Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Master Thesis

Computing the Endomorphism ring of a Drinfeld module in generic characteristic

Submitted for the degree of

Master of Science ETH

in Mathematics

Nikolas Kuhn

April 12, 2016

Advisor: Prof. Dr. Richard Pink

Contents

1 Introduction

1.1 Overview

Let K be a finitely generated field over $\mathbb{F}_q$, let A be an admissible coefficient ring and let $\varphi : A \to K[\tau]$ be a Drinfeld module of rank r over K in generic characteristic. In this thesis we describe algorithms for computing the endomorphism ring of φ both over K and over an algebraic closure.

Method

Let F denote the quotient field of A. Since we are in generic characteristic, the endomorphism ring $\mathrm{End}_K(\varphi)$ is a commutative integral domain. Let $\mathrm{End}_K^0(\varphi)$ denote its quotient field. The idea on which our approach is based is to find a suitable subring $R \subseteq K$ such that $\varphi(A) \subseteq R[\tau]$ and a maximal ideal λ of R with residue field k, such that the induced composition $A \to R[\tau] \to k[\tau]$ defines a Drinfeld A-module φ_λ over k. Under good conditions this gives a natural embedding $j : \mathrm{End}_K(\varphi) \to \mathrm{End}_k(\varphi_\lambda)$ of A-algebras. The endomorphism ring of a Drinfeld module over a finite field can be explicitly computed, so we may expect to get a better handle on $\mathrm{End}_K(\varphi)$ in this way. Moreover, it suggests breaking up the original problem into several pieces:

A: Compute the endomorphism ring $\mathrm{End}_k(\varphi_\lambda)$ over the finite field.

B: Determine the image of $\mathrm{End}_K(\varphi)$ under j.

C: Compute the inverse of j on $j(\mathrm{End}_K(\varphi))$.

While this captures the general idea, problem B turns out to be too hard to address directly. However, we can improve on this initial approach in several ways:

First, under good circumstances we can choose the reduction φ_λ such that $\mathrm{End}_k(\varphi)$ is commutative. Then $\mathrm{End}_k^0 := \mathrm{End}_k(\varphi) \otimes_A F$ is a field, which makes the situation simpler. Second, since φ has generic characteristic the map $D : K[\tau] \to K$ sending $f \in K[\tau]$ to its constant coefficient restricts to an injective ring homomorphism $\mathrm{End}_K(\varphi) \to K$. It turns out that we can explicitly compute inverse images of this homomorphism. This allows us to split problem C further. For the actual algorithm we break down the problem of finding $\mathrm{End}_K(\varphi)$ about as follows:

A': Compute the field extension $\mathrm{End}_k^0(\varphi_\lambda)/F$.

B1': Determine the subfield L generated by $j(\mathrm{End}_K(\varphi))$ in $\mathrm{End}_k^0(\varphi_\lambda)$.

B2': Determine an A-subalgebra S of L which is contained in $j(\mathrm{End}_K(\varphi_\lambda))$ and whose quotient field is L.

C1': Compute the possible embeddings of S into K.

C2': Lift S from K to a subalgebra of $\mathrm{End}_K(\varphi)$.

D': Recover $\mathrm{End}_K(\varphi)$ from S.

In this form B1' is still not solvable. However, since $\mathrm{End}_k^0(\varphi_\lambda)/F$ has only finitely many subfields, we can simply compute them all and do the remaining steps for each of them. It also turns out that to solve problem B2', we actually need to consider two reductions of φ with different characteristic ideal.

In order to proceed in this way, it is necessary to find reductions whose endomorphism ring is commutative. This is always possible if $\mathrm{End}_K(\varphi)$ is separable over A. The general case can be reduced to the separable one.

It is not evident from this short desription, but the algorithm to compute $\mathrm{End}_K(\varphi)$ that we will present, can with only some minor changes be used to compute the endomorphism ring over an algebraic closure $\overline{K}$. To understand roughly why this works, remember that there is a finite separable extension K' of K, such that all endomorphisms of φ over $\overline{K}$ are already defined over K'. It turns out that the reductions we choose to compute $\mathrm{End}_K(\varphi)$ in the original algorithm work as well for any finite extension of K and as a consequence of this, that we can solve problems A', B1' and B2' over K', without having any further information about it. The remaining problems can then directly be addressed over $\overline{K}$ instead of K.

General outline

In Section 2 we collect some of the standard theory of Drinfeld modules as well as several other results. This section serves mainly as a reference for the rest of the thesis.

The main part of the thesis are Sections 3 and 4, in which we work out the theoretical results on which the algorithm is based. The main technical obstacle was problem B2', which is addressed in 4.8. Since at first only Drinfeld modules over finite extensions of F were considered in this thesis, this is sometimes unnecessarily assumed.

The actual algorithm – albeit only for K a finite extensions of F – is presented in Section 5, where we also deal with the inseparable case and give a variation of the algorithm which computes the endomorphism ring over the algebraic closure.

In Section 6 we discuss how one obtains an algorithm when K is an arbitrary finitely generated field over $\mathbb{F}_q$.

Note on computational issues

We address several points that are silently assumed throughout the rest of the thesis.

We assume one can do arithmetic over the admissible coefficient ring A. By that we mean also being able to for example solve questions of ideal membership, computing

quotients of finitely generated A-modules and enumerating the elements of A. When implementing the algorithm, it might be desirable to pass to a subring of A of the form $\mathbb{F}_q[t]$, which does not change the endomorphism ring. Over the principal ideal domain $\mathbb{F}_q[t]$ many computations that are hard over a general A can be reduced to an explicit application of the theorem about elementary divisors.

We assume that one can compute the irreducible factors of a multivariate polynomial over a global function field. Further we assume that one can enumerate the places of a global function field K, and that for any given place v one can evaluate the associated normalized valuation on K and compute the degree and the residue field of v.

In the general version of the algorithm in Section 6 one further needs to be able to compute the integral closure of a finitely generated integral $\mathbb{F}_q$-algebra in a finite extension of its quotient field. Also, for a finitely generated integrally closed integral $\mathbb{F}_q$-algebra R one needs to be able to list its maximal ideals – and for a given maximal ideal to compute the residue field and determine ideal membership.

1.2 Terminology and Conventions

We use the following conventions for notation:

- We fix once and for all a finite field $\mathbb{F}_q$ and let throughout p denote the characteristic of $\mathbb{F}_q$.
- For any ring R containing $\mathbb{F}_q$, we let $R[\tau]$ denote the, in general non-commutative, ring of $\mathbb{F}_q$-linear polynomials over R with $\tau = X^q$. It is the subset $R[X]$ of polynomials of the form
$$\sum_{i=0}^{n} x_i X^{qi},$$
where $n \geq 0$ and $x_i \in R$ for $i = 0, \ldots, n$, with usual addition and whose multiplication law is composition. We refer to the book of Goss ([Gos96], Chapter 1) for its general theory when R is a field.
- We let $D : R[\tau] \to R$ denote the ring homomorphism which sends an $\mathbb{F}_q$-linear polynomial to its coefficient in τ-degree zero, or equivalently to its linear X-coefficient.
- For an $\mathbb{F}_q$-linear polynomial $f \in K[\tau]$, where K is a field, $\mathrm{ord}_\tau(f)$ denotes the highest power of τ dividing f from the right.
- For a field K containing $\mathbb{F}_q$, an additive polynomial $f \in K[\tau]$ and an overfield L of K, we denote by $\mathrm{Ker}_L\, f$ the set of zeros of f in L. Id est $\mathrm{Ker}_L\, f$ is the kernel of f, viewed as an endomorphism of the additive group of L.
- Unless specified otherwise A will always denote an admissible coefficient ring containing $\mathbb{F}_q$. The quotient field of A will be denoted by F. The distinguished place of F will be denoted by ∞.

- For any place v of a global function field K, denote by $\mathcal{O}_v$ the valuation ring associated to v, by $\mathfrak{m}_v$ its maximal ideal and by k_v the residue field at v. We let d_v stand for the degree of the field extension $k_v/\mathbb{F}_q$.
- By an "isogeny" we will always mean an "isogeny between Drinfeld modules with the same characteristic homomorphism".
- For a Drinfeld A-module $\varphi : A \to K[\tau]$, define $\mathrm{End}_K^0(\varphi) := \mathrm{End}_K(\varphi) \otimes_A F$.

2 Preliminaries

In the subsections titled with review we summarize mostly without proofs the relevant definitions and results from the theory of Drinfeld modules. This is standard material and can be found in [Dri74], [Gos96], [DH] or [Fli13]. The presentation given here is heavily influenced by the lecture notes of Professor Pink. We then collect some standard results from other fields, which are used later on.

2.1 Review of admissible coefficient rings

Definition 2.1.1. An integral domain A is an *admissible coefficient ring*, if the following conditions are met:

(a) The quotient field F of A is a global function field.

