. This construction is considered secure, but impractical. The group action that we compute in the present chapter is actually the Drinfeld module analogue of the action of CRS. As demonstrated in the previous section, practical computations are quite efficient, beating the time required to exchange a key with CRS [DKS18]. However, as we explain now, the cryptosystem obtained from the Drinfeld module case is not secure.

We first describe the construction of the cryptosystem, in the framework of hard homogeneous spaces (§ A.1.3.1) proposed by Couveignes in [Cou06], and following the construction of the CRS cryptosystem (§ A.1.3.2). More precisely, we explain how two characters, namely Alice and Bob, can create a secret key. After that, we demonstrate how the secret key can easily be recovered using an algorithm of Wesolowski [Wes22]. Contrary to the Drinfeld module version of CSIDH (§ A.2.3.2)—which is also based on a class group action—we use ordinary Drinfeld modules. This means that the endomorphism ring is an order in a quadratic imaginary function field § 2.1.5. Under the hypotheses of Chapter 7 (see § *Notations for the chapter* in § 7.1), the endomorphism ring is even the maximal order of the quadratic field generated by the characteristic polynomial of the Frobenius endomorphism; this quadratic field is imaginary hyperelliptic, and elements of the class group can be efficiently represented with Mumford coordinates (see § 1.2.4.3, § 7.2.4, and § 7.2.4).

Cryptosystem. We recall the notations of Chapter 7, and let $\mathcal{H}$ be an imaginary hyperelliptic curve over $\mathbb{F}_q$ defined by a bivariate polynomial

$$\chi_{\mathcal{H}} = X^2 + h(T)X - f(X).$$

Here, we have fixed an integer d, and f equals αp^m, for some m dividing d, and h has degree less than $d/2$. The ideal (p) is denoted $\mathfrak{p}$ and we let K be a finite extension of $\mathbb{F}_q$ with degree d, equipped with the $\mathbb{F}_q[T]$-characteristic morphism

$$\gamma : \mathbb{F}_q[T] \to \mathbb{F}_q[T]/\mathfrak{p} \to K.$$

We let $A_{\mathcal{H}}$ be the coordinate ring to $\mathcal{H}$, or equivalently, the ring of functions in $\mathbb{F}_q(\mathcal{H})$ that are regular on all points but the point at infinity of $\mathcal{H}$ (as $\mathcal{H}$ is supposed to be imaginary, the point at infinity of $\mathbb{P}^1(\mathbb{F}_q)$ extends to only one point at infinity on $\mathcal{H}$).

A key assumption we make is that $\chi_{\mathcal{H}}$ is the characteristic polynomial of the Frobenius endomorphism of some ordinary rank two Drinfeld $\mathbb{F}_q[T]$-module ϕ over K. This implies that

$$\mathrm{End}(\phi) \simeq A_{\mathcal{H}}$$

by Proposition 7.2.1, and subsequently that

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

by Lemma 7.2.11.

The conjunction of Proposition 7.2.4 and Theorem 7.2.9 implies that there is a free and transitive group action, denoted $*_K$, of

$$\mathrm{Pic}^0(\mathcal{H})$$

over

$$\mathrm{Dr}^\circ(\mathbb{F}_q[T], K)_{\chi_{\mathcal{H}}},$$

the category of Drinfeld $\mathbb{F}_q[T]$-modules over K that are isogenous to ϕ, seen as a concrete set.

Those objects yield a cryptosystem by following the construction of *hard homogeneous spaces* given in § A.1.3.1. The action is computed, in practice, with Algorithm 10.

Cryptanalysis. We now explain why this cryptosystem is insecure. Recall that, in Algorithm 10, isomorphism classes of Drinfeld modules are represented by j-invariants (§ 2.1.9.1). If ϕ is given by

$$\phi_T = \gamma(T) + g\tau + \Delta\tau^2,$$

its j-invariant is given by

$$\mathrm{j}(\phi) = \frac{g^{q+1}}{\Delta}.$$

Reciprocally, it is easily seen that if j is a nonzero of K, the Drinfeld module ψ given by

$$\begin{aligned} \psi_T &= \gamma(T) + \tau + j^{-1}\tau^2, \quad \text{if } j \neq 0, \\ \psi_T &= \gamma(T) + \tau^2, \quad \text{if } j = 0, \end{aligned}$$

has j-invariant j.

Let us say that Alice picked an element s_A of $\mathrm{Pic}_0(\mathcal{H})$, represented by a pair of Mumford coordinates (ρ_A, σ_A). In the process of the key exchange, Alice has computed an isomorphism class of Drinfeld modules

$$j_A = (\rho_A, \sigma_A) *_K \mathrm{j}(\phi).$$

The Mumford coordinates (ρ_A, σ_A) represent an ideal class $\overline{\mathfrak{a}}$ of $\mathrm{Cl}(A_{\mathcal{H}})$—they can be recovered from the representative $\mathfrak{a}$ as long as $\mathfrak{a}$ is *reduced*, meaning that it has no principal factor, as explained in [Coh+12, § 14.1.2]. In fact, nonzero ideals of $A_{\mathcal{H}}$ correspond to monic isogenies on ϕ, by a correspondence given in Lemma 7.3.3. It follows that if $\mathfrak{a}$ is reduced, then the isogeny defined by $\textsc{rgcd}(\phi_{\rho_A}, \tau_K - \phi_{\sigma_A})$ is the isogeny from ϕ to a Drinfeld module ϕ^A with smallest τ-degree, as otherwise it would have factors corresponding to endomorphisms of ϕ, that would themselves correspond to principal ideals of $A_{\mathcal{H}}$. To recover Alice's secret key, we thus start by picking a Drinfeld module ϕ^A such that $\mathrm{j}(\phi^A) = j_A$.

The first key step is to use Wesolowski's algorithm to compute bases of morphisms of Drinfeld modules [Wes22]. By iteratively calling its algorithms on the range of possible τ-degrees, which are bounded by $2d$, we find the isogeny u_A from ϕ to ϕ^A with the lowest τ-degree. Note that it does not matter which Drinfeld module ϕ^A is chosen in the isomorphism classes. Indeed, if ψ is another Drinfeld module with j-invariant j_A, and u is an isogeny from ϕ to ψ with lowest τ-degree, then it can be composed with an isomorphism $\psi \to \phi^A$ to yield an isogeny $\phi \to \phi_A$ with same τ-degree.

It is now a matter of retrieving the Mumford coordinates (ρ_A, σ_A), which correspond to the isogeny u_A we have computed. To do that, we compute the norm of u_A (*e.g.* using Algorithm 7) and let ρ be its monic generator. From this data, Algorithm 12 returns a factorization of the ideal corresponding to u_A. As u_A has minimal τ-degree, this ensures that the ideal is reduced. We then proceed to compute its Mumford coordinates under the isomorphism $\mathrm{Cl}(A_{\mathcal{H}}) \simeq \mathrm{Pic}^0(\mathcal{H})$, which are Alice's secret key. This breaks the cryptosystem.

Appendix A
A survey of Drinfeld modules in cryptography

We now propose to review the several attempts at using Drinfeld modules in cryptography. Given the similarities between Drinfeld modules and elliptic curves, and the fact that function field arithmetic is more efficient than that of number fields, we believe it is natural to try to use Drinfeld modules as alternatives to elliptic curves. However, this comes as a double-edged sword: while primitives are faster, they also are easier to break—in all previous attempts, including ours, they were proved insecure.

We first briefly review some of the predominant role of elliptic curves in cryptography (§ A.1)—this section can be safely skipped, and details are to be looked for in [Kob94]. We then review cryptographic primitives based on Drinfeld modules, in chronological order of their introductions.

A.1 Elliptic curves in cryptography

First of all, elliptic curves were used in computer algebra, with notable applications to primality testing and factorization.

A.1.1 For computer algebra

Goldwasser and Killian published in 1986 [GK86] a probabilistic Las-Vegas algorithm (that is, a randomized algorithm that either gives a correct answer or no answer at all) which decides if an input integer n is prime. Their idea is to derive a variant, in the setting of elliptic curves, of a primality test known as the *Pocklington criterion* [Kob87, § VI.3], where the ring $\mathbb{Z}/n\mathbb{Z}$ is replaced by the abelian group of $\mathbb{Z}/n\mathbb{Z}$-rational points $E(\mathbb{Z}/n\mathbb{Z})$ of an elliptic curve E; although $\mathbb{Z}/n\mathbb{Z}$ is not a field if n is composite, it is still possible to try and compute sums of points on E with coordinates in $\mathbb{Z}/n\mathbb{Z}$, by attempting to apply raw formulas for the chord and tangent's law. This operation may fail, in which case a new curve is picked. The strength of Goldwasser and Killian's method is that outputs of their algorithms include primality certificates. The algorithm, provided that it successfully gives an answer, is expected to run in polynomial time, and the certificates can be verified in deterministic polynomial time. Therefore, it is most common to use their method on integers that are strongly believed to be prime, for example having been tested with other faster probabilistic primality tests, like Miller and Rabin's method [Kob87, Page 130]. In [AM93], Atkin and Morain revised Goldwasser and Killian's method to create the ECPP primality algorithm, standing for *Elliptic Curve Primality Proving*, which is heuristically expected to run in $\tilde{O}(\log(n)^4)$ bit operations.

On the other hand, the *Elliptic Curve Method* (ECM), as introduced by Lenstra in [Mil86; Len87], is a mainstream factorization method. It is the elliptic curve analogue of Pollard's $p-1$ *method*. To

this date, the *Elliptic Curve Method*, which has subexponential asymptotic complexity, is for example used in intermediary computations of the *Number Field Sieve* algorithm, which as of 2024, holds many factorization records [Bou+20].

A.1.2 For pre-quantum cryptography

In pre-quantum cryptography, *i.e.* cryptography whose security can be bypassed using quantum algorithms, elliptic curves are notably used for *key exchange protocols*: protocols in which two parties—Alice and Bob—create a common password (more formally referred to a as a *private key*) then used to secure their communication. They can proceed as follows:

(i) As a preliminary step, Alice and Bob both publicly fix an elliptic curve E defined over a fixed finite field $\mathbb{F}_q$. They also agree on a point P of $E(\mathbb{F}_q)$, and make it public.

(ii) Then, Alice picks a random integer n, and sends $n \cdot P$ to Bob. The integer n is kept secret.

(iii) Bob follows by picks a random integer m and, sends $m \cdot P$ to Alice. The integer m is kept secret.

(iv) As the points of $E(\mathbb{F}_q)$ form an abelian group, Alice and Bob can both compute the point $(mn)\cdot P = m \cdot (n \cdot P) = n \cdot (m \cdot P)$ of $E(\mathbb{F}_q)$, which they independently do; they keep the result as their common secret key.

Provided that computing an integer ℓ knowing P and $\ell \cdot P$—a problem known as the *Elliptic Curve Discrete Logarithm* problem—is hard, then $mn \cdot P$ may not be computed efficiently. In other words, an adversary can theoretically solve this problem to find the secret key mn, but cannot do so in any practical time. Of course, this requires choosing q, E and P wisely; we do not go into details on this matter. This protocol is known as the *Elliptic Curve Diffie-Hellman* (ECDH) protocol [Kob87]. It is nowadays used in numerous practical protocols, and the *Elliptic Curve Discrete Logarithm* problem also supports the security of *authentification* and *signature methods*. However, while as of 2024, the most efficient methods on classical computer only achieve exponential complexity, Shor's quantum algorithm [Sho94] can break the *Elliptic Curve Discrete Logarithm* problem in quantum polynomial time.

A.1.3 For post-quantum cryptography

To prevent attacks by quantum computers (the Rivest-Shamir-Adleman cryptosystem [RSA78], more commonly known as RSA and one of the most widely used cryptographic primitives, is based on the hardness of integer factorization and can also be broken by Shor's algorithm), the American *National Institute of Standards and Technology* (NIST) opened a competition in 2016 to standardize *post-quantum* cryptographic protocols. Among the candidates, some—called *isogeny-based*—rely on the hardness of computing isogenies between elliptic curves (*i.e.* nonzero morphisms of groups that also are morphisms of algebraic curves). The first of this kind was the Couveignes-Rostovtsev-Stolbunov (CRS) cryptosystem [Cou06; RS06]. It uses a group action from the class group of the endomorphism ring of an ordinary elliptic curve to a set of isomorphism classes of elliptic curves. We define it in § A.1.3.2, after having introduced the necessary notion of *hard homogeneous space* (§ A.1.3.1).

A.1.3.1 Hard homogeneous spaces.

The following is a general framework to create *key exchange protocols*. Let G be an abelian group and X be a set acted upon by G. Alice and Bob can create a private key as follows.

(i) We assume that Alice and Bob have already agreed on G and X. They continue by agreeing on a point x in X, which they make public.

(ii) Then, Alice picks a random group element g_A, and sends $g_A \cdot x$ to Bob. The element g_A is kept secret.

(iii) Bob follows by picking a random group element g_B, and sends $g_B \cdot x$ to Alice. The element g_B is kept secret.

(iv) As the group G is abelian, Alice and Bob can both compute the element $(g_A g_B) \cdot x = g_A \cdot (g_B \cdot x) = g_B \cdot (g_A \cdot x)$ of X, which they independently do; they keep the result as their common secret key.

If the action of G on X is free and transitive, we say that X is a *principal homogeneous space* for G; if computing g knowing $g \cdot x$ and x is hard, we say that X is a *hard homogeneous space* for G. For more formal definitions, the reader is referred to [Cou06], where this framework was introduced. Hard homogeneous spaces are actually quite frequent:

— The ECDH protocol is based on a hard homogeneous space: if $P \in E(\mathbb{F}_q)$ is a point of order n, then $G = \mathbb{Z}/n\mathbb{Z}$ and X is the cyclic subgroup of $E(\mathbb{F}_q)$ generated by P. Its security is only pre-quantum.

— The *Diffie-Hellman key exchange protocol*—the first asymmetric cryptography protocol, introduced in 1976 [DH76] and still widely used—uses a pre-quantum hard homogeneous space: X is the group $\mathbb{F}_q{}^\times$ of nonzero elements in a finite field $\mathbb{F}_q$, and G is $\mathbb{Z}/(q-1)\mathbb{Z}$. Its security is only pre-quantum.

— The CRS cryptosystem, which we explain now.