(b) There is a place ∞ of F, such that A is the subring of F consisting of all elements which are regular at every place except ∞.

Proposition 2.1.2. *For any admissible coefficient ring A, the following are true:*

(a) A is finitely generated.

(b) Any quotient of A by a nonzero ideal is finite.

(c) A is a Dedekind domain whose ideal class group is finite.

On an admissible coefficient ring we define a degree function, which coincides with the degree of a polynomial in the case $A = \mathbb{F}_q[t]$. The definition depends on our initial choice of base $\mathbb{F}_q$. We will discuss it in more detail in 3.2.

Definition 2.1.3. The degree of a nonzero element $a \in A$ is the number

$$\deg_A a = \dim_{\mathbb{F}_q}(A/Aa).$$

We also set $\deg_A 0 = -\infty$.

Let A' be a subring of A which is itself an admissible coefficient ring. Let F' be the quotient field of A' and ∞' the distinguished place of F'. As an extension of global function fields, F/F' is finite.

Proposition 2.1.4. *We have the following properties.*

(a) The only place of F that lies over ∞' is ∞.

(b) A is the integral closure of A' in F.

(c) A is a finitely generated A'-module and $\mathrm{rank}_{A'} A = [F/F']$.

Proof. First we show (a). Since any valuation on F' extends to some valuation on F, it follows that for any $a \in A'$, being a constant in F' is equivalent to being a constant in F. Now let w be any extension of $v_{\infty'}$ to F. Then for any non-constant $a \in A'$, we have $w(a) = v_{\infty'}(a) < 0$, so w must belong to ∞.

Now we turn to (b). Let B denote the integral closure of A in F'. By [AM69], Corollary 5.22, B is equal to the intersection of all valuation rings of F containing A'. In other words an element $x \in F$ belongs to B if and only if for any valuation v on F that takes only non-negative values on A' we have $v(x) \geq 0$. Statement (a) implies that the valuations on F that take negative values on A' are exactly those that belong to $\tilde{\infty}$. Taking this into account, we have

$$B = \{x \in F | v(x) \geq 0 \text{ for any valuation } v \text{ on } F \text{ not belonging to } \infty\} \stackrel{\text{def}}{=} A.$$

Finally, since A is finitely generated and integral over A', it is a finitely generated module over A'. The equality in c) follows from the fact that we have a natural isomorphism $A \otimes_{A'} F' \cong F$, since every element of F can be written in the form a/a' for $a \in A$ and $a' \in A'$. □

2.2 Review of Drinfeld modules

Definition; rank and height

Definition 2.2.1. A Drinfeld A-module over a field K is a ring-homomorphism

$$\begin{aligned} \varphi : A &\to K[\tau] \\ a &\mapsto \varphi_a, \end{aligned}$$

whose image is not contained in the subring $K \subseteq K[\tau]$.

To a Drinfeld module $\varphi : A \to K[\tau]$ one associates the *characteristic homomorphism* of φ, which is just the composition $D\varphi : A \to K$ of φ with the lowest-coefficient map. Its kernel $\mathfrak{p}_0$ is called the *characteristic ideal* of φ. It is either the zero ideal of A, in which case φ is said to have *generic characteristic* or a maximal ideal, in which case one says that φ has *special characteristic*.

Prop./Def. 2.2.2. There exists a positive integer r, called the *rank* of φ, such that for all nonzero $a \in A$, we have

$$\deg_\tau \varphi_a = r \deg_A a.$$

Prop./Def. 2.2.3. Suppose that φ has special characteristic, and let $\mathfrak{p}_0$ be the characteristic ideal. Let $d_{\mathfrak{p}_0}$ denote the degree over $\mathbb{F}_q$ of the residue field at $\mathfrak{p}_0$. There exists a positive integer h, called the *height* of φ, such that for all nonzero $a \in A$, we have

$$\operatorname{ord}_\tau \varphi_a = h d_{\mathfrak{p}_0} \operatorname{ord}_{\mathfrak{p}_0}(a).$$

Homomorphisms

Now let φ, φ' be two Drinfeld A-modules over K and let L be a field containing K. Then $K[\tau]$ is naturally a subring of $L[\tau]$.

Definition 2.2.4. A *homomorphism of Drinfeld A-modules* $f : \varphi \to \varphi'$ over L is an element $f \in L[\tau]$ satisfying $f\varphi_a = \varphi'_a f$ for all $a \in A$. The set of all homomorphisms from φ to φ' over L is denoted by $\operatorname{Hom}_L(\varphi, \varphi')$.

The set of homomorphisms of A naturally forms an A-module.

Definition 2.2.5. A nonzero homomorphism between Drinfeld A-modules with the same characteristic homomorphism is called an *isogeny* and the Drinfeld modules are called *isogenous*.

Proposition 2.2.6. *Any isogeny between Drinfeld modules in generic characteristic is separable.*

Proposition 2.2.7. *If φ and φ' are isogenous, they have the same rank. If we are in special characteristic, they also have the same height.*

Proposition 2.2.8. *Let $f : \varphi \to \varphi'$ be an isogeny of Drinfeld A-modules over K. Then there exists an isogeny $g : \varphi' \to \varphi$ over K and a nonzero element $a \in A$, such that $gf = \varphi_a$ and $fg = \varphi'_a$.*

The endomorphism ring

Definition 2.2.9. The *endomorphism ring of φ over L* is

$$\operatorname{End}_L(\varphi) := Z_{L[\tau]}(\varphi(A)) = \operatorname{Hom}_L(\varphi, \varphi),$$

the centralizer of $\varphi(A)$ in $L[\tau]$. Its elements are called *endomorphisms of φ over L*.

Except for statement (a), the following theorem is usually proven for $\operatorname{Hom}_K(\varphi, \varphi')$, but we will not use the more general version.

Theorem 2.2.10. *The endomorphism ring* $\mathrm{End}_K(\varphi)$ *is a finitely generated torsion-free* A*-module of rank at most* r^2*. Further*

(a) $\mathrm{End}_K(\varphi) \otimes_A F$ *is a division ring.*

(b) There exists a finite separable extension K' *of* K *such that for any overfield* L *of* K *we have*

$$\mathrm{End}_{K'}(\varphi) = \mathrm{End}_L(\varphi).$$

Theorem 2.2.11. *If* φ *has generic characteristic, then* $\mathrm{End}_K(\varphi)$ *is a commutative* A*-algebra of rank dividing* r*.*

Torsion points

Let $\varphi : A \to K[\tau]$ be a Drinfeld A-module of rank r over K. Let L be an overfield of K. Besides the A module-structure induced by the characteristic homomorphism $A \to K$, there is another A-module structure on L given by $A \times L \to L, (a, x) \mapsto \varphi_a(x)$. For any $a \in A$, the a-torsion of L with respect to this module structure is exactly $\mathrm{Ker}_L \varphi_a$.

Definition 2.2.12. For any ideal $\mathfrak{a} \subset A$, we define

$$\varphi[\mathfrak{a}](L) := \{x \in L | \forall a \in \mathfrak{a} : \varphi_a(x) = 0\} = \bigcap_{a \in \mathfrak{a}} \mathrm{Ker}_L \varphi_a,$$

the set of $\mathfrak{a}$*-torsion points of* φ *in* L*.*

For any $\mathfrak{a} \subseteq A$, the set $\varphi[\mathfrak{a}](L)$ is naturally an A-submodule of L via φ.

We can even make L into an $\mathrm{End}_L(\varphi)$-module by $(g, x) \mapsto g(x)$ for $g \in \mathrm{End}_L(\varphi)$ and $x \in L$. One easily sees that then for any ideal $\mathfrak{a} \subseteq A$, the torsion points $\varphi[\mathfrak{a}](L)$ are an $\mathrm{End}_L(\varphi)$-submodule of L. Conversely, for any endomorphism g over L, the set $\mathrm{Ker}_L(g)$ is an A-submodule of L.

Now let $\overline{K}$ be an algebraic closure of K. Let $\mathfrak{p} \subseteq A$ be a maximal ideal. We denote the completion of A and F at $\mathfrak{p}$ by $A_\mathfrak{p}$ and $F_\mathfrak{p}$ respectively. Let $\mathfrak{p}_0$ denote the characteristic ideal of φ. For the following discussion we fix $\mathfrak{p}$.

Definition 2.2.13. The full $\mathfrak{p}$-power torsion module of φ is

$$\varphi[\mathfrak{p}^\infty](\overline{K}) := \bigcup_{n \geq 0} \varphi[\mathfrak{p}^n](\overline{K}).$$

If $\mathfrak{p} \neq \mathfrak{p}_0$ set $\tilde{r} := r$. If $\mathfrak{p} = \mathfrak{p}_0$, then φ has special characteristic and we set $\tilde{r} := r - h$, where h is the height of φ.

Proposition 2.2.14. *There exists an isomorphism of A-modules*

$$\varphi[\mathfrak{p}^\infty](\overline{K}) \cong (F_\mathfrak{p}/A_\mathfrak{p})^{\oplus \tilde{r}}.$$

Proposition 2.2.15. *(a) Let $\mathfrak{p}$ be a maximal ideal of A and $n \geq 0$. Then there exists an isomorphism of A-modules*

$$\varphi[\mathfrak{p}^n](\overline{K}) \cong (A/\mathfrak{p}^n)^{\oplus \tilde{r}}.$$

(b) For any $b \in A$ with $k := \mathrm{ord}_\mathfrak{p}(b) \leq n$, the A-module homomorphism

$$\begin{aligned} \varphi_b : \varphi[\mathfrak{p}^n](\overline{K}) &\to \varphi[\mathfrak{p}^{n-k}](\overline{K}) \\ x &\mapsto \varphi_b(x) \end{aligned}$$

is surjective.

(c) Let $\mathfrak{b}$ be a nonzero ideal of A with prime factorization $\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$. Then we have an equality of A-submodules of $\overline{K}$:

$$\varphi[\mathfrak{b}](\overline{K}) = \bigoplus_{i=1}^{k} \varphi[\mathfrak{p}_i^{r_i}](\overline{K}).$$

Tate Modules

Let the notation introduced in 2.2 remain in place.

Definition 2.2.16. (a) The $\mathfrak{p}$-*adic Tate-module of* φ is the $A_\mathfrak{p}$-module

$$T_\mathfrak{p}(\varphi) := \mathrm{Hom}_A(F_\mathfrak{p}/A_\mathfrak{p}, \varphi[\mathfrak{p}^\infty](\overline{K})).$$

(b) The *rational* $\mathfrak{p}$-*adic Tate module of* φ is the $F_\mathfrak{p}$-vector space

$$V_\mathfrak{p}(\varphi) := T_\mathfrak{p}(\varphi) \otimes_{A_\mathfrak{p}} F_\mathfrak{p}.$$

The action of $\mathrm{End}_K(\varphi)$ on torsion points induces an action on $T_\mathfrak{p}(\varphi)$

Proposition 2.2.17. *The $A_\mathfrak{p}$-module $T_\mathfrak{p}(\varphi)$ is free of rank $\tilde{r}$ and $V_\mathfrak{p}(\varphi)$ is an $\tilde{r}$-dimensional $F_\mathfrak{p}$-vector space.*

2.3 Finitely generated modules over Dedekind rings

Definition 2.3.1. Let B be an integral domain and M a B-module. Let $Q(B)$ denote the quotient field of B. We define the *rank* of M over B as

$$\operatorname{rank}_B M = \dim_{Q(B)} M \otimes_B Q(B)$$

Now let B be a Dedekind ring.

Theorem 2.3.2 (cf. [BJ89], Theorem 3.5.6)**.** *(a) Let M be a finitely generated B-module and let M_{tor} denote its torsion submodule. Then M has finite rank over B and M/M_{tor} is a projective B-module. We have* $\operatorname{rank}_B M = 0$ *if and only if $M = M_{tor}$. Otherwise M is isomorphic to a module of the form*

$$B^r \oplus \mathfrak{b} \oplus M_{tor},$$

with $\operatorname{rank}_B M = r+1$ *and $\mathfrak{b}$ is a nonzero ideal of B whose ideal class depends only on the isomorphism class of M.*

(b) Every finitely generated torsion B-module is isomorphic to a module of the form

$$B/\mathfrak{p}_1^{r_1} \oplus \cdots \oplus B/\mathfrak{p}_k^{r_k}.$$

Up to ordering, the prime powers appearing in this representation depend only on the isomorphism class of M.

We will also use the following basic fact, which is a consequence of the Chinese remainder theorem.

Proposition 2.3.3. *Let $\mathfrak{b}$ and $\mathfrak{c}$ be nonzero ideals of B. Suppose $\mathfrak{c} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ is the factorization of $\mathfrak{c}$ as a product of prime ideals, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are distinct. Then we have isomorphisms of B-modules*

$$\mathfrak{b}/\mathfrak{c}\mathfrak{b} \cong B/\mathfrak{c} \cong B/\mathfrak{p}_1^{r_1} \oplus \cdots \oplus B/\mathfrak{p}_k^{r_k}$$

Proof. With the chinese remainder theorem, choose an element $\pi \in B$ for which the following holds: Any maximal ideal $\mathfrak{p}$ of B which appears as a prime factor of $\mathfrak{b}\mathfrak{c}$ divides (π) with the same multiplicity as it divides $\mathfrak{b}$. Then $\pi \in \mathfrak{b}$ and $B/\mathfrak{c} \to \mathfrak{b}/\mathfrak{b}\mathfrak{c}, x+\mathfrak{c} \mapsto x+\mathfrak{b}\mathfrak{c}$ is an isomorphism. □

2.4 Degree of imperfection one

Let K be a field of positive characteristic p. By general field theory, K^p is a subfield of K and the degree of K/K^p is either infinite or a power of p.

Definition 2.4.1. If $[K/K^p] = p^d$ is finite, d is called the *degree of imperfection* of K.

The following properties are left as an exercise for the reader:

- A field is perfect iff its degree of imperfection is zero.
- The degree of imperfection is invariant under finite extensions.
- The degree of imperfection of a rational function field $K(t)$ is one more than the degree of imperfection of the base field K.
- A function field over a perfect field has degree of imperfection one.

In particular any global function field has degree of imperfection one.

Proposition 2.4.2. *If L/K is a finite field extension and K has degree of imperfection one, then there exists a unique intermediate field $K \subseteq K' \subseteq L$, such that L/K' is separable and K'/K is purely inseparable. Moreover $K = K'^{p^e}$, where p^e is the inseparable degree of the extension L/K.*

Proof. By induction, it is enough to show that if L/K is inseparable, there exists $K_1 \subseteq L$ such that $K_1^p = K$.

Since L/K is inseparable, there exists $\alpha \in L \backslash K$, such that $\alpha^p \in K$. So $K(\alpha)/K$ has degree p. Since $K(\alpha)$ is finite over K it has degree of inseparability one. Since we have $(K(\alpha))^p \subseteq K \subseteq K(\alpha)$, it follows that

$$p = [K(\alpha)/\left(K(\alpha)\right)^p] = [K(\alpha)/K][K/\left(K(\alpha)\right)^p] = p[K/\left(K(\alpha)\right)^p].$$

So $K = (K(\alpha))^p$. □

2.5 Splitting Formula

Let L/K be a finite extension of fields and v a discrete valuation on K. There is a positive finite number of ways to extend v to a valuation on L. Let $w_1, \ldots w_g$ be all the distinct extensions of v to L, where $g \geq 1$. For $i = 1, \ldots, g$ let $e_{w_i/v}$ denote the ramification index and $f_{w_i/v}$ the inertia degree of w_i over v. It is well known that if L/K is separable we have the formula

$$[L/K] = \sum_{i=1}^{g} e_{w_i/v} f_{w_i/v}. \tag{2.5.1}$$

This is discussed for example in [Neu90], Ch. II, §8.
We will be dealing with not necessarily separable extensions of global function fields. This case is covered in M. Rosen's book [Ros02], Theorem 7.6 (he formulates it using the prime ideals of valuation rings instead of valuations on K).

Theorem 2.5.2. *Equation* (2.5.1) *holds, given that K is an algebraic function field in one variable over a perfect field k and that v vanishes on k.*

2.6 Riemann-Roch

The following version of the Riemann-Roch Theorem is Remark 7.3.33 in the book "Algebraic Geometry and Arithmetic Curves" by Q. Liu ([Liu02]), with the difference that we will assume smoothness instead of the weaker requirement to be a local complete intersection.

Let C be a smooth projective curve over a field k, which is not assumed to be the field of constants of C. Let p_a be the arithmetic genus (Def. 7.3.19 in [Liu02]) of C and $\mathcal{K}_C$ a canonical divisor on C (Def. 7.3.32 in [Liu02]).

Theorem 2.6.1. *For any divisor D on C, we have*

$$\dim_k H^0(C, \mathcal{O}_C(D)) - \dim_k H^0(C, \mathcal{O}_C(\mathcal{K}_C - D)) = \deg D + 1 - p_a.$$

If C is connected and $\deg D > 2p_a - 2$, then

$$\dim_k H^0(C, \mathcal{O}_C(D)) = \deg D + 1 - p_a.$$

We will also use the following related result:

Proposition 2.6.2 (cf. [Liu02], Proposition 7.3.25, a)**.** *For any two divisors $D' \leq D$ on C, we have*

$$\dim_k H^0(C, \mathcal{O}_C(D')) \leq \dim_k H^0(C, \mathcal{O}_C(D)) \leq \dim_k H^0(C, \mathcal{O}_C(D')) + \deg D - D'$$

3 Preliminary results from algebra

3.1 Intermediate fields of a finite extension

Let K be a field and $f \in K[X]$ a monic polynomial of degree $n \geq 1$ with coefficients in K that is separable, i.e. has no multiple zeros in an algebraic closure of K. Let N be a splitting field of f over K and let $\gamma_1, \ldots, \gamma_n \in N$ be the zeros of f.