A.1.3.2 The CRS key exchange protocol

The so-called CRS cryptosystem, named after Couveignes [Cou06] and Rostovstsev & Stolbunov [RS06], is a hard homogeneous space instantiated within the following setting. Let E be an ordinary elliptic curve on the finite field $\mathbb{F}_q$ (meaning that the endomorphism ring of E is commutative and strictly larger than $\mathbb{Z}$), and let $\mathrm{End}(E)$ denote the endomorphism ring of E. Let $\mathfrak{a}$ be an ideal in $\mathrm{End}(E)$. We now associate to $\mathfrak{a}$ a new elliptic curve E', and most importantly, an isogeny $\varphi_\mathfrak{a}$ from E to E'. To do this, consider the intersection of the kernels of all endomorphisms in $\mathfrak{a}$. This space is a finite subgroup of E, and as such, it defines an isogeny from E to a new elliptic curve. We call it E', and φ is the associated isogeny. If $\mathfrak{a}$ is principal, then φ is, up to isomorphism, a generator of $\mathfrak{a}$, so that E equals E'. One ends up defining an action from the class group G of $\mathrm{End}(E)$, to the set X of isomorphism classes of elliptic curves over $\mathbb{F}_q$ that are isogenous to E, which can be proved to be free and transitive.

Remark A.1.1. The endomorphism ring of E may not be a Dedekind domain. In that case talking about the class group of $\mathrm{End}(E)$ may not make sense. However, $\mathrm{End}(E)$ is always an order in an imaginary quadratic number field. In that context, and with some restriction to the ideals that can be considered, class groups can still be constructed, as explained in [Cox22, Chapter 2, Section 7]. More generally, $\mathrm{End}(E)$ is a Dedekind domain if and only if it is the maximal order, *i.e.* the ring of integers, of the imaginary quadratic field that contains it.

The CRS protocol, as of the time of writing this thesis, is considered secure, both in pre and post-quantum threat models. However the computation of the action takes too much time for a practical use [DKS18]. In that context, the CSIDH cryptosystem [Cas+18] has been proposed as a variant of the CRS cryptosystem, using supersingular elliptic curves (elliptic curves over a finite field whose endomorphism

ring is noncommutative). One drawback of CSIDH (which is also true of CRS) is that the order of the class group of the endomorphism ring cannot, in practice, be computed [BKV19]. Such a computation would make some isogeny-based key exchange protocols more efficient [Feo+23; CLP24]. The construction described in § A.2.4 aims at removing these drawbacks, but was ultimately proved insecure.

A.2 Drinfeld modules in cryptography

The principal attempts at using Drinfeld modules in cryptography are:

(i) Scanlon's description and subsequent cryptanalysis of two families of cryptosystems [Sca01]. The first is analogous to the Diffie-Hellman key exchange protocol, and based on a problem called the *Drinfeld module discrete logarithm* problem. The second is based on a problem called the *Drinfeld module inversion* problem, from which analogues of the Rivest-Shamir-Adleman (RSA) and El Gamal cryptosystems can be derived.

(ii) Gillard, Leprévost, Panchishkin and Roblot's attempt at defining a trapdoor function [Gil+03]. This was cryptanalysed by Blackburn, Cid and Galbraith in [BCG06]. The construction is also mentioned in [Pan03], where the attack of [BCG06] is acknowledged.

(iii) Joux and Narayanan's description and subsequent cryptanalysis of Drinfeld module analogues of the SIDH and CSIDH cryptosystem [JN19]. To our knowledge, [JN19] was never formally published.

(iv) Spaenlehauer and the present author's description of a Drinfeld module analogue of the CRS cryptosystem [LS22]. This construction is based on Chapter 7 and was broken by Wesolowski's algorithm to compute isogenies between Drinfeld modules (introduced in [Wes22] and explained in § 2.1.6).

We also refer to the valuable § 13.6 of Villa-Salvador's book [Vil06], which presents the cryptosystems of Scanlon and Gillard-Leprévost-Panchishkin-Roblot, as well as the attacks on them.

Notations. In all this section, $\mathbb{F}_q$ is a finite field with q elements and K is a finite extension of $\mathbb{F}_q$, such that $[K : \mathbb{F}_q] = d$. All Drinfeld modules considered here are Drinfeld $\mathbb{F}_q[T]$-modules (following Proposition 7.2.4, the primitive of § A.2.4 could alternatively be formulated with rank one Drinfeld $A_{\mathcal{H}}$-modules). If ϕ is a Drinfeld module, we recall from Definition 2.1.8 that the $\mathbb{F}_q[T]$-module associated to ϕ is the left $\mathbb{F}_q[T]$-module

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, z) & \mapsto & \phi_a(z) \end{array}$$

and denoted by $\mathbb{E}(\phi)$. If L is a subextension of $\overline{K}/K$, we let $\mathbb{E}(\phi)(L)$ denote the intersection of $\mathbb{E}(\phi)$ and L. For the purpose of this section, we also introduce the function

$$\iota : \quad K\{\tau\} \quad \to \quad \mathrm{End}_{\mathbb{F}_q}(K),$$

which to an Ore polynomial f associates the $\mathbb{F}_q$-linear endomorphism $f \mapsto f(x)$.

A.2.1 Scanlon (2001)

Scanlon proposes two families of cryptosystems, each based on a different problem. His constructions are defined for general Drinfeld A-modules, but we explain them for $A = \mathbb{F}_q[T]$ for simplicity.

— The first family is based on the *Drinfeld module discrete logarithm* problem. A cryptosystem based on this problem is proposed: the *Drinfeld module Diffie-Hellman* protocol. Knowing its classical counterpart, its definition is straightforward.

— The second family is based on the *Drinfeld module inversion* problem. Scanlon does not explicitly derive a cryptosystem from it, but he mentions that doing so would be easy, by following the constructions of the RSA and El Gamal cryptosystems. As an example, we derive the Drinfeld module RSA version of the cryptosystem, and explain how it relates more to cyclotomic function fields and rank one Drinfeld modules than to rank two Drinfeld modules.

A.2.1.1 The Drinfeld module discrete logarithm problem

Definition (*Drinfeld module discrete logarithm* problem)**.** Given two elements x and y of K, and a fixed Drinfeld module ϕ over K, the *Drinfeld module discrete logarithm problem* (DMDLP) consists in finding an element a in $\mathbb{F}_q[T]$ such that $\phi_a(x) = y$, provided that such a exists.

Cryptographic primitive. The *Drinfeld module Diffie-Hellman* cryptosystem is a key exchange protocol, Alice and Bob proceed as follows:

(i) As a preliminary step, Alice and Bob both publicly fix a Drinfeld $\mathbb{F}_q[T]$-module over K. They also agree on an element x of $\mathbb{E}(\phi)$, and make it public.

(ii) Then, Alice picks a random polynomial a in $\mathbb{F}_q[T]$, and sends $\phi_a(x)$ to Bob. The polynomial a is kept secret.

(iii) Bob follows by picking a random polynomial b in $\mathbb{F}_q[T]$, and sends $\phi_b(x)$ to Alice. The polynomial b is kept secret.

(iv) As $\mathbb{E}(\phi)$ is an $\mathbb{F}_q[T]$-module, Alice and Bob can both compute the element $\phi_{ab}(x) = \phi_a(\phi_b(x)) = \phi_b(\phi_a(x))$ of $\mathbb{E}(\phi)$, which they independently do; they keep the result as their common secret key.

Remark A.2.1. This primitive can be formulated with the language of principal homogeneous spaces, providing better symmetry with the Diffie-Hellman and Elliptic Curve Diffie-Hellman protocols (§ A.1.3.1). To do that, notice that

$$\mathfrak{a}_x = \{a' \in \mathbb{F}_q[T] : \phi_{a'}(x) = 0\}$$

is an ideal of $\mathbb{F}_q[T]$. One can consider the quotient group

$$G = \mathbb{F}_q[T]/\mathfrak{a}_x$$

and obtains the desired principal homogeneous space setting

$$X = \{\phi_{a'}(x) : \overline{a'} \in G\}.$$

Cryptanalysis. To break the cryptosystem, *i.e.* compute the private key $\phi_{ab}(x)$, it suffices to solve the DMDLP problem. Indeed, if one computes elements a' and b' such that $\phi_a(x) = \phi_{a'}(x)$ and $\phi_b(x) = \phi_{b'}(x)$, then the private key is recovered by computing $\phi_{a'b'}(x) = \phi_{a'}(\phi_{b'}(x)) = \phi_{a'}(\phi_b(x)) = \phi_b(\phi_{a'}(x)) = \phi_b(\phi_a(x)) = \phi_{ab}(x)$. Let then x and y be in K. Notice that the map

$$\begin{array}{rcl} \mathbb{F}_q[T] & \to & K \\ a & \mapsto & \phi_a(x) \end{array}$$

is $\mathbb{F}_q$-linear. Thus, we want to find the solution of an $\mathbb{F}_q$-linear system. The only apparent obstacle is that $\mathbb{F}_q[T]$ has infinite $\mathbb{F}_q$-dimension. However, we can consider

$$\iota : \quad K\{\tau\} \quad \to \quad \mathrm{End}_{\mathbb{F}_q}(K),$$

the map which to an Ore polynomial f associates the $\mathbb{F}_q$-linear endomorphism $z \mapsto f(z)$ of K. The composite $\iota \circ \phi$ then maps $\mathbb{F}_q[T]$ to a commutative sub-$\mathbb{F}_q$-algebra $\mathcal{A}$ of $\mathrm{End}_{\mathbb{F}_q}(K)$, which therefore has degree $\leqslant d$. And one can extract an $\mathbb{F}_q$-basis of $\mathcal{A}$ from the family

$$\{\mathrm{Id}, \iota(\phi_T), \ldots, \iota(\phi_{T^{d-1}})\}.$$

To finish, we look at the application

$$\begin{array}{rcl} {\mathbb{F}_q}^d & \to & K \\ (a_0, \ldots, a_{d-1}) & \mapsto & \sum_{i=0}^{d-1} a_i \phi_{T^i}(x). \end{array}$$

By fixing a basis of K over $\mathbb{F}_q$, we can compute its matrix M in polynomial time, which then gives an element a' such that $\phi_{a'}(x) = y$.

A.2.1.2 The Drinfeld module inversion problem

Definition (*Drinfeld module inversion* problem)**.** Given two elements x and y of K, a fixed Drinfeld module ϕ over K, and an element a in $\mathbb{F}_q[T]$ such that $\iota(\phi_a)$ is bijective, find b in $\mathbb{F}_q[T]$ such that $\iota(\phi_b)$ is the compositional inverse of $\iota(\phi_a)$.

Cryptographic primitive. With the definition of this problem, one would aim at defining an *encryption* protocol. More generally, we call *trapdoor* any instance of the following construction:

(i) the computation of an image $y = f(x)$ is fast (assuming a complexity model have been fixed);

(ii) recovering a preimage x of y is computationally hard, unless some extra information s is known.

We call f the *public key*, and s is the *secret key*. In cryptography, trapdoors can be used to receive encrypted messages; if Bob wants to be able to receive encrypted messages—even from people he does not share a secret key with—he can choose a trapdoor, openly publish the public key f, and keep the corresponding secret key s secret. To send a message x to Bob, Alice simply computes and sends $f(x)$ to Bob, who decrypts it with the help of s. In our case, we aim at defining an encryption primitive as follows:

(i) Bob picks a finite field K and a Drinfeld $\mathbb{F}_q[T]$-module over K.

(ii) Bob computes two elements a and b in $\mathbb{F}_q[T]$ such that the endomorphisms $\iota(\phi_a)$ and $\iota(\phi_b)$ are automorphisms and inverses of each other.

(iii) Bob openly publishes ϕ_a, for example as an Ore polynomial defined by its coefficients, and keeps any other data (including a) secret.

Then, to encrypt a message $x \in K$, Alice simply computes $\phi_a(x)$. Once received, Bob decrypts it by computing $\phi_b(\phi_a(x)) = x$.

Cryptanalysis. To be able to decrypt messages on behalf of Bob, it is enough to obtain a computational inverse of $\iota(\phi_b)$. As $\iota(\phi_b)$ is $\mathbb{F}_q$-linear, a computational inverse is given by the inverse matrix of $\iota(\phi_a)$.

Remark A.2.2. While it is not necessary to recover b, Scanlon explains how to find it in Proposition 3.

A.2.1.3 Discussion on the RSA cryptosystem

We now explain why the *Drinfeld module inversion problem* (§ A.2.1.2) is a natural analogue of the computational problem behind the RSA cryptosystem, an encryption primitive based on a trapdoor. If Bob wants to receive encrypted messages, he proceeds as follows:

(i) Bob picks two appropriate large prime integers p and q, and compute their product n. Knowing p and q, he can easily compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, φ being the Euler totient function.

(ii) Bob picks an integer $1 < e < \varphi(n)$ that is coprime to $\varphi(n)$. He then computes d, the inverse of e modulo $\varphi(n)$. This implies that the map

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & x^e \end{array}$$

is a multiplicative bijection of $\mathbb{Z}/n\mathbb{Z}$, whose inverse is given by

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & x^d. \end{array}$$

(iii) Bob openly publishes n and e, and keeps any other data secret.

To encrypt a message $x \in \mathbb{Z}/n\mathbb{Z}$, Alice would simply compute x^e. Upon receiving it, Bob decrypts it by computing $(x^e)^d = x^{ed}$, which equals x; this is because e has order $\varphi(n)$ and ed is 1 modulo $\varphi(n)$. The security of the cryptosystem comes from the fact that computing a compositional inverse of $x \mapsto x^e$ is hard. In fact, knowing n and $\varphi(n)$ is equivalent to knowing p and q. Factoring n is, to the extent of our knowledge, the best way for an attacker to decrypt encrypted messages. However, it is not proved whether or not breaking RSA, *i.e.* decrypting as much as one single message, is equivalent to factoring n; this is the *RSA conjecture*.