We consider the natural left action of S_n on $N[X, Y_1, \ldots, Y_n]$ by permutation of the Y_i, i.e. for $\sigma \in S_n$, let $(\sigma g)(X, Y_1, \ldots, Y_n) = g(X, Y_{\sigma 1}, \ldots Y_{\sigma n})$. For every $\sigma \in S_n$, we define:

$$l_\sigma := \sum_{i=1}^{n} \gamma_i Y_{\sigma i} \in N[X, Y_1, \ldots, Y_n],$$

and further for every subgroup $\tilde{G}$ of S_n

$$Q_{\tilde{G}} := \prod_{\tau \in \tilde{G}} (X - l_\tau).$$

We will also write Q for Q_{S_n}. For any $\tau, \sigma \in S_n$ we have $\tau l_\sigma = l_{\tau\sigma}$ and Q is fixed under the action of S_n. Each coefficient of Q is a symmetric polynomial expression in the γ_i with integer coefficients. By the fundamental theorem of symmetric polynomials, it can be expressed as an integer polynomial in the coefficients of f. For fixed degree n, the polynomial associated to each coefficient is independent of both f and the base field K and can be computed in advance.

We identify the Galois group $\mathrm{Gal}(N/F)$ with a subgroup G of S_n by its action on the zeros $\gamma_1, \ldots, \gamma_n$ of f, so that $\tau(\gamma_i) = \gamma_{\tau i}$ for any $\tau \in G$ and $1 \leq i \leq n$. Letting G act on coefficients, we obtain another group action on $N[X, Y_1, \ldots, Y_n]$, which we denote by $(\tau, g) \mapsto {}^\tau g$ for $\tau \in G$, and $g \in N[X, Y_1, \ldots, Y_n]$. It is straightforward to check that for any $\sigma \in S_n$ and $\tau \in G$, we have ${}^\tau(l_\sigma) = l_{\sigma\tau^{-1}}$.

For any $\sigma \in G$, we can calculate

$${}^\sigma(Q_G) = \prod_{\tau \in G} (X - {}^\sigma(l_\tau)) = \prod_{\tau \in G} (X - l_{\tau\sigma^{-1}}) = \prod_{\tau \in G\sigma^{-1}} (X - l_\tau) = Q_G.$$

This shows that Q_G must have coefficients in F. Let L be an intermediate field of N/K and let H be the associated subgroup of G under the Galois correspondence. Then the same calculation with G replaced by H shows that the polynomial Q_H has coefficients in L. This observation can be extended to the following

Theorem 3.1.1. *(a) The decomposition of Q into irreducible factors over L is given by*

$$Q = \prod_{\sigma \in S_n/H} \sigma Q_H,$$

where the product is understood over a set of representatives for the left cosets of H in S_n.

(b) We have $\mathrm{Stab}_{S_n}(\sigma Q_H) = \sigma H \sigma^{-1}$ for any $\sigma \in S_n$, where the stabilizer is with respect to the action of S_n by permutation of the variables Y_i.

(c) The field L is generated over K by the coefficients of Q_H.

Proof. The set $\{X - l_\sigma\}_{\sigma \in S_n}$ consists of $n!$ distinct, pairwise not associated irreducible polynomials. Working over N, for $\sigma \in S_n$, we have

$$\sigma Q_H = \prod_{\tau \in H} (X - l_{\sigma\tau}) = \prod_{\tau \in \sigma H} (X - l_\tau).$$

This product depends only on the coset σH, in particular Q_H is fixed by elements of H. Conversely, for $\sigma \notin H$ one sees that $X - l_\sigma$ is an irreducible factor of σQ_H but not of Q_H, so Q_H is fixed only by elements of H. Hence H is the stabilizer of Q_H. By basic group theory we have $\mathrm{Stab}_{S_n}(\sigma Q_H) = \sigma \,\mathrm{Stab}_{S_n}(Q_H)\sigma^{-1} = \sigma H \sigma^{-1}$, which is (b).

The equality in (a) holds since both sides are equal to the product over all the $X - l_\sigma$ for $\sigma \in S_n$. In order to show that the factors on the right hand side are irreducible over L, it is enough to consider Q_H. Suppose P is not constant and divides Q_H in $L[X, Y_1, \ldots, Y_n]$. We can assume P is monic in X. Calculating over N, the polynomial Q_H splits into the factors $(X - l_\sigma)_{\sigma \in H}$, so there must be at least one $\sigma_0 \in H$, such that $X - l_{\sigma_0}$ divides P. The action of H as the Galois group of N/L leaves P invariant, since it has coefficients in L. We find that for all $\sigma \in H$:

$$X - l_\sigma = {}^{\sigma\sigma_0}(X - l_{\sigma_0}) \quad \text{divides} \quad {}^{\sigma\sigma_0}P = P.$$

Therefore P has the same irreducible factors as H and since both are monic in X, they must be equal. This shows that H is irreducible, which implies (a).

Now we turn to statement (c). We already know that Q_H has coefficients in L. Let L' be the subfield of L generated over K by the coefficients of Q_H, and let H' denote the corresponding Galois-subgroup of G. We have $H \subseteq H'$ by Galois-correspondence. From their definitions this implies that Q_H divides $Q_{H'}$ in $N[X, Y_1, \ldots, Y_n]$. This remains true over $L'[X, Y_1, \ldots, Y_n]$, since both polynomials have coefficients in L'. By part (a), $Q_{H'}$ is irreducible over L'. This shows $Q_H = Q_{H'}$. We deduce $H = H'$ and $L = L'$.

□

Algorithm 3.1.2 (Intermediate fields of a simple separable extension)**.** Given a field K and a separable irreducible poynomial f over K of degree n, the algorithm computes the intermediate fields of the extension L/K, where $L := K[X]/(f)$.

1. Determine the auxiliary polynomial $Q(X, Y_1, \ldots, Y_n) \in K[X, Y_1, \ldots, Y_n]$ using symmetric polynomials.
2. Compute an irreducible factor Q_K of Q over K.
3. Determine the subgroup G of S_n, which leaves Q_K invariant. By the results of this subsection, G is the Galois group of f over K up to conjugation in S_n.
4. Compute an irreducible factor Q_L of Q_K over L and determine its stabilizer H in S_n. We have $H \subseteq G$.
5. Compute the groups H' with $H \subseteq H' \subseteq G$. By Galois theory, those groups correspond bijectively to the intermediate fields of L/K.

6. For each H' with corresponding field L', compute the product

$$Q_{L'} = \prod_{\sigma \in H'/H} \sigma Q_H.$$

The coefficients of $Q_{L'}$ generate L' over K.

Remark 3.1.3. If K has degree of imperfection one, the algorithm can be extended to arbitrary simple finite extensions, given that one can determine p-th roots: If f is irreducible, but not separable, take $g \in K[X]$, such that $g(X^{p^e}) = f(X)$ for some $e > 0$. The field $K[X]/(g)$ embeds naturally in L with image the maximal separable extension L_s of K in L. Then run the algorithm with g instead of f to obtain the intermediate fields of L_s/K. For every intermediate field L' of L_s/K one obtains exactly e intermediate fields of L/K, namely $L', L'^{1/p}, \ldots, L'^{1/p^e}$.

3.2 Degree in admissible coefficient rings

We collect some results concerning the degree on the admissible coefficient ring A, which was introduced in Definition 2.1.3.

Let v_∞ denote the normalized valuation of F at ∞. It is related to the degree as follows.

Proposition 3.2.1. *For any $a \in A$ we have*

$$\deg_A a = -[k_\infty/\mathbb{F}_q] v_\infty(a) = d_\infty v_\infty(a). \tag{3.2.2}$$

Corollary 3.2.3. *For any $a, b \in A$ we have*

- $\deg_A ab = \deg_A a + \deg_A b$,
- $\deg_A(a+b) \leq \max(\deg_A a, \deg_A b)$.

To see why this is true we first consider how the degree behaves in an extension of admissible coefficient rings. Let A' be an admissible coefficient subring of A that also contains $\mathbb{F}_q$.

Let $a \in A'$. If $a \neq 0$, then by the structure theorem for finitely generated modules over Dedekind rings together with Proposition 2.3.3 it follows that for some nonzero ideal $\mathfrak{b}' \subseteq A'$, we have

$$A/aA \cong (A'/aA')^{r-1} \oplus \mathfrak{b}'/a\mathfrak{b}' \cong (A'/aA')^r,$$

where $r = \operatorname{rank}_{A'} A$. This shows that

$$\deg_A a = \operatorname{rank}_{A'} A \cdot \deg_{A'} a. \tag{3.2.4}$$

The following proof is essentially the same as in the lecture notes of Professor Pink.