We now explain how this construction corresponds to that of Scanlon. Recall from § 2.2.2.2 that rank one Drinfeld modules over $\mathbb{F}_q(T)$ correspond to roots of unity. The latter can be described as the torsion of the $\mathbb{Z}$-module

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Q}^* & \to & \mathbb{Q}^* \\ (e, x) & \mapsto & x^e. \end{array}$$

The RSA trapdoor can be seen as a reduction modulo n of a multiplication endomorphism of $\mathbb{Q}^*$. For Drinfeld modules, § 2.2.2.2 states that the analogous construction is the following. We make $\mathbb{F}_q[T]$ act on $\mathbb{F}_q(T)$ via a Drinfeld $\mathbb{F}_q[T]$-module ϕ defined over $\mathbb{F}_q(T)$. In this context, the multiplication endomorphism $x \mapsto \phi_a(x)$ of $\mathbb{E}(\phi)(\mathbb{F}_q(T))$, where $a \in \mathbb{F}_q[T]$ is given, is never bijective. We obtain the cryptosystem of Scanlon by restricting $\mathbb{E}(\phi)(\mathbb{F}_q(T))$ to $\mathbb{F}_q[T]$, and quotienting $\mathbb{F}_q[T]$ to a finite field K.

A.2.2 Gillard-Leprévost-Panchishkin-Roblot (2003)

The construction of Gilles, Leprévost, Panchishkin and Roblot aims at making the *Drinfeld module inversion problem* safer by adding a non-linear layer [Gil+03]. It is also an encryption primitive. The authors also go in further details as to how Bob can generate its public and private keys (respectively ϕ_a and b in § A.2.1.2).

Cryptographic primitive. Let ϕ be an $\mathbb{F}_q[T]$-Drinfeld module over K. Recall that $\mathbb{E}(\phi)(K)$ is an $\mathbb{F}_q[T]$-module; as K is finite, $\mathbb{E}(\phi)(K)$ is finite, and there exists a polynomial f_ϕ of $\mathbb{F}_q[T]$ such that

$$\mathbb{E}(\phi)(K) \simeq \mathbb{F}_q[T]/(f_\phi).$$

Consequently, Bob can pick two polynomials b_1 and b_2 in $\mathbb{F}_q[T]$ that are coprime to f_ϕ; he then computes their respective inverses b_1' and b_2' modulo f_ϕ. This implies that the maps $\iota(\phi_{b_1})$ and $\iota(\phi_{b_2})$ are automorphisms, whose respective inverses are $\iota(\phi_{b_1'})$ and $\iota(\phi_{b_2'})$.

For the moment, all ingredients of the constructions are of linear nature, which is not enough for a secure cryptosystem. To bypass this issue, Bob picks a random permutation σ of K. He then publishes the composite map

$$f = \iota(\phi_{b_1}) \circ \sigma \circ \iota(\phi_{b_2})$$

as its public key. The private key is the inverse function of f, which is given by

$$f^{-1} = \iota(\phi_{b_2'}) \circ \sigma^{-1} \circ \iota(\phi_{b_1'}).$$

The public key f must be specified without leaking any information on b_1, σ and b_2. However, no matter the way of doing that, it suffices for an attacker to have the ability to compute a vast number of pairs $(m, f(m))$ to break the cryptosystem, *i.e.* recovering compositional inverse of f.

Remark A.2.3. The presentation of [Gil+03] slightly differs from ours. Instead of defining Drinfeld $\mathbb{F}_q[T]$-modules over a finite field, they rather define Drinfeld $\mathbb{F}_q[T]$-modules over the function field $\mathbb{F}_q(T)$, with the assumption that all coefficients defining the Drinfeld module are in the subring $\mathbb{F}_q[T]$. Let φ be such a Drinfeld module. The authors then pick a monic irreducible polynomial f of $\mathbb{F}_q[T]$ of degree d, and consider $\mathcal{B} = \mathbb{F}_q[T]/(f)$. This quotient is a finite field, and by reduction modulo (p), it is endowed with an $\mathbb{F}_q[T]$-module structure given by ϕ. This new module is denoted by $\mathcal{B}_\varphi$, and corresponds to our $\mathbb{E}(\phi)(K)$. The rest of the construction is the same.

Cryptanalysis. Sections of [Gil+03] entitled *Présentation pratique du protocole* and *Choix des paramètres* (sections are not numbered) explain further how Bob can pick the parameters q (which is in fact assumed to be a prime number), b_1, b_2, σ, etc. An important point of the cryptanalysis is the authors suggest choosing σ as a function of the form

$$\sigma(z) = z^e + \delta, \quad \forall z \in K,$$

where e is an integer and δ a random element of K. Section *Présentation pratique du protocole* suggests to publish the public key as a polynomial to evaluate, and Section *Choix des paramètres* proposes to keep e low as to minimize the degree of the polynomial. At the time of writing their articles, the authors suggested picking e to be either 5 or 7.

Under this specification, the cryptanalysis goes as follows. The attacker will be able to recover a compositional inverse of f with the sole knowledge on the method to encrypt messages f.

(i) The first step is to pick a value for e, *e.g.* $e = 5$. If this value is not correct, the cryptanalysis is performed again for another one.

(ii) The second step is to compute a large number of couples $(m, f(m))$. This step can easily be parallelized.

(iii) The idea is then to recover $\iota(\phi_{b_1})$ and $\iota(\phi_{b_2})$ by expressing them as sums of Frobenius endomorphisms, and treating coefficients as variables. Let F be the Frobenius endomorphism $x \mapsto x^q$ of K. To shorten notations, write

$$\begin{cases} \lambda_1 = \iota(\phi_{b_1}), \\ \lambda_2 = \iota(\phi_{b_2}). \end{cases}$$

There exists scalars $x_0, \dots, x_{d-1}$ and $y_0, \dots, y_{d-1}$ of $\mathbb{F}_q$ such that

$$\begin{aligned} \lambda_1^{-1} &= x_0 + x_1 F + \cdots + x_{d-1} F^{d-1}, \\ \lambda_2 &= y_0 + y_1 F + \cdots + y_{d-1} F^{d-1}. \end{aligned}$$

Consequently, for any couple $(m, f(m))$ computed in Step 2, one obtains the two relations

$$\begin{aligned} \lambda_1^{-1}(f(m)) &= x_0 + x_1 f(m)^q + \cdots + x_{d-1} f(m)^{q^{d-1}}, \\ \lambda_2(m) &= y_0 + y_1 m^q + \cdots + y_{d-1} m^{q^{d-1}}. \end{aligned}$$

The important feature is now to plugin the value for e and create a variable δ, giving the equation

$$\lambda_1^{-1}(f(m)) = \lambda_2(m)^e + \delta.$$

We thus have obtained N polynomial equations in $2d + 1$ variables and with coefficients in K, where N is the number of computed encrypted messages.

(iv) We now ought to solve the system obtained at the end of the previous step, to find values for the variables x_i, y_i, $0 \leqslant i \leqslant d - 1$, as well as δ. Several approaches are possible, and the authors of [BCG06] suggest using Gröbner bases techniques, or linearization techniques. The second method appears more efficient. It relies on developing (with respect to e) the equations, and replacing each product of variables $y_0^{e_0} \cdots y_{d_1}^{e_{d-1}}$ by a new formal variable $u_{(e_0,\dots,e_{d-1})}$. That is, we obtain an $\mathbb{F}_q$-linear system S in the variables $x_i, y_i, u_{(e_0,\dots,e_{d-1})}, \delta$, with the added constraint (nonlinear) that

$$y_0^{e_0} \cdots y_{d_1}^{e_{d-1}} = u_{(e_0,\dots,e_{d-1})}.$$

One then proceeds to solve the system S. Not adding in the above constraint, not all solutions are valid. However, one can take the constraint into account using Gröbner bases techniques. Provided that enough encrypted messages were computed, and that the guess for the value of e was correct, this leads to the recovery of a compositional inverse of the encryption function f.

Remark A.2.4. This attack is possible because of the specific form chosen for the permutation σ, and because the maps λ_1 and λ_2 are $\mathbb{F}_q$-linear functions on an extension of $\mathbb{F}_q$, which can therefore be expressed as sums of Frobenius endomorphisms. Then, the relatively small values suggested by the authors of the cryptosystem in Section *Choix des paramètres* (*e.g.* q is a prime number with 32 bits, $q^d > 2^{160}$) allow to generate the equations and run the cryptanalysis in about one minute (data provided by the authors of [BCG06], computations run on a 700 MHz Pentium III machine).

It is worth noting that the authors of the cryptosystem seem to fully acknowledge the attack of [BCG06]: in his course on Drinfeld modules and cryptography [Pan03], Panchishkin, who is one of the authors of [Gil+03], fully describes the attack of Blackburn-Cid-Galbraith (see § 9.2 and § 9.3).

A.2.3 Joux-Narayanan (2019)

The next construction was that of Joux and Narayanan, proposed in [JN19], which to our knowledge has not been formally published. Contrary to the 2001 and 2003 constructions, the authors look at the specific case of *post-quantum* cryptography. To do that, rather than to derive Drinfeld module analogues of well-known but *pre-quantum* primitives like the Diffie-Hellman and RSA cryptosystems, the authors take inspirations from primitives called *Supersingular Isogeny Diffie-Hellman* (SIDH) and *Commutative Supersingular Isogeny Diffie-Hellman* (CSIDH) [JD11; CD23]. The authors define the Drinfeld module analogues of SIDH and CSIDH, and subsequently claim their insecurity. Their constructions rely on supersingular rank two Drinfeld $\mathbb{F}_q[T]$-modules over a finite field.

A.2.3.1 The Drinfeld module analogue of SIDH

The *Supersingular Isogeny Diffie-Hellman* (SIDH) cryptosystem is a key exchange protocol [JD11]. Its security comes from using supersingular elliptic curves, whose ℓ-isogeny graph (the graph whose vertices are isomorphism classes of elliptic curves and the edges are ℓ-isogenies between them, ℓ being an integer) is a *Ramanujan graph*. The idea is that any two vertices in such a graph are connected by a very small path, which is computationally hard to find. To create a common secret key, Alice and Bob would each pick an integer ℓ_i, randomly walk in the ℓ_i-isogeny graph, and combine their respective arrival points to create their secret key. The protocol is secure under the assumption that recovering an isogeny between two elliptic curves is hard, even if a few images of torsion elements are known. This problem was proved easy in a series of articles started in 2022 by Castryck-Decru [CD23] and Maino-Martindale [Mai+23; Mai+23], that culminated in a publication of Robert [Rob23]. This happened as SIDH had recently entered a new round of the NIST competition to standardize new post-quantum cryptosystems.

Cryptographic primitive. Alice and Bob start by fixing a few objects. First, they let $\mathfrak{p}$ be a prime ideal of $\mathbb{F}_q[T]$. The finite field $\mathbb{F}_q[T]/\mathfrak{p}$ is denoted $\mathbb{F}_\mathfrak{p}$, and $\mathbb{F}_{\mathfrak{p}^2}$ is a degree two extension of $\mathbb{F}_\mathfrak{p}$. The authors then let L be a set of monic and degree one polynomials in $\mathbb{F}_q[T]$. From L, Alice and Bob generate two L-smooth elements P_A and P_B of $\mathbb{F}_q[T]$ (that is, the respective prime factors of P_A and P_B all lie in L), that are coprime. They now let ϕ be a rank two Drinfeld $\mathbb{F}_q[T]$-module over $\mathbb{F}_{\mathfrak{p}^2}$. It then is stated that P_AP_B should divide $\xi(\mathbb{E}(\phi)(\mathbb{F}_\mathfrak{p}))$, the Euler-Poincaré characteristic of $\mathbb{E}(\phi)(\mathbb{F}_\mathfrak{p})$.

Remark A.2.5. We do not fully understand this hypothesis, as it seems that the $\mathbb{F}_q[T]$-module $\mathbb{E}(\phi)(\mathbb{F}_\mathfrak{p})$ may not be well-defined if ϕ is only defined over $\mathbb{F}_{\mathfrak{p}^2}$, but not over $\mathbb{F}_\mathfrak{p}$. In fact, the assumption that P_AP_B divides $\xi(\mathbb{E}(\phi)(\mathbb{F}_{\mathfrak{p}^2}))$ (notice the 2 here) is the Drinfeld module analogue of an integer n dividing the order of $E(\mathbb{F}_{p^2})$, where E is an hyperelliptic curve defined over $\mathbb{F}_{p^2}$. Our understanding is that replacing $\mathbb{E}(\phi)(\mathbb{F}_{\mathfrak{p}^2})$ by $\mathbb{E}(\phi)(\mathbb{F}_p)$ would be equivalent to replacing $E(\mathbb{F}_{p^2})$ by $E(\mathbb{F}_p)$, which only seems to make sense if E is defined over $\mathbb{F}_p$. While it is possible that some P_AP_B-torsion elements lie in the prime field $\mathbb{F}_\mathfrak{p}$, the submodule they generate may not be $\mathbb{F}_\mathfrak{p}$-rational. To fix this, it is also possible to take ϕ defined over $\mathbb{F}_p$. However, doing so may hinder the targeted security of the cryptosystem, as the graph of a-isogenies, $a \in \mathbb{F}_q[T]$, of a supersingular Drinfeld $\mathbb{F}_q[T]$-module defined over $\mathbb{F}_p$ would likely not be a Ramanujan graph.

Under this assumption (see Remark A.2.5), Lemma 3.1 of [JN19] is called, claiming that both the P_A and P_B-torsion are defined over $\mathbb{F}_{\mathfrak{p}^2}$, and that there exist elements λ_1^A of $\mathbb{E}(\phi)(\mathbb{F}_\mathfrak{p})$ and λ_{-1}^A of $\mathbb{E}(\phi)(\mathbb{F}_{\mathfrak{p}^2})$ such that $(\lambda_1^A, \lambda_{-1}^A)$ is an $\mathbb{F}_q[T]$-basis of the P_A-torsion. The same would exist for the P_B-torsion with

elements $\lambda_1^B \in \mathbb{E}(\phi)(\mathbb{F}_p)$ and $\lambda_{-1}^B \in \mathbb{E}(\phi)(\mathbb{F}_{\mathfrak{p}^2})$ such that

$$\begin{cases} \mathbb{E}_{P_A}(\phi) = \lambda_1^A \mathbb{F}_q[T] \oplus \lambda_{-1}^A \mathbb{F}_q[T], \\ \mathbb{E}_{P_B}(\phi) = \lambda_1^B \mathbb{F}_q[T] \oplus \lambda_{-1}^B \mathbb{F}_q[T]. \end{cases}$$

Remark A.2.6. We do not fully understand Lemma 3.1 and its proof. If ϕ is defined over $\mathbb{F}_{\mathfrak{p}^2}$ but not $\mathbb{F}_p$, it seems that the Frobenius trace may be nonzero with ϕ still being supersingular—see Proposition 2.1.25. Arguably, supersingular Drinfeld modules over $\mathbb{F}_{\mathfrak{p}^2}$ with nonzero Frobenius trace are less frequent than those with zero Frobenius trace. However, Drinfeld modules of the latter kind do exist (see also the examples of § 2.1.4):

```
sage: Fq = GF(5)
sage: A.<T> = Fq[]
sage: Fp.<zp> = Fq.extension(2)
sage: Fptwo.<z> = Fp.extension(2)
sage: phi = DrinfeldModule(A, [Fptwo(zp), 1, z + z^2 + z^3])
sage: phi.is_supersingular()
True
sage: phi.frobenius_charpoly()
X^2 + (4*T^2 + T + 3)*X + 4*T^4 + 2*T^3 + 4*T + 1
sage: 4 * phi.characteristic()
4*T^2 + T + 3
```

With all of these, Alice and Bob should exchange a secret key as follows:

(i) Alice randomly picks two elements m_A and n_A in $\mathbb{F}_q[T]$. They have to be multiple of no element of L, and their degrees must be less than P_A. The secret key of Alice is the part

$$(m_A, n_A).$$

From there, Alice computes the sum

$$\phi_{m_A}(\lambda_1^A) + \phi_{n_A}(\lambda_{-1}^A) \in \mathbb{E}(\phi)(\mathbb{F}_{\mathfrak{p}^2}).$$

This sum generates a submodule E_A of $\mathbb{E}(\phi)$, that is also in the P_A-torsion of ϕ. Proposition 2.1.33 implies that the monic Ore polynomial whose kernel is E_A defines an isogeny u_A from ϕ, to some other Drinfeld module denote ϕ^A:

$$u_A : \quad \phi \quad \longrightarrow \quad \phi^A.$$

In particular, notice that

$$\mathrm{Ker}(\mathbb{E}(u_A)) \subset \mathbb{E}_{P_A}(\phi) \subset \mathbb{E}(\phi)(\mathbb{F}_{\mathfrak{p}^2}),$$

making u_A a P_A-isogeny. Alice proceeds to send ϕ^A to Bob.

(ii) Bob does the same manipulation, picking different random elements m and n, and using its own data. He ends up on a Drinfeld module ϕ_B, which he sends to Alice.

(iii) A key step is that Alice publicly sends the images of the basis elements λ_1^B and λ_{-1}^B under her isogeny u_A. Bob does the reciprocal manipulation, by sending the images of λ_1^A and λ_{-1}^A under his own secret isogeny u_B.

(iv) Now, Alice and Bob can construct their shared secret. On her side, Alice has received the points $u_B(\lambda_1^A)$ and $u_B(\lambda_{-1}^A)$ from Bob, as well as the Drinfeld module ϕ_B. She computes the submodule of $\mathbb{E}(\phi^B)(\mathbb{F}_{\mathfrak{p}^2})$ generated by the sum

$$\phi^B_{P_A}(u_B(\lambda_1^A)) + \phi^B_{P_A}(u_B(\lambda_{-1}^A)),$$

and the isogeny it corresponds to by Proposition 2.1.33. The codomain of this isogeny is a Drinfeld module denoted $\phi^{A\circ B}$.

(v) Bob does reciprocal manipulation and arrives to a Drinfeld module denoted $\phi_{A\circ B}$. Joux and Narayanan prove that the two Drinfeld modules are isomorphic in Paragraph *Shared Secret*. This means that their j-invariants are equal, and that this j-invariant can be chosen as the shared secret of Alice and Bob.

Remark A.2.7. Computing $\phi_{m_A}(\lambda_1^A) + \phi_{n_A}(\lambda_{-1}^A)$ is the Drinfeld module equivalent of computing $mP + nQ$, where m, n are two integers and P, Q to points of an elliptic curve. The only difference is that our coefficients are in $\mathbb{F}_q[T]$.

Cryptanalysis. Joux and Narayanan choose to prove that anyone can recover Alice's secret key (m_A, n_A). By symmetry, the same can be done for Bob's secret key, and the secret key common to Alice and Bob can be recovered. The key to recover (m_A, n_A) is that Alice not only sends ϕ^A, the Drinfeld module obtained from her isogeny u_A, but also the images $u_A(\lambda_1^B)$ and $u_A(\lambda_{-1}^B)$. We recover the secret key by interpolating u_A, which can be seen as an $\mathbb{F}_q$-linear endomorphism of the finite field $\mathbb{F}_{\mathfrak{p}^2}$. Recall that u_A is defined by the separable and monic Ore polynomial whose kernel is exactly E_A. As this kernel is contained in the P_A-torsion of ϕ, § 1.1.1.3 implies that that u_A, seen as an Ore polynomial, right-divides ϕ_{P_A}. The latter has τ-degree $2\deg(P_A)$. Without loss of generality, we can assume that $\deg(P_A)$ is less than $\deg(P_B)$, which means that

$$\deg_\tau(u_A) \leqslant 2\deg(P_B).$$

From there, it only remains to perform some linear algebra with the images $u_A(\lambda_1^B)$ and $u_B(\lambda_{-1}^B)$. Let them be respectively denoted x and y. As u_A is an isogeny from ϕ to ϕ^A, one has, for any element a of $\mathbb{F}_q[T]$, the following equality:

$$\begin{cases} u_A(\phi_a(x)) = \phi^A_a(u_A(x)) \\ u_A(\phi_a(y)) = \phi^A_a(u_A(y)). \end{cases}$$

As ϕ^A, $u_A(x)$ and $u_A(y)$ are all known, one can compute $u_A(\phi_\ell(x))$ and $u_A(\phi_\ell(y))$ for all ℓ in L that divides P_B; recall that L is a set of monic degree one polynomials of $\mathbb{F}_q[T]$ fixed before the key-exchange. There are $2\deg(P_B)$ of those polynomials ℓ. In consequence, we have computed the images of u_A under $2\deg(P_B)$ elements; but u_A defines an $\mathbb{F}_q$-linear endomorphism of $\mathbb{F}_{\mathfrak{p}^2}$, which, as an Ore polynomial, has τ-degree less than $2\deg(P)$. Thus, u_A is fully determined by those images, and can be recovered as the solution to an $\mathbb{F}_q$-linear system.

It now remains to recover (m_A, n_A). As we now know u_A, we can compute its kernel, which is a finite $\mathbb{F}_q$-vector space. By definition of u_A, this kernel contains

$$\phi_{m_A}(\lambda_1^A) + \phi_{n_A}(\lambda_{-1}^A).$$

The authors then state that the secret key (m_A, n_A) can be recovered from the kernel of u_A; no further details are given.

A.2.3.2 The Drinfeld module analogue of CSIDH

The *Commutative Supersingular Isogeny Diffie-Hellman* (CSIDH) cryptosystem is a key exchange protocol [CD23]. It is aimed at making a practical cryptosystem with the ideas behind the CRS protocol. One way to do so is to use *supersingular* elliptic curves instead of *ordinary* elliptic curves. Supersingular elliptic curves lead to faster computations, with the downside that their endomorphism ring is noncommutative. This means that defining a group action with the class group of the endomorphism ring, like in the CRS protocol (§ A.1.3.2, see also § A.2.4), is not directly possible. However, the endomorphism ring stills contains commutative subrings, and the set of endomorphisms that are defined on the prime field $\mathbb{F}_p$ is one of them. The CSIDH cryptosystem then follows the construction of CRS, considering the restricted ring of $\mathbb{F}_p$-endomorphisms, rather than the whole endomorphism ring. This construction is secure under the assumption that computing an isogeny between two supersingular elliptic curves is hard. As of the time of writing this thesis, this is considered to be the case [PW23].

Cryptographic primitive. To exchange a secret key, Alice and Bob start by fixing a prime ideal $\mathfrak{p}$ of $\mathbb{F}_q[T]$, and let p be its monic generator. They let $\mathbb{F}_\mathfrak{p}$ denote the field $\mathbb{F}_q[T]/\mathfrak{p}$ and fix a supersingular Drinfeld $\mathbb{F}_q[T]$-module ϕ defined over $\mathbb{F}_\mathfrak{p}$. Like in the SIDH protocol (§ A.2.3.1), they then let L be a set of monic degree one polynomials of $\mathbb{F}_q[T]$. Once again, it has to be assumed that the ℓ-torsion, for ℓ in L, is $\mathbb{F}_\mathfrak{p}$-rational. Therefore, the authors assume that any ℓ of L divides the Euler-Poincaré characteristic $\xi_{\mathbb{F}_q[T]}(\mathbb{E}(\phi)(\phi_p))$, so that they can apply Lemma 3.1—see Remarks A.2.5 and A.2.6. This lemma states that there exists an $\mathbb{F}_q[T]$-basis $(\lambda_1, \lambda_{-1})$ of the ℓ-torsion, such that λ_1 would be in $\mathbb{E}(\phi)(\mathbb{F}_\mathfrak{p})$ and λ_{-1} would be in $\mathbb{E}(\phi)(\mathbb{F}_{\mathfrak{p}^2})$. Assuming it is well-defined, this implies that the $\mathbb{F}_q[T]$-submodule of $\mathbb{E}_\ell(\phi)$ generated by λ_1 lies in $\mathbb{E}(\phi)(\mathbb{F}_\mathfrak{p})$. In particular, it is the kernel of a separable and monic isogeny u_ℓ by Proposition 2.1.33. We let

$$\ell * \phi$$

be the codomain of u_ℓ.

The authors now aim at making $*$ an action from the multiplicative monoid of L-smooth elements of $\mathbb{F}_q[T]$, on the set of isomorphism classes of Drinfeld modules that are isogenous to ϕ. Let ℓ be in L. First, $*$ is extended to powers of ℓ. Fix an integer $n \geqslant 2$. One can recursively define

$$\ell^n * \phi = \ell * (\ell^{n-1} * \phi).$$

It is not obvious that this operation is well defined. To see it, recall that two Drinfeld modules over a finite field are isogenous if and only if they have the same characteristic polynomial of the Frobenius endomorphism (Theorem 2.1.26). In particular, evaluated at 1, those characteristic polynomials have the same values, which is nothing else but a generator of the Euler-Poincaré characteristic of $\mathbb{E}(\phi)(\mathbb{F}_p)$, by [Gek91, Theorem 5.1(i)], and we have

$$\xi_{\mathbb{F}_q[T]}(\mathbb{E}(\phi)(\mathbb{F}_\mathfrak{p})) = \xi_{\mathbb{F}_q[T]}(\mathbb{E}(\ell^{n-1} * (\phi))(\mathbb{F}_\mathfrak{p})).$$

As a consequence, $\xi_{\mathbb{F}_q[T]}(\mathbb{E}(\ell^{n-1} * (\phi))(\mathbb{F}_\mathfrak{p}))$ is divided by any element of L, which is the only thing that $\ell^{n-1} * \phi$ has to verify besides being supersingular, which it does by being isogenous to ϕ. Consequently, the action of any power of an element ℓ of L on any Drinfeld module isogenous to ϕ is well-defined.

It remains to extend the definition of $*$ to arbitrary products in L. If ℓ and ℓ' are two coprime elements of L, one can define

$$(\ell\ell') * \phi = \ell * (\ell' * \phi)$$

or

$$(\ell\ell') * \phi = \ell' * (\ell * \phi).$$

The authors state that because the isogenies are $\mathbb{F}_p$-defined, the order of applications does not matter, which fully defines the action.

Remark A.2.8. The construction of Joux-Narayanan can likely be described in the language of *hard homogeneous spaces* (see § A.1.3.1), where the map $*$ would be seen as a group action from the class group of $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$, the ring of $\mathbb{F}_\mathfrak{p}$-endomorphisms of ϕ. In § A.2.4, we contemplate the creation of a *hard homogeneous space* based on Drinfeld modules and Algorithm 10.

Alice and Bob can then perform a key exchange:

(i) We assume that Alice and Bob have already agreed on a setting.

(ii) Then, Alice picks a random L-smooth polynomial s_A, and sends $s_A * \phi$ to Bob. The polynomial s_A is kept secret.

(iii) Bob follows by picks a random L-smooth polynomial s_B, and sends $s_B * \phi$ to Alice. The polynomial s_B is kept secret.

(iv) As $*$ is the action of a commutative monoid, Alice and Bob can both compute the Drinfeld module$(s_A s_B) \cdot \phi = s_A \cdot (s_B \cdot \phi) = s_B \cdot (s_A \cdot \phi)$, which they independently do; they keep the result as their common secret key.

Cryptanalysis. The authors claim breaking their cryptosystem in two steps. First of all, they derive a procedure to compute an isogeny with prescribed τ-degree between any two rank two Drinfeld modules (supersingular or not) on a finite field. This is done in the paragraph entitled *Testing existence of isogenies of prescribed τ-degrees*. Such isogenies can in any case be efficiently computed using the primitives of Wesolowski [Wes22] or Musleh [Mus23, § 7.3]—see § 2.1.6.