Proof of Proposition 3.2.1. For constant a both sides are zero, unless $a = 0$, in which case both sides equal $-\infty$. Let $a \in A$ be any nonconstant element. Then $\mathbb{F}_q[a]$ is a subring of A and a polynomial ring over $\mathbb{F}_q$, hence itself an admissible coefficient ring. We can therefore apply equation (3.2.4) with $A' = \mathbb{F}_q[a]$, which yields $\deg_A a = [F/\mathbb{F}_q(a)]$. Let ∞' denote the place at infinity of $\mathbb{F}_q(a)$ and $v_{\infty'}$ the associated normalized valuation on $\mathbb{F}_q(a)$. Note that the residue field at ∞' is just $\mathbb{F}_q$ and that $v_{\infty'}(a) = -1$. Then ∞ lies over ∞' with inertial degree $f_{\infty/\infty'} = [k_\infty/\mathbb{F}_q]$ and ramification index $e_{\infty/\infty'} = v_\infty(a)/v_{\infty'}(a) = -v_\infty(a)$. By the splitting formula Theorem 2.5.2, we have $[F/\mathbb{F}_q(a)] = f_{\infty/\infty'}e_{\infty/\infty'}$. The proposition follows by putting these equalities together. □

Let again A', F' and ∞' be as in Proposition 2.1.4 above. Let $v_{\infty'}$ be the normalized valuation at ∞'. Let $e_{\infty/\infty'}$ denote the ramification index and $f_{\infty/\infty'}$ the inertia degree of ∞ over ∞'. For arbitrary $x \in F$, consider its minimal polynomial m_x over F'. Since ∞ is the only place of F lying over ∞', the Newton polygon of m_x with respect to $v_{\infty'}$ has a unique slope equal to $v_{\infty'}(x)$ (for reference, see [Neu90], Chapter 2, §6). This is also true for the characteristic polynomial χ_x as it is a power of the minimal polynomial. Taking this consideration further we have

Proposition 3.2.5. *For any $a \in A$, let*

$$\chi_a = X^n + b_1 X^{n-1} + \cdots + b_n$$

be the characteristic polynomial of a for the extension F/F'. Then for $k = 1, \ldots, n$ we have $b_k \in A'$ and

(a) $\deg_{A'} b_k \leq \frac{k}{n} \deg_A x$ *for* $k = 1, \ldots, n-1$

(b) $\deg_{A'} b_n = \deg_A a$.

Proof. By Proposition 2.1.4, (b) the element a is integral over A'. Since A' is integrally closed and we are dealing with integral domains, it follows that the minimal polynomial m_a of a over F' has coefficients in A' (cf. [AM69], Proposition 5.15). Consequently, χ_a also has coefficients in A'. By the preceding discussion, the Newton polygon of χ_a has the unique slope $v_{\infty'}(a)$. By definition of the Newton polygon, this means for $k = 1, \ldots, d$ that $v_{\infty'}(b_k) \geq k v_{\infty'}(a)$, with equality for $k = n$. Now we have

$$\deg_{A'} b_k = -d_{\infty'} v_{\infty'}(b_k) \leq -d_{\infty'} k v_{\infty'}(a) \overset{(*)}{=} \frac{k}{n} \deg_A a,$$

with equality if $k = n$. To obtain (*), rewrite

$$\deg_A a = -d_\infty v_\infty(a) = -(d_{\infty'} f_{\infty/\infty'})(e_{\infty/\infty'} v_{\infty'}(a)) = -d_{\infty'} n v_{\infty'}(a).$$

□

3.3 Subspaces of bounded degree

For a non-negative integer d, let $A_{\leq d}$ denote the $\mathbb{F}_q$-subspace of A consisting of elements of A-degree at most d. We will see that it is finite-dimensional and give a way to compute a basis.

Since F is a function field in one variable over the perfect field $\mathbb{F}_q$, it arises as the field of rational functions of a connected smooth projective curve C over $\mathbb{F}_q$ (cf. [Liu02], Proposition 7.3.13 together with Corollary 4.3.33). We identify the places of F with the closed points of C. Then A is naturally identified with the coordinate ring of $C\backslash\{\infty\}$. The notion of degree defined in 3.2 is related to the degree of a divisor on C: For nonzero $a \in A$, let $(a)_+$ denote the part outside ∞ of the principal divisor defined by a . Then

$$\deg_A a = \sum_{\mathfrak{p}\in \mathrm{Max}(A)} [k_\mathfrak{p}/\mathbb{F}_q] \operatorname{ord}_\mathfrak{p} a = \deg(a)_+. \tag{3.3.1}$$

Here, $\mathrm{Max}(A)$ is the set of maximal ideals of A and for $p \in \mathrm{Max}(A)$, its residue field is denoted by $k_\mathfrak{p}$.
The advantage of this viewpoint is that we can use the theorem of Riemann-Roch (Theorem 2.6.1). Let p_a be the arithmetic genus of C over $\mathbb{F}_q$ as in the given version of the theorem. We use the arithmetic instead of the geometric genus because it allows us to formulate the intended result relative to $\mathbb{F}_q$ in a uniform way. One could also use the geometric genus and work over the constant field of C instead.

Proposition 3.3.2. *The degree function* $\deg_A : A^\times \to \mathbb{Z}_{\geq 0}$ *takes values in* $d_\infty\mathbb{Z}_{\geq 0}$. *Also*

(a) the dimension of $A_{\leq nd_\infty}$ *over* $\mathbb{F}_q$ *increases by at most* d_∞ *when* n *increases by one,*

(b) $1 \leq \dim_{\mathbb{F}_q} A_{\leq 0} \leq d_\infty$,

(c) for $n > 2(p_a - 1)/d_\infty$,

$$\dim_{\mathbb{F}_q} A_{\leq nd_\infty} = nd_\infty + 1 - p_a.$$

Proof. The first statement follows from formula (3.2.2). Next we show that

$$A_{\leq nd_\infty} = H^0(C, \mathcal{O}_C(n\infty)).$$

Notice that $H^0(C, \mathcal{O}_C(n\infty))$ is the subset of F consisting of functions with a pole of order at most n at ∞ and no other poles. This is the geometric way of saying it is the subset of all $a \in A$ for which $v_\infty(a) \geq -n$. By formula (3.2.2), this is just the set $A_{\leq nd_\infty}$.

Now let $n > 2(p_a - 1)/d_\infty$. Then the degree nd_∞ of the divisor $n\infty$ exceeds $2(p_a - 1)$. So the Riemann-Roch theorem gives the desired equality in (c).

One obtains (b) from the fact that $A_{\leq 0}$ is just the field of constants of C, which contains $\mathbb{F}_q$ and is naturally a subfield of k_∞. Finally (a) follows from Proposition 2.6.2. □

Remark 3.3.3. In the case of a polynomial ring $A = \mathbb{F}_q[t]$, we have $p_a = 0$ and Proposition 3.3.2 states simply that the polynomials of degree at most n over $\mathbb{F}_q$ form an $\mathbb{F}_q$-vector space of dimension $n + 1$.

Definition 3.3.4. For $n \geq 0$ we define a *graded representation of* $A_{\leq nd_\infty}$ to be a sequence of lists $\mathcal{L}_0, \ldots, \mathcal{L}_n$, such that the following hold for $0 \leq k \leq n$.

(a) Each $\mathcal{L}_k$ is a list of distinct and linearly independent elements of A of degree kd_∞. This includes the possibility that $\mathcal{L}_k$ is empty.

(b) Let V_k denote the $\mathbb{F}_q$-subspace of A spanned by the elements of $\mathcal{L}_k$. Then $A_{\leq kd_\infty} = A_{\leq (k-1)d_\infty} \oplus V_k$.

In particular the collection of all elements in $\mathcal{L}_0, \mathcal{L}_1, \ldots, \mathcal{L}_k$ forms a basis of $A_{\leq k \deg \infty}$ for any $0 \leq k \leq n$.

By Proposition 3.3.2, each $\mathcal{L}_k$ in a graded representation of A contains $\leq d_\infty$ elements, with equality for k big enough.