Remark A.2.9. It seems that the method employed by the authors to find an isogeny closely follows that of [CGS20, § 8]. In [CGS20], the authors propose Algorithm 8.1 as a mean to compute an $\mathbb{F}_q$-basis of $\mathrm{Hom}_n(\phi, \psi)$, where ϕ and ψ are two rank two Drinfeld $\mathbb{F}_q[T]$-modules over a finite field, and n is an integer. Theorem 8.1 implies that Algorithm 8.1 has exponential complexity in the n (this is because the norm map they consider is such that $|a| = q^{\deg(a)}$, for any a in $\mathbb{F}_q[T]$). On the contrary, the authors of [JN19] suggest that the algorithm has polynomial worst-case complexity. To understand, recall that the elements of $\mathrm{Hom}_n(\phi, \psi)$ are defined by Equation (2.1). Writing $\phi_T = \gamma(T) + g\tau + \Delta\tau^2$ and $\psi_T = \gamma(T) + g'\tau + \Delta'\tau^2$, one way to solve this system is to first compute the leading coefficient u_n of u by solving in x the equation

$$\Delta' X^{q^2-1} - \Delta^{q^n} = 0.$$

There are at most $q^2 - 1$ solutions in the ground field. If we let u_n, denote one of them, we can obtain a value u_{n-1}—which depends on u_n—by solving in x the equation

$$\Delta' X^{q^2-1} - \Delta^{q^{n-1}} X + g' u_n^q - u_n g^{q^n} = 0.$$

It has at most $q^2 - 1$ solutions in the ground field. We may again let u_{n-1} be one of them. By using Equation (2.1), we end up with a recursive system of equations; the equation in X to compute a coefficient u_k, $0 \leqslant k \leqslant n-2$ depends on two previously computed values u_{k+1} and u_{k+2}:

$$\Delta' X^{q^2} - \Delta^{q^n - k} X = u_{k+1} g^{q^{k+1}} - g' u_{k+1}^q + u_{k+1}(\gamma(T)^{q^{k+2}} - \gamma(T)). \tag{A.1}$$

Note that the coefficient u_{k+1} may come from any computed value for the coefficient u_{k+2}. If ϕ_T and ψ_T are monic, then the above equation is $\mathbb{F}_{q^2}$-linear. This assumption is realistic, as Alice and Bob can always pick such Drinfeld modules. In that case, the set of solutions of Equation A.1 is $u_k + \mathbb{F}_{q^2}$, where u_k is a particular solution. The solutions of the system 2.1 therefore consists of vectors of $n+1$ elements, and each coefficients depends on its previous two coefficients. It follows that the space of possible solutions has the structure of a tree in which each leaf has either zero or q^2 nodes (or q, under some hypotheses, see [JN19]). Finding a solution to our problem means finding a path in the tree that has length $n+1$.

Our understanding is that the authors of [JN19] suggest it is not necessary to explore all the tree (and compute it at the same time) to find a solution. Indeed, it seems they claim that if $(u_0 + \lambda_0, \dots, u_n + \lambda_n)$ is a solution that defines an isogeny, and that the λ_i's are in $\mathbb{F}_q$, then the vector $(u_0, \dots, u_n)$ should also define a solution. This seems wrong, as per the following counterexample:

```
sage: Fq = GF(2)
sage: Fp.<z> = Fq.extension(3)
sage: A.<T> = Fq[]
sage: phi = DrinfeldModule(A, [z, 1, z])
sage: psi = DrinfeldModule(A, [z, 0, z])
sage: phi.is_isogenous(psi)
True
```

Here, `phi` and `psi` are supersingular and the degree d is odd. By computing the characteristic polynomial of the Frobenius endomorphism of both `phi` and `psi`, it is easily checked that the two Drinfeld modules are isogenous. We can then pick one isogeny, and test if we obtain a new isogeny by substracting the $\mathbb{F}_q$-components of the coefficients:

```
sage: Hom(phi, psi).basis()
[Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> z*t^2 + t + z
  To:   Drinfeld module defined by T |--> z*t^2 + z
  Defn: z*t^2 + (z + 1)*t + 1, Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> z*t^2 + t + z
  To:   Drinfeld module defined by T |--> z*t^2 + z
  Defn: z*t^5 + (z + 1)*t^4 + (z^2 + z)*t^2 + t + z^2 + z, Drinfeld Module morphism:
  From: Drinfeld module defined by T |--> z*t^2 + t + z
  To:   Drinfeld module defined by T |--> z*t^2 + z
  Defn: (z^2 + z + 1)*t + z^2]
sage: t = phi.ore_variable()
sage: isogeny = z*t^2 + (z + 1)*t + 1
sage: isogeny * phi(T) == psi(T) * isogeny
True
sage: candidate = z*t^2 + (z)*t
sage: candidate * phi(T) == psi(T) * candidate
False
```

We rather think that exploring all the tree is necessary, and agree with the conclusions of [CGS20, § 8]. We also suggested an analysis of the procedure to find an isogeny in [LS22, § 4.2]. However, we stress that while solving the system recursively may not be the most efficient approach, there is no doubt that Wesolowski's approach completely solves the problem [Wes22].

The paragraph entitled *Recovery of the secret* then assumes that an isogeny u_A between ϕ and $s_A * \phi$ has been computed. Using the algorithm of Wesolowski, one may assume that u_A has the smallest τ-degree of all isogenies $\phi \to s_A\phi$. For any ℓ in L, it is easily checked if, as Ore polynomials, u_A is divided by u_ℓ; one may use one of the algorithms detailed in § 4.3.1.2. The authors suggest to factor u_A as a product of powers of isogenies u_ℓ, which would lead to the recovery of the secret key s_A of Alice.

Remark A.2.10. We are not sure why the isogeny with smallest τ-degrees would factor as a product of ℓ-isogenies. However, the conclusion might still be valid by formulating the cryptosystem using the class group of $\mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi)$ and using an adaptation of the methods of § 7.3.2.

A.2.4 Leudière-Spaenlehauer (2022)

The last proposal we review was proposed jointly with Pierre-Jean Spaenlehauer in [LS22]. It is a hard homogeneous space based on the group action computed with 10. We discuss it in § 7.4.2.

A.3 Discussion

Due to their similarities with elliptic curves, Drinfeld modules had for long been considered to replace elliptic curves in cryptography. In the previous sections, we have seen that all previous attempts had failed. All have in common the adaptation of an already existing cryptosystem. Even the RSA cryptosystem—which is based on rank one $\mathbb{Z}$-modules rather than elliptic curves, which are rank two objects—found a Drinfeld module analogue (§ A.2.1.2). In all instances, the cryptosystems we presented were broken by exploiting a certain structure of finite $\mathbb{F}_q$-vector space, leading to the recovery of a secret information by solving a finite $\mathbb{F}_q$-linear system. For the constructions of Joux-Narayanan (§ A.2.3) and Leudière-Spaenlehauer (§ A.2.4), the key is that morphisms of bounded τ-degree between two Drinfeld $\mathbb{F}_q[T]$-modules over a finite field form a finite $\mathbb{F}_q$-vector space, which can be computed using the primitives of [Wes22]. The constructions of Scanlon (§ A.2.1) and Gillard-Leprévost-Panchishkin-Roblot (§ A.2.2) were broken by finding *ad hoc* finite $\mathbb{F}_q$-linear systems. It is undeniable that the methods employed to break those cryptosytems are rather elementary, at least by the standards of modern computer algebra, and that the cryptosystems were broken rapidly after the submission. All in all, the constructions we have seen cover most areas (that is, cryptosystems based on rank one objects like RSA, and pre and post-quantum cryptosystems based on elliptic curves) in which Drinfeld modules could be anticipated to serve. Although this is a bad start, which brought a lot of valuable insights, this does not mean that Drinfeld modules will never be useful in cryptography.

(i) The first reason for that is that Drinfeld modules are yet to be used in a completely original way. For the moment, they have only been considered as replacements of other objects, and we are not aware of any work that aims at using *ad hoc* methods for Drinfeld modules. For example, Drinfeld modules of rank greater than three, or on a general function ring A, could possibly be used.

(ii) The second reason is that to this day Drinfeld modules have only been considered in *constructive* applications, like building a cryptosystem. However, we learnt that many problems underlying the security of classical cryptosystems have Drinfeld module analogues that are easily broken. Establishing a bridge between those two worlds, *i.e.* between computational problems in characteristic zero and computational problems in characteristic p, could lead to using Drinfeld modules and the arithmetics of function fields to attack important problems of characteristic zero.

Appendix B
Résumé en français

Cette thèse de doctorat traite de l'algorithmique des modules de Drinfeld. Nos résultats sont principalement algorithmiques et logiciels, et sont motivés par des applications au calcul formel et à la cryptographie. Ces travaux s'inscrivent dans la lignée de ceux commencés dans la dernière décennie, qui établissent l'algorithmique des modules de Drinfeld comme un sujet de recherche en soi [Car18; DNS21; MS19; CGS20; MS23; Ayo23; Mus23].

B.1 Aperçu des contributions

Nous avons deux contributions algorithmiques et une contribution logicielle.

B.1.1 Calcul de polynômes caractéristiques d'endomorphismes et de normes d'isogénies

Nous calculons efficacement des polynômes caractéristiques d'endomorphismes de modules de Drinfeld et des normes d'isogénies de modules de Drinfeld. Nos méthodes sont décrites pour des rangs, corps de base, et anneaux de fonctions, tous arbitraires. Dans le cas où l'anneau de fonction est $A = \mathbb{F}_q[T]$, nous proposons des analyses de complexité asymptotique rigoureuses, et des implémentations. Ces algorithmes et leurs implémentations sont fortement optimisés dans le cas suivants : quand le corps de base est fini, ou quand l'endomorphisme considéré est l'endomorphisme de Frobenius. Nous comparons les méthodes de la littérature sur le calcul de polynômes caractéristiques d'endomorphismes ou de normes d'isogénies.

À notre connaissance, nos travaux constituent les premiers à étudier le problème du calcul de polynômes caractéristiques d'endomorphismes et de normes d'isogénies dans le cas où l'anneau de fonctions A n'est pas restreint à $A = \mathbb{F}_q[T]$. Ces résultats sont issus d'une collaboration avec Xavier Caruso [CL23]. Ils constituent les chapitres 4, 5 et 6.

Les deux premiers de ces chapitres sont basés sur une même philosophie : le polynôme caractéristique (resp. la norme d'une isogénie) peut se lire comme le polynôme caractéristique (resp. le déterminant) de l'action de l'endomorphisme (resp. de l'isogénie) sur les motifs d'Anderson. Nous pensons que cette approche basée sur la dualité entre les modules de Drinfeld et les motifs d'Anderson a vocation à être employée plus systématiquement pour traiter des algorithmiques sur les modules de Drinfeld.

Enfin, les résultats du chapitre 6 ne portent que sur le cas de l'endomorphisme de Frobenius. Ils interprètent son polynôme caractéristique comme une norme réduite dans une algèbre centrale simple.

B.1.2 Calcul d'une action de groupe issue de la théorie du corps de classes des corps de fonctions

Dans le chapitre 7, nous nous proposons de calculer une action de groupe issue de la théorie du corps de classes des corps de fonctions. Plus prosaïquement, la résolution de ce problème algorithmique était motivée par la cryptographie, et plus précisément la cryptographie dite *post-quantique*. Cette branche de la cryptographie vise à établir des protocoles cryptographiques qui résistent non seulement aux attaques menées par des ordinateurs classiques, mais aussi à celles menées par des ordinateurs quantiques. Ces derniers, s'ils étaient amenés à exister, auraient en effet la capacité de mettre à mal de nombreuses constructions actuelles, en ce qu'ils peuvent efficacement factoriser des entiers, ou calculer des logarithmes discrets, grâce à des implémentations de l'algorithme de Shor [Sho94].

L'action de groupe que nous calculons est en fait une « version modules de Drinfeld » d'une action de groupe bien connue en cryptographie post-quantique : celle qui est à l'origine du cryptosystème de Couveignes-Rostovtsev-Stolbunov [CL09; RS06]. Dans cette action de groupe, le groupe agissant est le groupe de classes d'un ordre dans un corps de nombres quadratique imaginaire, et il agit sur l'ensemble des classes d'isomorphismes de courbes elliptiques qui ont multiplication complexe dans ce corps. Un problème de cette construction, malgré sa sécurité, est sa faible efficacité pratique [DKS18].

Nous nous proposons donc d'établir un algorithme efficace pour calculer l'équivalent de cette action de groupe dans le monde des modules de Drinfeld. Toutefois, comme les travaux de Wesolowski l'ont montré [Wes22], cette action de groupe ne pourra pas être employée de manière robuste en cryptographie, ou du moins pas en application directe de la méthode développée dans la primitive CRS. Cependant, nos résultats montrent une nouvelle fois la force des modules de Drinfeld pour obtenir des algorithmes efficaces, tant en théorie qu'en pratique. Sur des tailles cryptographiques, notre implémentation C++ (basée sur la bibliothèque NTL) permet de calculer un échange de clefs en une poignée de millisecondes.

La rapidité de cette méthode est permise par l'interprétation suivante : dans le contexte des modules de Drinfeld ordinaires de rang 2 sur un corps fini (qui doit vérifier certaines autres hypothèses données dans le chapitre), le groupe de classes peut parfois se réinterpréter comme le groupe de Picard de degré zéro d'une courbe hyperelliptique. Cette courbe hyperelliptique n'est nulle autre que la courbe définie par le polynôme caractéristique du Frobenius, qui est un polynôme bivarié dans $\mathbb{F}_q[T][X]$ — dans le cas des courbes elliptiques, ce polynôme est univarié et dans $\mathbb{Z}[X]$, et ne définit donc pas *a priori* une courbe algébrique.

À cette première observation s'ajoute la suivante : dans le cas des modules de Drinfeld, on peut contourner le besoin de travailler avec des noyaux d'isogénies vivant dans de grandes extensions, en manipulant directement les polynômes de Ore qui les définissent. Les polynômes de Ore vivent dans un espace qui existe indépendamment de la théorie des modules de Drinfeld. Cet espace est extrêmement structuré : c'est un anneau euclidien à gauche, pour une notion de degré propre aux polynômes de Ore (on parle de *τ-degré*). Par chance, cette structure euclidienne est compatible avec l'arithmétique des noyaux d'isogénies de modules de Drinfeld. C'est la combinaison de ces deux observations qui nous permet d'obtenir un algorithme très compétitif. Tous ces résultats sont le fruit d'une collaboration avec Pierre-Jean Spaenlehauer [LS24].

B.1.3 Implémentation SageMath des modules de Drinfeld

La dernière contribution de cette thèse n'est pas algorithmique, mais logicielle. Avec l'aide de David Ayotte, Xavier Caruso, et Joseph Musleh, nous avons proposé la toute première implémentation d'une

bibliothèque de calcul sur les modules de Drinfeld qui soit directement intégrée à SageMath. C'est même, à notre connaissance, la première bibliothèque de ce genre qui soit intégrée à un outil numérique de calcul formel majeur. Cette implémentation a fait l'objet d'une *software presentation* à la conférence ISSAC [Ayo+23].

Nous avons implémenté de nombreuses fonctionnalités. En premier lieu, nous donnons accès à des structures de données pour les modules de Drinfeld, leur catégorie, leurs morphismes, isogénies et endomorphismes, et leurs espaces de morphismes. Sur ces modules de Drinfeld, peuvent être calculés le rang, la hauteur, l'action de $\mathbb{F}_q[T]$ sur le corps de base. Si un polynôme de Ore provient du module de Drinfeld via un élément de $\mathbb{F}_q[T]$, cet élément peut être retrouvé. Les algorithmes de Wesolowski et Musleh pour calculer des bases d'espaces de morphismes sur $\mathbb{F}_q$ ou sur $\mathbb{F}_q[\pi]$ (π étant un endomorphisme de Frobenius peuvent être calculés) sont implémentés. Tous les algorithmes de calcul de polynômes caractéristiques d'endomorphismes sont implémentés, et le meilleur algorithme est automatiquement sélectionné en fonction des paramètres d'entrée ; il demeure possible de choisir un algorithme spécifique en spécifiant un mot-clef. Des fonctionnalités sur la théorie analytique des modules de Drinfeld (séries exponentielle et logarithme, polynômes de Goss) sont également disponibles.

Outre ces fonctionnalités, l'effort de développement a été porté sur la pérennité du code, sa facilité d'utilisation et la qualité de sa documentation. Notre objectif était de créer un outil généraliste, que toute personne intéressée par l'arithmétique des modules de Drinfeld pourrait intégrer à son processus de recherche. Nous avons en particulier veillé à agrémenter la documentation de nombreux exemples, et avons fait en sorte que l'interface soit la mieux intégrée possible à l'écosystème SageMath. Depuis la première version, publiquement intégrée à la version 10.0 de SageMath, de nombreuses autres contributions ont été ajoutées, ou sont en développement.

B.2 Résumé des chapitres

Nous proposons à présent un résumé de chaque chapitre. Il y a deux chapitres de prérequis, et cinq chapitres de contributions, suivis d'une annexe.

B.2.1 Chapitre 1

Ce chapitre expose les prérequis nécessaires sur les polynômes de Ore, en géométrie algébrique, et en algorithmique.

Pour la géométrie algébrique, les objectifs principaux sont la définition des courbes algébriques, de leurs corps de fonctions, des courbes hyperelliptiques imaginaires, et des coordonnées de Mumford. Pour ce faire, nous définissons les variétés et courbes algébriques affines, ainsi que les notions associées suivantes : points rationnels, corps de fonctions, dimension, points singuliers et non-singuliers, pôles et zéros, et les anneaux de valuation discrète que nous associons à des points non-singuliers. Nous étendons ensuite ces définitions aux variétés et courbes algébriques projectives. Il est alors possible de définir les courbes hyperelliptiques imaginaires, ainsi que leur groupe de Picard de degré zéro. Nous expliquons ensuite comment décrire ce groupe de Picard à l'aide de coordonnées de Mumford.

L'exposition sur les polynômes de Ore est très classique : définitions, divisions Euclidienne de Ore. Une particularité est que nous étudions aussi certains polynômes de Ore généralisés ; les nôtres n'ont pas de dérivation, mais l'endomorphisme de corps qui les définit n'est pas restreint au seul Frobenius.

Enfin, nous précisons notre modèle de calcul, et rappelons quelques résultats algorithmiques sur :

(i) L'algorithmique des corps finis. Nous précisions comment les opérations arithmétiques sont comptées, et suggérons plusieurs méthodes de calcul et complexités pour l'application de l'endomorphisme de Frobenius (*i.e.* mettre à la puissance q, lorsque le corps est une extension de $\mathbb{F}_q$).

(ii) L'algorithmique des polynômes de Ore. Nous énonçons les résultats de Caruso et Le Borgne sur la multiplication rapide des polynômes de Ore, et les conséquences de leurs travaux sur le calcul efficace de divisions euclidiennes à droite, et de plus grands diviseurs communs à droite. Nous mentionnons que l'algorithmique classique d'Euclide est donné dans nos contributions, et que sa complexité asymptotique y est analysée.

(iii) L'algorithmique des matrices. Plus précisément, nous nous concentrons sur le calcul de déterminants et de polynômes caractéristiques de matrices à coefficients dans un anneau de polynômes (ces polynômes ayant leurs coefficients dans un corps fixé). Des méthodes *ad hoc*, plus adaptées à nos besoins, sont proposées dans les contributions.

B.2.2 Chapitre 2

Ce chapitre présente les prérequis nécessaires sur les modules de Drinfeld. Il est divisé en deux parties.

(i) La première traite de $\mathbb{F}_q[T]$-modules de Drinfeld : les modules de Drinfeld pour lesquels l'anneau de fonctions de base est $\mathbb{F}_q[T]$. C'est le cas le plus simple, et le plus étudié, en tous cas d'un point de vue algorithmique.

(ii) La deuxième partie passe des $\mathbb{F}_q[T]$-modules de Drinfeld aux modules de Drinfeld généraux, c'est à dire ceux pour lesquels aucune hypothèse particulière n'est faite sur l'anneau de fonctions A. Dans cette partie, nous reprenons les définitions et énoncés donnés dans la première partie, et terminons par quelques développements mathématiques qui ne sont pas nécessaires dans la suite, mais qui nous semblent mettre en valeur la force de la théorie des modules de Drinfeld.

Enfin, dans tout ce chapitre, la relation entre modules de Drinfeld et motifs d'Anderson est mise en avant. Formellement, la catégorie des modules de Drinfeld correspond à une sous-cagégorie des motifs d'Anderson, *via* un foncteur contravariant. Nous insistons sur le fait que lorsque l'anneau de fonctions est restreint à $\mathbb{F}_q[T]$, le motif d'Anderson est un module libre de rang r (le rang du module de Drinfeld) sur un anneau de polynômes ($K[T]$, où K est le corps de base du module de Drinfeld). Nous proposons des méthodes algorithmiques pour l'arithmétique de base des motifs d'Anderson. Cette relation entre les modules de Drinfeld et les motifs d'Anderson, couplée à ces méthodes, est indispensable pour nos contributions, et nous gageons que l'un des apports de cette thèse est de mettre en lumière la pertinence de l'utilisation des motifs d'Anderson pour résoudre des problèmes algorithmiques sur les modules de Drinfeld.

B.2.2.1 $\mathbb{F}_q[T]$-modules de Drinfeld

Une particularité de notre exposition est de donner nos exemples (théoriques ou algorithmiques) sous forme de code SageMath. Plus précisément, nous présentons des requêtes et la réponse de SageMath, tel qu'un utilisateur ou une utilisatrice les observerait dans la console. Notre objectif est de mettre en valeur l'effectivité pratique des modules de Drinfeld et de notre contribution logicielle (le chapitre 3 est entièrement dédié à cette implémentation).

Les énoncés présentés dans la première partie sont très classiques. Dans l'ordre : $\mathbb{F}_q[T]$-modules de Drinfeld et motifs d'Anderson. On associe à un module de Drinfeld un $\mathbb{F}_q[T]$-module (l'ensemble sous-jacent est une clôture algébrique fixée du corps de base). Cela mène à considérer la notion de $\mathbb{F}_q[T]$-caractéristique (un idéal de $\mathbb{F}_q[T]$, et non un entier de $\mathbb{Z}$), la notion de torsion, et les modules de Tate $\mathfrak{a}$-adiques : les objets qui encodent la structure de toutes les $\mathfrak{a}^n$-torsion, où $\mathfrak{a}$ est un certain idéal de $\mathbb{F}_q[T]$ préalablement fixé, et n varie dans les entiers positifs. Il est dit que le module de Tate (où un idéal $\mathfrak{a}$ a été fixé) est un foncteur, ce qui permet d'associer à tout endomorphisme de module de Drinfeld un endomorphisme sur son module de Tate. Le polynôme caractéristique d'un endomorphisme de module de Drinfeld est alors défini comme le polynôme caractéristique de l'action dudit endomorphisme sur le module de Tate (cette action étant bien une application linéaire sur un module libre de rang fini). Quelques propriétés sont énoncées.

Suite à cela, sont énoncés les résultats de structure de l'anneau d'endomorphismes d'un module de Drinfeld de rang deux. Les énoncés sont similaires à ce que l'on trouve pour les courbes elliptiques, exception faite d'un phénomène propre aux modules de Drinfeld : il existe des modules de Drinfeld de rang deux qui soient supersinguliers et dont l'anneau d'endomorphisme soit un ordre dans un corps de fonctions quadratique imaginaire, et non dans une algèbre de quaternions. Cette classification suppose connues les notions d'ordinarité et de supersingularité, qui sont définies après la notion de $\mathbb{F}_q[T]$-caractéristique.

Ces énoncés de classification de l'anneau d'endomorphismes ne sont à ce jour pas effectifs. Nous présentons des descriptions alternatives de l'anneau d'endomorphismes permettant de pallier ce problème. Plus généralement, l'espace des morphismes entre deux modules de Drinfeld est à la fois : un $\mathbb{F}_q$-espace vectoriel, un $\mathbb{F}_q[T]$-module, et, dans le cas des corps finis, un $\mathbb{F}_q[\pi]$-module, où π est l'endomorphisme de Frobenius du domaine. Nous mentionnons les algorithmes (et leurs implémentations par Musleh) de Wesolowski et Musleh pour calculer des bases sur ces espaces.

Le reste de la section est d'avantage dédié aux isogénies générales qu'aux endomorphismes. Cela sert dans toute la thèse. La notion de séparabilité est présentée, ainsi que la plupart des propriétés classiques qui y sont liées. Vient alors la notion de norme, dont le calcul effectif est un sujet central de cette thèse. Enfin, nous présentons les j-invariants pour les modules de Drinfeld, et mentionnons qu'ils permettent d'encoder les classes d'isomorphisme.

B.2.2.2 Modules de Drinfeld généraux

Cette section est bien plus brève. Elle est principalement utile pour deux raisons. Dans le chapitre 7, nous avons besoin d'une correspondance bijective entre certains $\mathbb{F}_q[T]$-modules de Drinfeld ordinaire de rang 2 et des modules de Drinfeld généraux. Nos travaux de calcul de normes d'isogénies et de polynômes caractéristiques de modules de Drinfeld sont à notre connaissance les premiers aborder les modules de Drinfeld généraux d'un point de vue algorithmique, sans se restreindre aux $\mathbb{F}_q[T]$-modules de Drinfeld.

Cette section, hormis les mentions culturelles qui la terminent, consiste essentiellement à étendre les définitions et énoncés que nous avons vus pour les $\mathbb{F}_q[T]$-modules de Drinfeld. Quand c'est pertinent, nous mentionnons en quoi travailler sur un anneau général est algorithmiquement plus complexe que le faire sur $\mathbb{F}_q[T]$, qui est principal. Nous définissons aussi la notion de *restriction de modules de Drinfeld*.

B.2.3 Chapitre 3

Ce premier chapitre de contributions constitue la présentation de notre implémentation des modules de Drinfeld dans SageMath. Il s'agit du premier projet logiciel de ce genre à être directement intégré dans un logiciel de calcul mathématique majeur. SageMath est un projet *logiciel libre* ; notre implémentation a été

développée en étroite collaboration avec la communauté, de façon à obtenir une interface la plus pérenne, et la mieux intégrée possible.

Ce chapitre est divisé en deux sections :

(i) Dans la première section, nous proposons une liste détaillée des fonctionnalités de notre implémentation. Cette liste comprend explications et exemples.

(ii) Dans la deuxième partie, nous expliquons certaines de nos décisions d'interface. Par exemple, nous présentons en détail les options possibles pour le type de base des modules de Drinfeld, et l'option que nous avons finalement choisie.

B.2.4 Chapitre 4

Ce chapitre présente un algorithme de calcul de polynômes caractéristiques d'endomorphismes de modules de Drinfeld. Sa force est de fonctionner en grande généralité : pour n'importe quel corps de base, endomorphisme, rang, et anneau de fonctions. Dans le cas où l'anneau de fonctions est $\mathbb{F}_q[T]$, nous proposons une analyse de complexité, et déclinons l'algorithme en plusieurs variantes optimisées, utilisables quand le corps de base est fini, ou quand l'endomorphisme considéré est l'endomorphisme de Frobenius. Dans ces cas là, deux paramètres importants sont le coût de la division euclidienne de polynômes de Ore, et le coût de la mise à la puissance q dans le corps de base. Le but de nos variantes est essentiellement de minimiser ces coûts. Nous proposons également des méthodes *ad hoc* pour calculer le polynôme caractéristique des matrices à coefficients polynomiaux qui apparaissent dans nos calculs.

Dans le cas où A est $\mathbb{F}_q[T]$, l'algorithme est relativement simple : le polynôme caractéristique d'un endomorphisme est obtenu comme le polynôme caractéristique de l'action de cet endomorphisme sur le motif d'Anderson du module de Drinfeld. Comme le motif d'Anderson est libre de rang r (r étant le rang du module de Drinfeld) sur $K[T]$ (K étant le corps de base du module de Drinfeld), il suffit donc pour calculer le polynôme caractéristique de l'endomorphisme de module de Drinfeld de calculer la matrice de l'endomorphisme induit sur le motif d'Anderson, puis de calculer son polynôme caractéristique. Nous expliquons comment effectuer la première étape simplement, à l'aide de divisions euclidiennes de Ore. Une partie de notre contribution consiste donc à développer des algorithmes de base pour l'arithmétique des motifs d'Anderson.

La difficulté du chapitre se trouve d'avantage dans la preuve que le polynôme caractéristique d'un endomorphisme se lit sur les motifs d'Anderson. Ce résultat était déjà connu pour $A = \mathbb{F}_q[T]$, mais nous le prouvons pour un anneau A général. Cela nécessite de redéfinir la notion de polynôme caractéristique et de déterminant. Une fois cela fait, nous établissons une dualité (au sens de l'algèbre linéaire) entre l'espace de $\mathfrak{a}$-torsion ($\mathfrak{a}$ étant un idéal de A), et, essentiellement, le quotient du motif d'Anderson par l'action de l'idéal $\mathfrak{a}$. Cette correspondance est essentielle : le polynôme caractéristique est défini sur un module de Tate bien choisi, qui n'est autre qu'une limite projective d'espaces de $\mathfrak{a}^n$-torsion. La correspondance se relève sur le motif d'Anderson tout entier, ce qui donne le résultat voulu.

B.2.5 Chapitre 5

Ce chapitre est la suite directe du précédent : on y présente un algorithme de calcul de normes d'isogénies de modules de Drinfeld. Dans le cas où l'isogénie est un endomorphisme, nous montrons qu'il suffit de calculer le déterminant de l'action de l'isogénie sur les motifs d'Anderson (là où nous calculions le polynôme caractéristique de la matrice pour obtenir le polynôme caractéristique de l'endomorphisme).