Lemma 3.3.5. *Let V_k be an $\mathbb{F}_q$-subspace of A with $A_{\leq kd_\infty} = A_{\leq (k-1)d_\infty} \oplus V_k$. Suppose V_k has dimension d_∞. Then for any $a \in A$, which has degree ld_∞, we have $A_{\leq (k+l)d_\infty} = A_{\leq (k+l-1)d_\infty} \oplus aV_k$.*

Proof. Since $V_k \cap A_{\leq (k-1)d_\infty} = \{0\}$, all nonzero elements of V_k have degree kd_∞. It follows that all nonzero elements of aV_k have degree $(k + l)d_\infty$ by Corollary 3.2.3, and so $aV_k \cap A_{\leq (k+l-1)d_\infty} = \{0\}$. By the dimension formula, we have that

$$\dim_{\mathbb{F}_q} \left(aV_k \oplus A_{\leq (k+l-1)d_\infty} \right) = \dim_{\mathbb{F}_q} aV_k + \dim_{\mathbb{F}_q} A_{\leq (k+l-1)d_\infty} = d_\infty + \dim_{\mathbb{F}_q} A_{\leq (k+l-1)d_\infty}$$

and by Proposition 3.3.2, that

$$d_\infty + \dim_{\mathbb{F}_q} A_{\leq (k+l-1)d_\infty} \geq \dim_{\mathbb{F}_q} A_{\leq (k+l)d_\infty}.$$

This shows that aV_k and $A_{\leq (k+l-1)d_\infty}$ together span $A_{\leq (k+l)d_\infty}$, and hence they are complements. □

Algorithm 3.3.6 (Determine a graded representation of A)**.** The algorithm takes a non-negative integer n and returns lists $\mathcal{L}_0, \mathcal{L}_1, \ldots, \mathcal{L}_n$, which give a graded representation for $A_{\leq nd_\infty}$.

1. Compute $\deg \infty$.
2. Pick a non-constant element $t \in A$ and compute $r := \deg_A t$, which equals the degree of $F/\mathbb{F}_q(t)$ by (3.2.4).
3. Set $k := 0$

4. If there exists $1 \leq i \leq k-1$, such that the list $\mathcal{L}_i$ is not empty and $\mathcal{L}_{k-i}$ has exactly d_∞ entries, let $a \in \mathcal{L}_i$ and compute $\mathcal{L}_k$ by multiplying every entry in $\mathcal{L}_{k-i}$ by a, which gives a list with the desired properties due to Lemma 3.3.5. In this case proceed with step 7. If no such i exists continue with step 5.

5. For each of the finitely many polynomials χ of the form $\chi = X^r + b_1 X^{r-1} + \ldots + b_{r-1}X + b_r$, such that for $j = 1, \ldots, r$ we have $b_j \in \mathbb{F}_q[t]$ and $\deg_t b_j \leq \frac{j}{r} k d_\infty$ with equality for $j = r$, compute the roots of χ in F. Since A is integrally closed, this gives a collection $\mathcal{S}_k$ of elements of A. By Proposition 3.2.5 this is exactly the set of elements of A of degree kd_∞.

6. Using the lists $\mathcal{L}_0, \ldots, \mathcal{L}_{k-1}$ and the elements $\mathcal{S}_k$, determine the list $\mathcal{L}_k$ such that (a) and (b) of Definition 3.3.4 are fulfilled.

7. If $k < n$, increase k by one and go to step 3. If $k = n$, return $\mathcal{L}_0, \mathcal{L}_1, \ldots, \mathcal{L}_n$.

3.4 Integral closure in global function fields

We want to be able to compute the integral closure of an admissible coefficient ring in a finite extension of its quotient field. We present a simple algorithm which works in a slightly more general setting.

Let B be a finitely generated and integrally closed integral domain whose quotient field is a global function field K containing $\mathbb{F}_q$. Any such ring is in fact a Dedekind domain and has the property that any quotient by a nonzero ideal is finite. Let further L be a finite extension of K.

Let $\mathrm{Tr}_{L/K} : L \to K$ denote the relative trace of the extension. For $x \in L$ the value $\mathrm{Tr}_{L/K}(x)$ is by definition equal to the trace of the endomorphism of the K-vector space L given by multiplication by x. For a K-basis $\alpha_1, \ldots, \alpha_n$ of L, the discriminant of $d(\alpha_1, \ldots, \alpha_n)$ is defined as the determinant of the Matrix $(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))_{i,j}$. If γ is a primitive element of L over K, then $d(1, \gamma, \gamma^2, \ldots, \gamma^{n-1})$ is equal to the discriminant of the minimal polynomial of γ over K (see [Neu90], before Prop. 2.8). We will make use of some basic results:

Proposition 3.4.1 (cf. Neukirch [Neu90], Prop. 2.8)**.**

If L/K is separable, the symmetric bilinear form

$$\begin{aligned} L \times L &\to K \\ (x, y) &\mapsto \mathrm{Tr}_{L/K}(xy) \end{aligned}$$

is nondegenerate and for any K-basis $\alpha_1, \ldots, \alpha_n$ of L we have

$$d(\alpha_1, \ldots, \alpha_n) \neq 0.$$

Lemma 3.4.2 (cf.[Neu90], Lemma 2.9)**.** *Let C denote the integral closure of B in L. Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L, all elements of which lie in C. Then $d := d(\alpha_1, \ldots, \alpha_n)$ is contained in B and we have $dC \subseteq B\alpha_1 + \cdots + B\alpha_n$.*

As a direct consequence of combining those, we have

Proposition 3.4.3. *Let $\gamma \in L$ be a primitive element for L/K and let f denote the minimal polynomial of γ. Let d denote the discriminant of f. Then d is a nonzero element of B and*

$$B[\gamma] \subseteq C \subseteq \frac{1}{d}B[\gamma].$$

This suggests the following

Algorithm 3.4.4 (Integral closure in a separable extension of global function field.)**.** Given a function field K in one variable over $\mathbb{F}_q$, a finitely generated integrally closed subring B of K whose quotient field is K and a separable irreducible monic polynomial f over K of degree n, the algorithm returns the integral closure C of B in the extension $L := K[X]/(f)$ of K. We suppose that B is given by a finite subset of K which generates B as an $\mathbb{F}_q$-algebra. The algorithm returns C by giving a finite subset of L which generates C as a B-algebra.

1. In the subsequent steps we will assume that f has coefficients in B. If this is not already true, modify f as follows: Suppose $f = X^n + y_1X^{n-1} + \cdots + y_{n-1}X + y_n$, where $y_i \in K$. For each i where y_i is nonzero determine $b_i \in B$ such that $y_ib_i \in B$. Let $b \in B$ be the product of all such b_i. Replace f by the polynomial

$$X^n + (by_1)X^{n-1} + \cdots + (b^{n-1}y_{n-1})X + b^ny_n.$$

2. Compute the discriminant d of the polynomial f.

3. Let γ denote the image of X in L. Compute the basis $1, \gamma, \ldots, \gamma^{n-1}$ of the free B-module $B[\gamma]$. Divide each element in the basis by d to obtain a basis for $\frac{1}{d}B[\gamma]$.

4. With $M := \frac{1}{d}B[\gamma]$, we have by Proposition 3.4.3

$$dM \subseteq C \subseteq M.$$

   For each of the $|B/dB|^n$ cosets of dM in M choose a representative y and compute the characteristic polynomial χ_y of y for the extension L/K. Test whether $y \in C$, by testing if all coefficients of χ_y lie in B, which is equivalent by [AM69], Proposition 5.15.

   Let $\mathcal{S} \subseteq M$ be the set of those elements y where the test was positive.

5. As B-modules, C is the sum of $B[\gamma]$ and the module generated by $\mathcal{S}$. It follows that C is generated as an algebra over B by $\mathcal{S} \cup \{\gamma\}$.

Remark 3.4.5. In order to compute the integral closure of B in an extension L/K which has degree of inseparability p^e, one applies the algorithm to the separable part of the extension to obtain a B-algebra C^{sep}. Then one draws p^e-th roots of every element in a generating set of C^{sep} as a B-algebra and of the given generators of B as an $\mathbb{F}_q$-algebra. Together those elements then generate the algebraic closure of B in L as a B-algebra.

3.5 Results from noncommutative algebra

We recall some definitions and results concerning central simple algebras without further discussion. For a more detailed presentation of the relevant material see the book of Goss ([Gos96], § 4.11). Throughout let L be a field.

Definition 3.5.1. Let R be a finite-dimensional nonzero L-algebra.

- We say R is *simple*, if R has no two-sided ideals except $\{0\}$ and R.
- We say R is *central over* L, if L is equal to the center of R.