Dans le cas où l'isogénie n'est pas un endomorphisme, elle donne un morphisme entre deux motifs d'Anderson distincts. Pour les $\mathbb{F}_q[T]$-modules de Drinfeld, nous montrons que si l'on munit ces deux motifs d'Anderson de leurs bases canoniques respectives (cette notion est précisée dans le chapitre 2), l'isogénie peut être présentée comme une matrice carrée à coefficients dans $\mathbb{F}_q[T]$, et que son déterminant est la norme de l'isogénie. Comme précédemment, lorsque A n'est pas restreint à $\mathbb{F}_q[T]$, et que le motif d'Anderson n'est plus libre de rang fini, mais simplement projectif de rang projectif fini, la notion de déterminant est à repréciser. Nous le faisons, en définissant le déterminant d'un morphisme comme la caractéristique d'Euler-Poincaré du conoyau du morphisme. Les contributions algorithmiques sont, du reste, essentiellement les mêmes que dans le chapitre précédent. Au lieu de considérer des polynômes caractéristiques, sont considérés des déterminants.

B.2.6 Chapitre 6

Pour ce dernier chapitre sur le calcul de polynômes caractéristiques, nous nous concentrons sur le cas particulier de l'endomorphisme de Frobenius, supposant alors que le corps de base est fini. Cette méthode est totalement différente de celle développée dans les deux chapitres précédents, qui était basée sur la correspondance entre les modules de Drinfeld et les motif d'Anderson. Ici, nous considérons au contraire des algèbres centrales simples. Si nous notons K le corps de base, d son degré sur $\mathbb{F}_q$, et $K\{\tau\}$ l'algèbre des polynômes de Ore, alors τ^d, qui définit l'endomorphisme de Frobenius, est aussi un invariant de $K\{\tau\}$, en ce sens que $\mathbb{F}_q\{\tau^d\}$ est le centre de $K\{\tau\}$. Nous pouvons en outre identifier deux sous-algèbres commutatives maximales de $K\{\tau\}$: $\mathbb{F}_q\{\tau\}$ et $K\{\tau^d\}$. Avec ces objets, vient la notion de polynôme caractéristique réduit, et plus généralement, de norme réduite : $K\{\tau\}$ est libre de rang d sur $\mathbb{F}_q\{\tau\}$ comme sur $K\{\tau^d\}$. Des bases canoniques existent, et l'on peut calculer le polynôme caractéristique d'un endomorphisme de $K\{\tau\}$ par rapport à $\mathbb{F}_q\{\tau\}$, ou par rapport à $K\{\tau^d\}$. Il se trouve que le résultat est le même dans les deux cas, ce qui définit le *polynôme caractéristique réduit*. On obtient alors le polynôme caractéristique du Frobenius comme le polynôme caractéristique de l'endomorphisme de multiplication (à droite) par ϕ_T, où ϕ est le module de Drinfeld considéré. Bien sûr, il convient de considérer $\mathbb{F}_q\{\tau^d\}$ comme un anneau de polynômes classique, et un changement de variable est à opérer. Une difficulté importante est encore une fois de démontrer ce résultat en grande généralité, *i.e.* quand l'anneau de fonctions n'est pas restreint à $\mathbb{F}_q[T]$.

B.2.7 Chapitre 7

Le dernier chapitre de contributions traite du calcul d'une action de groupe issue de la théorie du corps de classes des corps de fonctions. Nous avons déjà évoqué nos motivations venant de la cryptographie, et la comparaison de notre algorithme et de sa version « courbes elliptiques ». Nous allons ici évoquer certains aspects théoriques de cette contribution, notamment la preuve que notre objet d'étude — une certaine action de groupe simplement transitive — est un objet bien défini. L'idée est la suivante. Pour un certain module de Drinfeld ϕ ordinaire de rang 2 sur un corps fini K (qui vérifie certaines hypothèses données dans le chapitre), l'on fait l'hypothèse que le polynôme caractéristique de son endomorphisme de Frobenius définit une courbe hyperelliptique imaginaire. On note A son anneau de coordonnées, $\mathbb{F}_q(C)$ son corps de fonctions. On peut alors regarder la catégorie des A-modules de Drinfeld de rang 1 sur K. Un premier résultat est de montrer que celle-ci est équivalente à la catégorie des $\mathbb{F}_q[T]$-modules de Drinfeld de rang 2 sur K. La correspondance est explicite, et permet d'établir un lien entre les $\mathbb{F}_q[T]$-modules de Drinfeld de rang 2 sur K et la catégorie des A-modules de Drinfeld de rang 1 non pas sur K, mais

sur une certaine extension $\mathbb{C}_C$ (dont la définition précise est aussi donnée dans le chapitre) du corps de fonctions $\mathbb{F}_q(C)$. Pour ces modules de Drinfeld sur $\mathbb{C}_C$, l'existence d'une action de groupe simplement transitive comme celle que nous voulons calculer est depuis longtemps établie. Notre approche consiste donc à utiliser ces résultats, et décrire notre action de groupe sur K comme une réduction modulo un idéal premier de l'action de groupe sur $\mathbb{C}_C$.

Cette question théorique traitée, le reste du chapitre consiste à expliquer et prouver comment calculer l'action de groupe avec des coordonnées de Mumford et l'arithmétique des polynômes de Ore. Nous donnons en outre une méthode qui permet non plus de calculer une isogénie (sous forme d'un polynôme de Ore) à partir d'une classe d'idéaux dans le groupe de classes de l'anneau d'endomorphismes, mais de calculer une telle classe à partir d'une isogénie.

B.2.8 Annexe A

Cette annexe liste les tentatives d'utilisations des modules de Drinfeld en cryptographie. Celles-ci peuvent être classifiées en deux parties, selon qu'elles s'inscrivent dans un modèle de sécurité pré ou post-quantique. Pour chacune de ces contributions, nous expliquons en quoi elle est inspirée des courbes elliptiques, nous la décrivons précisément, et nous décrivons les attaques qui la rendent inutilisable de manière robuste en cryptographie.

Bibliography

[ACL22] Simon Abelard, Alain Couvreur, and Grégoire Lecerf. "Efficient computation of Riemann–Roch spaces for plane curves with ordinary singularities." In: *Applicable Algebra in Engineering, Communication and Computing* (2022). DOI: 10.1007/s00200-022-00588-x.

[AM93] A. O. L. Atkin and François Morain. "Elliptic curves and primality proving." In: *Mathematics of Computation* 61.203 (1993), DOI: 10.1090/S0025-5718-1993-1199989-X.

[And86] Greg W. Anderson. "t-Motives." In: *Duke Mathematical Journal* 53.2 (1986), DOI: 10.1215/S0012-7094-86-05328-7.

[Ang94] Bruno Anglès. "Modules de Drinfeld sur les corps finis." PhD thesis. Université Toulouse-III-Paul-Sabatier, 1994. URL: https://theses.fr/1994TOU30238.

[AW21] Josh Alman and Virginia Vassilevska Williams. "A Refined Laser Method and Faster Matrix Multiplication." In: *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*. Proceedings. Society for Industrial and Applied Mathematics, 2021, DOI: 10.1137/1.9781611976465.32.

[Ayo+23] David Ayotte, Xavier Caruso, Antoine Leudière, and Joseph Musleh. "Drinfeld Modules in SageMath." In: *ACM Communications in Computer Algebra* 57.2 (2023), DOI: 10.1145/3614408.3614417.

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

[Bab+20] Liljana Babinkostova, Andrew Gao, Ben Kuehnert, Geneva Schlafly, and Zecheng Yi. *On Isomorphic K-rational Groups of Isogenous Elliptic Curves over Finite Fields*. 2020. DOI: 10.48550/arXiv.2011.08471.

[Bas+24] Andrea Basso, Luca De Feo, Pierrick Dartois, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. *SQIsign2D-West: The Fast, the Small, and the Safer*. 2024. URL: https://eprint.iacr.org/2024/760.

[BC24] Elena Berardini and Xavier Caruso. *Reed-Muller codes in the sum-rank metric*. 2024. DOI: 10.48550/arXiv.2405.09944.

[BCG06] Simon R. Blackburn, Carlos Cid, and Steven Galbraith. "Cryptanalysis of a cryptosystem based on Drinfeld modules." In: *Information Security, IEE Proceedings* 153 (2006), DOI: 10.1049/ip-ifs:20055035.

[Ber+20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. "Faster computation of isogenies of large prime degree." In: *Open Book Series* 4.1 (2020), DOI: 10.2140/obs.2020.4.39.

[BK92] Sunghan Bae and Ja Kyung Koo. "On the singular Drinfeld modules of rank 2." In: *Mathematische Zeitschrift* 210.1 (1992), DOI: 10.1007/BF02571797.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. "CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations." In: *Advances in Cryptology – ASIACRYPT 2019*. Ed. by Steven D. Galbraith and Shiho Moriai. Springer International Publishing, 2019, DOI: 10.1007/978-3-030-34578-5_9.

[Bou+20] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. "Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment." In: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Springer International Publishing, 2020, DOI: 10.1007/978-3-030-56880-1_3.

[Car17] Xavier Caruso. "Polynômes de Ore en une variable." Lecture notes. 2017. URL: https://xavier.caruso.ovh/papers/publis/cours-ore.pdf.

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

[Car35] Leonard Carlitz. "On certain functions connected with polynomials in a Galois field." In: *Duke Mathematical Journal* 1.2 (1935). DOI: 10.1215/S0012-7094-35-00114-4.

[Cas+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action." In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by Thomas Peyrin and Steven Galbraith. Springer International Publishing, 2018, DOI: 10.1007/978-3-030-03332-3_15.

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH." In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Springer Nature Switzerland, 2023, DOI: 10.1007/978-3-031-30589-4_15.

[CG24] Xavier Caruso and Quentin Gazda. *Computation of classical and v-adic L-series of t-motives*. 2024. DOI: 10.48550/arXiv.2401.12618.

[CGS20] Perlas Caranay, Matthew Greenberg, and Renate Scheidler. "Computing modular polynomials and isogenies of rank two Drinfeld modules over finite fields." In: *Contemporary Mathematics* 754 (2020). Ed. by Susanne Brenner, Igor Shparlinski, Chi-Wang Shu, and Daniel Szyld, DOI: 10.1090/conm/754/15148.

[CL09] Jean-Marc Couveignes and Reynald Lercier. "Elliptic periods for finite fields." In: *Finite Fields and Their Applications* 15.1 (2009), DOI: 10.1016/j.ffa.2008.07.004.

[CL13] Jean-Marc Couveignes and Reynald Lercier. "Fast construction of irreducible polynomials over finite fields." In: *Israel Journal of Mathematics* 194.1 (2013), DOI: 10.1007/s11856-012-0070-8.

[CL17a] Xavier Caruso and Jérémy Le Borgne. "A new faster algorithm for factoring skew polynomials over finite fields." In: *Journal of Symbolic Computation* 79 (2017), DOI: 10.1016/j.jsc.2016.02.016.

[CL17b] 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. Association for Computing Machinery, 2017, DOI: 10.1145/3087604.3087617.

[CL23] Xavier Caruso and Antoine Leudière. *Algorithms for computing norms and characteristic polynomials on general Drinfeld modules*. 2023. DOI: 10.48550/arXiv.2307.02879.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. DOI: 10.1007/978-3-319-16721-3.

[CLP24] Mingjie Chen, Antonin Leroux, and Lorenz Panny. "SCALLOP-HD: Group Action from 2-Dimensional Isogenies." In: *Public-Key Cryptography – PKC 2024*. Ed. by Qiang Tang and Vanessa Teague. Springer Nature Switzerland, 2024, DOI: 10.1007/978-3-031-57725-3_7.

[Coh+12] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. 2nd ed. Chapman & Hall/CRC, 2012. ISBN: 978-1-4398-4000-9.

[Cor+22] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. 4th ed. MIT Press, 2022. DOI: 10.5555/1614191.

[Cou06] Jean-Marc Couveignes. *Hard Homogeneous Spaces*. Cryptography seminar of the *École normale supérieure*. 2006. URL: https://eprint.iacr.org/2006/291.

[Cox22] David A. Cox. *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*. 3rd ed. Vol. 387. AMS Chelsea Publishing, 2022. ISBN: 978-1-4704-7183-5.

[CZ81] David G. Cantor and Hans Zassenhaus. "A New Algorithm for Factoring Polynomials Over Finite Fields." In: *Mathematics of Computation* 36.154 (1981), DOI: 10.2307/2007663.

[Dar+24] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. "SQIsignHD: New Dimensions in Cryptography." In: *Advances in Cryptology – EUROCRYPT 2024*. Ed. by Marc Joye and Gregor Leander. Springer Nature Switzerland, 2024, DOI: 10.1007/978-3-031-58716-0_1.

[De +20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies." In: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by Shiho Moriai and Huaxiong Wang. Springer International Publishing, 2020, DOI: 10.1007/978-3-030-64837-4_3.

[DF24] Max Duparc and Tako Boris Fouotsa. *SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies*. 2024. URL: https://eprint.iacr.org/2024/773.

[DH76] Whitfield Diffie and Martin Hellman. "New directions in cryptography." In: *IEEE Transactions on Information Theory* 22.6 (1976), DOI: 10.1109/TIT.1976.1055638.

[DKS18] Luca De Feo, Jean Kieffer, and Benjamin Smith. "Towards Practical Key Exchange from Ordinary Isogeny Graphs." In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by Thomas Peyrin and Steven Galbraith. Lecture Notes in Computer Science. Springer International Publishing, 2018, DOI: 10.1007/978-3-030-03332-3_14.

[DNS21] Javad Doliskani, Anand Kumar Narayanan, and Éric Schost. "Drinfeld modules with complex multiplication, Hasse invariants and factoring polynomials over finite fields." In: *Journal of Symbolic Computation*. MICA 2016 105 (2021), DOI: 10.1016/j.jsc.2020.06.007.

[Dri77] V. G. Drinfel'd. "Commutative subrings of certain noncommutative rings." In: *Functional Analysis and Its Applications* 11.1 (1977), DOI: 10.1007/BF01135527.