Proposition 3.5.2 (cf. [Gos96], Proposition 4.11.10)**.** *Let R be a central simple algebra over L and L' a field containing L. Then $R \otimes_L L'$ is central simple over L'.*

For any nonzero, not necessarily commutative ring with unit R, let $Z(R)$ denote the center of R, which is a subring. For a subset $B \subset R$, let $Z_R(B)$ denote the centralizer of B in R, which is a subring containing $Z(R)$. We then have

Theorem 3.5.3 (cf. [Gos96], Theorem 4.11.14)**.** *For a central simple L-algebra R and a simple subalgebra $S \subseteq R$ we have:*

(a) $Z_R(S)$ *is simple,*

(b) $\dim_L(R) = \dim_L(S) \dim_L(Z_R(S))$*,*

(c) $Z_R(Z_R(S)) = S$*.*

Proposition 3.5.4 (cf. [Gos96], Corollary 4.11.15)**.** *Let R be central simple over L. Then* $\dim_L(R)$ *is a square.*

We will also need the following fact:

Proposition 3.5.5 (cf. [GS06], Example 2.1.4)**.** *Let R be a central simple L-algebra with* $\dim_L(R) = b^2$*. Let M be a finitely generated left R-module. Then* $\dim_L(M)$ *is a multiple of b.*

4 Preliminary results about Drinfeld modules

4.1 Isogenies

Let φ, φ' be two Drinfeld A-modules over a field K, and $f \in K[\tau]$ an isogeny from φ to φ'. Then f induces an isomorphism of F-algebras

$$\mathrm{End}_K(\varphi) \otimes_A F \cong \mathrm{End}_K(\varphi') \otimes_A F, \tag{4.1.1}$$

which is uniquely characterized by $e \otimes 1 \mapsto e' \otimes 1$, whenever $f \circ e = e' \circ f$. We will use the following result from [PD12][Prop. 4.3]:

Theorem 4.1.2. *Let $\varphi : A \to K[\tau]$ be a Drinfeld A-module, let S be any A-subalgebra of $\mathrm{End}_K(\varphi)$ and let S' be a maximal A-order in $S \otimes_A F$ which contains S. Then there exist a Drinfeld A-module $\varphi' : A \to K[\tau]$ and an isogeny $f : \varphi \to \varphi'$ over K such that S' corresponds to $\mathrm{End}_K(\varphi') \cap (S \otimes_A F)$ via the isomorphism (4.1.1).*

The proof given in [PD12] shows that a possible choice of f can be obtained as follows: Take any $a \in A$ for which $aS' \subset S$ and let f be the unique element of $K[\tau]$ for which

$$\mathrm{Ker}\, f = \sum_{s \in aS'/aS} \varphi_s(\mathrm{Ker}\, \varphi_a),$$

which is to be understood as an equality of subgroup schemes of the additive group scheme $\mathbb{G}_{a,K}$ over K (From the formulation in [PD12], it is not obvious that f should preserve the characteristic homomorphism of φ, but this follows from the characterization in [Gos96], Proposition 4.7.11.). Note that the sum can be taken over any choice of representatives for the finitely many classes in aS'/aS.

To obtain an algorithm that finds f, we use the fact that any finite set $h_1, \ldots, h_k$ of nonzero elements in $K[\tau]$ has a unique monic least common left multiple $\mathrm{lclm}(h_1, \ldots, h_k)$ in $K[\tau]$, which can be effectively determined. It can be checked that for $g, h \in K[\tau]$ the group scheme $g(\mathrm{Ker}\, h)$ is given by the kernel of the unique $l \in K[\tau]$ for which $lg = \mathrm{lclm}(g, h)$, and that for finitely many $h_1, \ldots, h_k \in K[\tau]$, we have an equality

$$\mathrm{Ker}\, h_1 + \cdots + \mathrm{Ker}\, h_k = \mathrm{Ker}\, (\mathrm{lclm}(h_1, \ldots, h_k))$$

of subgroupschemes of $\mathbb{G}_{a,K}$. This gives us the following algorithm:

Algorithm 4.1.3 (Determining an isogenous module)**.** Given a Drinfeld module $\varphi : A \to K[\tau]$ together with an A-subalgebra S of $\mathrm{End}_K(\varphi)$ and a maximal order S' of $S \otimes_A F$ which contains S, this algorithm determines a Drinfeld A-module φ' over K and an isogeny $f : \varphi \to \varphi'$ over K such that the endomorphism ring of φ' over K is all of S' in the sense of Theorem 4.1.2.

1. Determine $a \in A$, such that $aS' \subset S$.

2. Choose a finite set $E \subseteq aS'$ of representatives for aS'/aS.
3. For every $s \in E$, compute $g_s := \mathrm{lclm}(\varphi_s, \varphi_a)$ and divide g_s by φ_s from the right to obtain l_s.
4. Compute $f := \mathrm{lclm}(\{\varphi_s\}_{s\in E})$.
5. To obtain φ', compute φ'_b by dividing $f\varphi_b$ from the right by f, where b runs through a set of generators of A over $\mathbb{F}_q$.

4.2 Finer structure of the endomorphism ring

The following general result will be useful for studying the endomorphism ring more closely.

Proposition 4.2.1 (cf. [Yu95], Theorem 1)**.** *Let φ be a Drinfeld A-module over a field K. Let E be any subfield of $\mathrm{End}_K^0(\varphi)$ which contains F. Then there is only one place of E lying over ∞ and the integral closure of A in E is an admissible coefficient ring.*

Remark 4.2.2. We usually combine this with Theorem 4.1.2: By possibly passing to an isogenous module, we can assume that $A' := \mathrm{End}_K(\varphi) \cap E$ is the integral closure of A in E. Then Proposition 4.2.1 tells us that the natural embedding of A' in $K[\tau]$ defines a Drinfeld module with coefficient ring A', which can be studied in its own right.

Let K be a field and let $\varphi : A \to K[\tau]$ be a Drinfeld module in special characteristic of rank r and height h. Let $L = Z(\mathrm{End}_K^0(\varphi))$. Since $\mathrm{End}_K^0(\varphi)$ is a division ring, L is a field. It contains the image of F under the natural embedding into $\mathrm{End}_K^0(\varphi)$, hence $\dim_L \mathrm{End}_K^0(\varphi) \leq \dim_F \mathrm{End}_K^0(\varphi) \leq r^2$ is finite. As a division ring, $\mathrm{End}_K^0(\varphi)$ is simple and therefore a central simple L-algebra. Let a denote the degree of the field extension L/F and b^2 the dimension of $\mathrm{End}_K^0(\varphi)$ as an L-algebra, which is a square by Proposition 3.5.4. Then $\mathrm{End}_K^0(\varphi)$ is an F-vector space of dimension ab^2.

Proposition 4.2.3. *In the above notation we have*

(a) $ab \mid r$,

(b) $b \mid h$.

In particular if $h = 1$ then $\mathrm{End}_K^0(\varphi)$ is commutative.

Proof. The numbers a, b, r and h remain unchanged when we modify the Drinfeld module by an isogeny over K. According to Theorem 4.1.2 we can thus assume that $A' := L \cap \mathrm{End}_K(\varphi)$ is integrally closed. It follows from Proposition 4.2.1 that A' is an admissible coefficient ring and that φ extends naturally to a Drinfeld A'-module φ' over K. Since A' is contained in the center of the endomorphism ring, we have $\mathrm{End}_K(\varphi) = \mathrm{End}_K(\varphi')$.

Lemma 4.2.4. *Let r' denote the rank and h' the height of φ'. Then $r' = r/a$ and h' divides h.*

Proof of the Lemma. For any $x \in A$ we have the formula $\deg_{A'}(x) = \deg_A(x) \operatorname{rank}_A(A')$ and $\operatorname{rank}_A(A') = \dim_F L = a$. It follows that φ' has rank $r' := r/a$.

Now let $\mathfrak{q}_0$ be the characteristic ideal of φ' and $\mathfrak{p}_0$ that of φ. Then clearly $\mathfrak{q}_0$ lies over $\mathfrak{p}_0$. Let $f(\mathfrak{q}_0 \mid \mathfrak{p}_0)$ denote the inertial degree and $e(\mathfrak{q}_0 \mid \mathfrak{p}_0)$ the ramification index of $\mathfrak{q}_0$ over $\mathfrak{p}_0$. By the basic properties of the height, we have for any $x \in A$:

$$h' \dim_{\mathbb{F}_q}(A'/\mathfrak{q}_0) \operatorname{ord}_{\mathfrak{q}_0}(x) = \operatorname{ord}_\tau(\varphi'_x) = \operatorname{ord}_\tau(\varphi_x) = h \dim_{\mathbb{F}_q}(A/\mathfrak{p}_0) \operatorname{ord}_{\mathfrak{p}_0}(x). \tag{4.2.5}$$

By the definition of the inertial degree

$$\dim_{\mathbb{F}_q}(A'/\mathfrak{q}_0) = f(\mathfrak{q}_0 \mid \mathfrak{p}_0) \dim_{\mathbb{F}_q}(A/\mathfrak{p}_0)$$

and by the definition of the ramification index

$$\operatorname{ord}_{\mathfrak{q}_0}(x) = e(\mathfrak{q}_0 \mid \mathfrak{p}_0) \operatorname{ord}_{\mathfrak{p}_0}(x).$$

Now insert those in (4.2.5), evaluate it for any nonzero $x \in \mathfrak{p}_0$ and cancel on both sides to find

$$h' f(\mathfrak{q}_0 \mid \mathfrak{p}_0) e(\mathfrak{q}_0 \mid \mathfrak{p}_0) = h.$$

□

With Lemma 4.2.4, in order to prove the proposition it is enough to show that b divides both the rank and the height of φ'. In other words, it is enough to show Proposition 4.2.3 in the case where $a = 1$, i.e. where $\operatorname{End}^0_K(\varphi)$ is central simple over F of dimension b^2, which we will now assume.