[DV06a] Jan Denef and Frederik Vercauteren. "An Extension of Kedlaya's Algorithm to Hyperelliptic Curves in Characteristic 2." In: *Journal of Cryptology* 19.1 (2006), DOI: 10.1007/s00145-004-0231-y.

[DV06b] Jan Denef and Frederik Vercauteren. "An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2." In: *Journal of cryptology* 19.1 (2006),

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. Graduate Texts in Mathematics. Springer, 1995. DOI: 10.1007/978-1-4612-5350-1.

[Eng00] Andreas Enge. "Hyperelliptic Cryptosystems. Efficiency and Subexponential Attacks." PhD thesis. Universität Augsburg, 2000. URL: https://theses.hal.science/tel-00505980.

[Feo+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. "SCALLOP: Scaling the CSI-FiSh." In: *Public-Key Cryptography – PKC 2023*. Ed. by Alexandra Boldyreva and Vladimir Kolesnikov. Springer Nature Switzerland, 2023, DOI: 10.1007/978-3-031-31368-4_13.

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139012843.

[Gek08] Ernst-Ulrich Gekeler. "Frobenius Distributions of Drinfeld Modules over Finite Fields." In: *Transactions of the American Mathematical Society* 360.4 (2008), ISSN: 0002-9947.

[Gek83] Ernst-Ulrich Gekeler. "Zur Arithmetik von Drinfeld-Moduln." In: *Mathematische Annalen* 262.2 (1983), DOI: 10.1007/BF01455309.

[Gek88] Ernst-Ulrich Gekeler. "On the coefficients of Drinfeld modular forms." In: *Inventiones mathematicae* 93.3 (1988), DOI: 10.1007/BF01410204.

[Gek91] Ernst-Ulrich Gekeler. "On finite Drinfeld modules." In: *Journal of Algebra* 141.1 (1991), DOI: 10.1016/0021-8693(91)90211-P.

[GG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. 3rd ed. Cambridge University Press, 2013. DOI: 10.1017/CBO9781139856065.

[Gil+03] Rolland Gillard, Franck Leprévost, Alexei Panchishkin, and Xavier-François Roblot. "Utilisation des modules de Drinfeld en cryptologie." In: *Comptes Rendus Mathematique* 336.11 (2003), DOI: 10.1016/S1631-073X(03)00227-9.

[GJ23] Quentin Gazda and Damien Junger. *Pour une définition commune des courbes elliptiques et modules de Drinfeld*. 2023. DOI: 10.48550/arXiv.2306.13160.

[GJV03] Pascal Giorgi, Claude-Pierre Jeannerod, and Gilles Villard. "On the complexity of polynomial matrix computations." In: *Proceedings of the 2003 international symposium on Symbolic and algebraic computation*. ISSAC '03. Association for Computing Machinery, 2003, DOI: 10.1145/860854.860889.

[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. Association for Computing Machinery, 1986, DOI: 10.1145/12130.12162.

[Gos80] David Goss. "The algebraist's upper half-plane." In: *Bulletin of the American Mathematical Society* (1980).

[Gos96] David Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1996. DOI: 10.1007/978-3-642-61480-4.

[GP20] Sumita Garai and Mihran Papikian. "Endomorphism rings of reductions of Drinfeld modules." In: *Journal of Number Theory* 212 (2020), DOI: 10.1016/j.jnt.2019.02.008.

[GS06] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006. DOI: 10.1017/CBO9780511607219.

[Hay11] David R. Hayes. "A Brief Introduction to Drinfeld Modules." In: *A Brief Introduction to Drinfeld Modules*. De Gruyter, 2011, DOI: 10.1515/9783110886153.1.

[Hei04] Gert-Jan van der Heiden. "Weil Pairing for Drinfeld Modules." In: *Monatshefte für Mathematik* 143.2 (2004), DOI: 10.1007/s00605-004-0261-4.

[Jac96] Nathan Jacobson. *Finite-Dimensional Division Algebras over Fields*. Springer, 1996. DOI: 10.1007/978-3-642-02429-0.

[JD11] David Jao and Luca De Feo. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies." In: *Post-Quantum Cryptography*. Ed. by Bo-Yin Yang. Springer, 2011, DOI: 10.1007/978-3-642-25405-5_2.

[JN19] Antoine Joux and Anand Kumar Narayanan. *Drinfeld modules may not be for isogeny based cryptography*. 2019. URL: https://eprint.iacr.org/2019/1329.

[JSS10] Michael J. Jacobson Jr, Renate Scheidler, and Andreas Stein. "Cryptographic Aspects of Real Hyperelliptic Curves." In: *IACR Cryptology ePrint Archive* 2010 (2010), DOI: 10.2478/v10127-010-0030-9.

[JV06] Claude-Pierre Jeannerod and Gilles Villard. "Asymptotically fast polynomial matrix algorithms for multivariable systems." In: *International Journal of Control* 79.11 (2006), DOI: 10.1080/00207170600726477.

[Kal92] Erich Kaltofen. "On computing determinants of matrices without divisions." In: *Papers from the international symposium on Symbolic and algebraic computation*. ISSAC '92. Association for Computing Machinery, 1992, DOI: 10.1145/143242.143350.

[Kat73] Nicholas M. Katz. "*p*-adic properties of modular schemes and modular forms." In: *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Springer, 1973,

[Ked01] Kiran S. Kedlaya. "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology." In: *Journal of the Ramanujan Mathematical Society* 16 (2001),

[KL24] Yasunori Kinoshita and Baitian Li. *Power Series Composition in Near-Linear Time*. 2024. DOI: 10.48550/arXiv.2404.05177.

[Kob87] Neal Koblitz. "Elliptic curve cryptosystems." In: *Mathematics of Computation* 48.177 (1987), DOI: 10.1090/S0025-5718-1987-0866109-5.

[Kob94] Neal Koblitz. *A Course in Number Theory and Cryptography*. Vol. 114. Graduate Texts in Mathematics. Springer, 1994. DOI: 10.1007/978-1-4419-8592-7.

[Koh96] David Kohel. "Endomorphism rings of elliptic curves over finite fields." PhD thesis. University of California, Berkeley, 1996.

[KU11] Kiran S. Kedlaya and Christopher Umans. "Fast Polynomial Factorization and Modular Composition." In: *SIAM Journal on Computing* 40.6 (2011), DOI: 10.1137/08073408X.

[KV05] Erich Kaltofen and Gilles Villard. "On the complexity of computing determinants." In: *computational complexity* 13.3 (2005), DOI: 10.1007/s00037-004-0185-3.

[Laf01] Laurent Lafforgue. "Chtoucas de Drinfeld et correspondance de Langlands." In: *Inventiones mathematicae* 147 (2001), DOI: 10.1007/s002220100174.

[Lan02] Serge Lang. *Algebra*. Vol. 211. Graduate Texts in Mathematics. Springer, 2002. DOI: 10.1007/978-1-4613-0041-0.

[Lan87] Serge Lang. *Elliptic Functions*. Vol. 112. Graduate Texts in Mathematics. Springer New York, 1987. DOI: 10.5555/1614191.

[Len87] Hendrik W. Lenstra Jr. "Factoring Integers with Elliptic Curves." In: *The Annals of Mathematics* 126.3 (1987), DOI: 10.2307/1971363.

[Li98] Ziming Li. "A subresultant theory for Ore polynomials with applications." In: *Proceedings of the 1998 international symposium on Symbolic and algebraic computation*. ISSAC '98. Association for Computing Machinery, 1998, DOI: 10.1145/281508.281594.

[Lor96] Dino Lorenzini. *An Invitation to Arithmetic Geometry*. American Mathematical Society, 1996. DOI: 10.5555/1614191.

[LS20] Aude Le Gluher and Pierre-Jean Spaenlehauer. "A fast randomized geometric algorithm for computing Riemann-Roch spaces." In: *Mathematics of Computation* 89 (2020), DOI: 10.1090/mcom/3517.

[LS22] Antoine Leudière and Pierre-Jean Spaenlehauer. *Hard Homogeneous Spaces from the Class Field Theory of Imaginary Hyperelliptic Function Fields*. 2022. URL: https://eprint.iacr.org/2022/349.

[LS24] Antoine Leudière and Pierre-Jean Spaenlehauer. "Computing a group action from the class field theory of imaginary hyperelliptic function fields." In: *Journal of Symbolic Computation* 125 (2024), DOI: 10.1016/j.jsc.2024.102311.

[Mai+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. "A Direct Key Recovery Attack on SIDH." In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Springer Nature Switzerland, 2023, DOI: 10.1007/978-3-031-30589-4_16.

[Mil20] John S. Milne. *Class Field Theory*. Lecture notes (version 4.03). 2020. URL: https://www.jmilne.org/math/CourseNotes/CFT.pdf.

[Mil86] Victor S. Miller. "Use of Elliptic Curves in Cryptography." In: *Advances in Cryptology — CRYPTO '85 Proceedings*. Ed. by Hugh C. Williams. Springer, 1986, DOI: 10.1007/3-540-39799-X_31.

[MS19] Yossef Musleh and Éric Schost. "Computing the Characteristic Polynomial of a Finite Rank Two Drinfeld Module." In: *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation* (2019), DOI: 10.1145/3326229.3326256.

[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. Association for Computing Machinery, 2023, DOI: 10.1145/3597066.3597080.

[Mus23] Yossef Musleh. "Algorithms for Drinfeld Modules." PhD thesis. University of Waterloo, 2023. URL: https://uwspace.uwaterloo.ca/handle/10012/20473.

[Nar18] Anand Kumar Narayanan. "Polynomial factorization over finite fields by computing Euler–Poincaré characteristics of Drinfeld modules." In: *Finite Fields and Their Applications* 54 (2018), DOI: 10.1016/j.ffa.2018.08.003.

[NO24] Kohei Nakagawa and Hiroshi Onuki. *SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies*. 2024. URL: https://eprint.iacr.org/2024/771.

[NP21] Vincent Neiger and Clément Pernet. "Deterministic computation of the characteristic polynomial in the time of matrix multiplication." In: *Journal of Complexity* 67 (2021), DOI: 10.1016/j.jco.2021.101572.

[Ore33] Oystein Ore. "Theory of Non-Commutative Polynomials." In: *Annals of Mathematics* 34.3 (1933), DOI: 10.2307/1968173.

[Pan03] Alexei Panchishkin. "Modules de Drinfeld et Cryptologie." Lecture notes. 2003. URL: https://www-fourier.ujf-grenoble.fr/~panchish/03ens.pdf.

[Pap23] Mihran Papikian. *Drinfeld Modules*. Vol. 296. Graduate Texts in Mathematics. Springer International Publishing, 2023. DOI: 10.1007/978-3-031-19707-9.

[Per08] Daniel Perrin. *Algebraic Geometry. An Introduction*. Springer, 2008. DOI: 10.1007/978-1-84800-056-8.

[Poo21] Bjorn Poonen. "Introduction to Drinfeld modules." In: (2021). Expository article. URL: https://math.mit.edu/~poonen/papers/drinfeld.pdf.

[Pot98] Igor Yu. Potemine. "Minimal Terminal $\mathbb{Q}$-Factorial Models of Drinfeld Coarse Moduli Schemes." In: *Mathematical Physics, Analysis and Geometry* 1.2 (1998), DOI: 10.1023/A:1009724323513.

[PS07] Clément Pernet and Arne Storjohann. "Faster algorithms for the characteristic polynomial." In: *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*. ISSAC '07. Association for Computing Machinery, 2007, DOI: 10.1145/1277548.1277590.

[PW23] Aurel Page and Benjamin Wesolowski. *The supersingular Endomorphism Ring and One Endomorphism problems are equivalent*. 2023. URL: https://eprint.iacr.org/2023/1399.

[Rei88] Miles Reid. *Undergraduate Algebraic Geometry*. London Mathematical Society Student Texts. Cambridge University Press, 1988. DOI: 10.1017/CBO9781139163699.

[Rob23] Damien Robert. "Breaking SIDH in Polynomial Time." In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Springer Nature Switzerland, 2023, DOI: 10.1007/978-3-031-30589-4_17.

[Ros02] Michael Rosen. *Number Theory in Function Fields*. Vol. 210. Graduate Texts in Mathematics. Springer, 2002. DOI: 10.1007/978-1-4757-6046-0.

[RS06] Alexander Rostovtsev and Anton Stolbunov. *Public-key cryptosystem based on isogenies*. 2006. URL: https://eprint.iacr.org/2006/145.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems." In: *Communications of the ACM* 21.2 (1978), DOI: 10.1145/359340.359342.

[Sca01] Thomas Scanlon. "Public Key Cryptosystems Based on Drinfeld Modules Are Insecure." In: *Journal of Cryptology* 14.4 (2001), DOI: 10.1007/s00145-001-0004-9.

[Séc20] Vincent Séchère. "Courbes algébriques." Lecture notes. 2020. URL: https://lmv.math.cnrs.fr/wp-content/uploads/2020/09/Cours-CA-2015.pdf.

[Sho94] Peter W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring." In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994, DOI: 10.1109/SFCS.1994.365700.

[Sil00] John R. Silvester. "Determinants of block matrices." In: *The Mathematical Gazette* 84.501 (2000), DOI: 10.2307/3620776.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Vol. 106. Graduate Texts in Mathematics. Springer, 2009. DOI: 10.1007/978-0-387-09494-6.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer, 1994.

[Vél71] Jacques Vélu. "Isogénies entre courbes elliptiques." In: *Comptes Rendus de l'Académie des Sciences de Paris*. A et B, Sciences mathématiques et Sciences physiques 273 (1971), URL: https://gallica.bnf.fr/ark:/12148/bpt6k56191248/f52.item.

[Vil06] Gabriel Daniel Villa Salvador. *Topics in the Theory of Algebraic Function Fields*. Mathematics: Theory & Applications. Birkhäuser, 2006. DOI: 10.1007/0-8176-4515-2.

[Wes22] Benjamin Wesolowski. *Computing isogenies between finite Drinfeld modules*. 2022. URL: https://eprint.iacr.org/2022/438.

[Wil+24] Virginia Vassilevska Williams, Yinzhan Xu, Zixuan Xu, and Renfei Zhou. "New Bounds for Matrix Multiplication: from Alpha to Omega." In: *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. Proceedings. Society for Industrial and Applied Mathematics, 2024, DOI: 10.1137/1.9781611977912.134.