Let $\mathfrak{p}$ be any maximal ideal of A. By Proposition 3.5.2, $\operatorname{End}^0_K(\varphi) \otimes_F F_\mathfrak{p}$ is central simple of dimension b^2 over the completion $F_\mathfrak{p}$. On the other hand, since $\operatorname{End}_K(\varphi)$ acts on the Tate-modules of φ, the rational $\mathfrak{p}$-adic Tate-module $V_\mathfrak{p}(\varphi)$ has a natural structure as an $\operatorname{End}^0_K(\varphi) \otimes_F F_\mathfrak{p}$-module, compatible with its $F_\mathfrak{p}$-vector space structure. Now by Proposition 3.5.5, b divides the $F_\mathfrak{p}$-dimension of $V_\mathfrak{p}(\varphi)$, which by Proposition 2.2.17 is equal to r if $\mathfrak{p} \neq \mathfrak{p}_0$, and equal to $r - h$ if $\mathfrak{p} = \mathfrak{p}_0$. Choosing any $\mathfrak{p} \neq \mathfrak{p}_0$ we find $b \mid r$, thus proving (a) of Proposition 4.2.3. Taking $\mathfrak{p} = \mathfrak{p}_0$ yields $b \mid r - h$, and it follows that $b \mid h$. □

4.3 Endomorphisms with given constant coefficient

Let K be a finite extension of F and let $\varphi : A \to K[\tau]$ be a rank r Drinfeld module over K. We consider the restriction of the constant-coefficient map $D : K[\tau] \to K$ to $\operatorname{End}_K(\varphi)$. Any endomorphism of a Drinfeld module in generic characteristic is separable, so $\operatorname{Ker} D \cap \operatorname{End}_K(\varphi) = 0$ and it follows that D is injective on $\operatorname{End}_K(\varphi)$. The image $D(\operatorname{End}_K(\varphi))$ is contained in the integral closure of A in K, since $\operatorname{End}_K(\varphi)$ is a finite and hence integral, A-algebra.

Conversely, given an element $\varepsilon \in K$ which is integral over A, we want to be able to tell if ε lies in $D(\mathrm{End}_K(\varphi))$ and if so, to determine its preimage under D. First the following result, which states that the isomorphism (4.1.1) respects the embedding of the endomorphism rings into K.

Lemma 4.3.1. *The subfield of K generated by $D(\mathrm{End}_K(\varphi))$ remains unchanged when φ is altered by an isogeny f defined over K.*

Proof. Suppose $f : \varphi \to \varphi'$ is an isogeny of Drinfeld A-modules over K. Let E and E' denote the subfields of K generated by the images under D of $\mathrm{End}_K(\varphi)$ and $\mathrm{End}_K(\varphi')$ respectively. Let $e \in K[\tau]$ be a dual isogeny such that $ef = \varphi_a$ for some nonzero $a \in A$. Then if $g \in \mathrm{End}_K(\varphi)$ has least coefficient $x \in K$, the polynomial egf is an endomorphism of φ' and has least coefficient ax, hence $x \in E'$. It follows that $E \subset E'$. By reversing the roles of φ and φ' in the argument we obtain the reverse inclusion. □

The following lemma gives a necessary condition for an endomorphism to have a prescribed constant coefficient.

Lemma 4.3.2. *Let $g \in \mathrm{End}_K(\varphi)$ and ε the lowest coefficient of g. Let d_ε denote the degree and $a_\varepsilon \in A$ the constant coefficient of the minimal polynomial of ε over F. Then we have*

$$\deg_\tau(g) = r\frac{\deg_A a_\varepsilon}{d_\varepsilon}.$$

Proof. By Theorem 4.1.2, there is a Drinfeld A-module φ' which is isogenous to φ over K by an isogeny f, and whose endomorphism ring is integrally closed. Let E denote the field of fractions of the image of $\mathrm{End}_K(\varphi)$ in K. By Lemma 4.3.1, it follows that the image of $\mathrm{End}_K(\varphi')$ in K is the integral closure of A in E and in particular contains the image of $\mathrm{End}_K(\varphi)$. Let $g' \in \mathrm{End}_K(\varphi')$ be the element mapping to ε. Then $g'f$ and fg are both isogenies from φ to φ' and have the same constant coefficient. Since isogenies in generic characteristic are separable it follows that $g'f = fg$. In particular, g and g' must have the same degree.

By this argument, it is enough to prove the Lemma when $\mathrm{End}_K(\varphi)$ is integrally closed. By Proposition 4.2.1, $\mathrm{End}_K(\varphi)$ is then itself an admissible coefficient ring and the natural inclusion $\mathrm{End}_K(\varphi) \to K[\tau]$ defines a Drinfeld module $\tilde{\varphi}$ of rank $\tilde{r}$ with $r = \tilde{r}[E/F]$. We identify $\mathrm{End}_K(\varphi)$ via D with its image $\tilde{A}$ in K. With Proposition 3.2.5, we obtain

$$\deg_\tau(g) = \tilde{r}\deg_{\tilde{A}}(\varepsilon) = \tilde{r}\deg_A(a_\varepsilon)\frac{[E/F]}{d_\varepsilon} = r\frac{\deg_A a_\varepsilon}{d_\varepsilon}.$$

□

Let $\overline{K}$ be an algebraic closure of K. Given a non-negative integer s and an element $\varepsilon \in \overline{K}$, it is straightforward to determine if φ possesses an endomorphism g over $\overline{K}$ of degree at most s and constant coefficient ε: Make the Ansatz $g = \varepsilon + y_1\tau + \cdots + y_s\tau^s$ for $y_1, \ldots, y_s \in \overline{K}$. Now take any non-constant $a \in A$ with $\varphi_a = \sum_i a_i\tau^i \in K[\tau]$, where $a_0 = a$ and $a_i = 0$ for $i < 0$ or $i > r \deg_A a$. Comparing coefficients in the relation $g\varphi_a = \varphi_a g$, we obtain equations

$$y_k = \frac{a_k(\varepsilon - \varepsilon^{q^k}) + \sum_{i=1}^{k-1}(a_{k-i}^{q^i} y_i - a_{k-i} y_i^{q^{k-i}})}{a - a^{q^k}} \tag{4.3.3}$$

for $k = 1, \ldots, s$ and

$$a_k(\varepsilon - \varepsilon^{q^k}) + \sum_{i=1}^{s}(a_{k-i}^{q^i} y_i - a_{k-i} y_i^{q^{k-i}}) = 0 \tag{4.3.4}$$

for $k = s+1, \ldots, s + \deg_t \varphi_a$.

Lemma 4.3.5. *A necessary and sufficient condition for g to be in $\mathrm{End}_{\overline{K}}(\varphi)$ is that $y_1, \ldots, y_s$ fulfil the equations* (4.3.3) *and* (4.3.4).

Proof. By construction, the system of equations is equivalent to the condition that g commutes with φ_a, which is clearly necessary for g to be an endomorphism. Conversely, if g and φ_a commute, by restricting φ to $\mathbb{F}_q[a]$, we obtain a Drinfeld $\mathbb{F}_q[a]$-module whose endomorphism ring contains both g and the image of A in $K[\tau]$ under φ. In generic characteristic the endomorphism ring is commutative, so it follows that g commutes with every element in $\varphi(A)$. □

Immediate from (4.3.3) is also the following

Proposition 4.3.6. *Let $\varphi : A \to K$ be a Drinfeld module in generic characteristic and $\overline{K}$ a fixed algebraic closure of K. Suppose $g \in \mathrm{End}_{\overline{K}}(\varphi)$ has constant coefficient $\varepsilon \in K$. Then g is defined over the field $K[\varepsilon]$.*

Algorithm 4.3.7 (Finding endomorphisms with prescribed constant coefficient)**.** Given a rank r Drinfeld A-module $\varphi : A \to K[\tau]$ in generic characteristic and an element $\varepsilon \in K$, which is integral over A, this algorithm determines if there is an endomorphism of φ with lowest coefficient ε. If so, the unique such endomorphism g is returned.

1. Determine the degree d_ε and the lowest coefficient a_ε of the minimal polynomial of ε over F. Compute $s := r \deg_A(a_\varepsilon)/d_\varepsilon$.
2. Pick a non-constant $a \in A$. Recursively determine the coefficients y_k using equations (4.3.3) for $k = 1, \ldots, s$.
3. Check if the y_k fulfill the system (4.3.4). If so, return g by giving the y_k, if not return that no endomorphism exists.

4.4 Saturation in the endomorphism ring

Let $\varphi : A \to K[\tau]$ be a Drinfeld module in generic characteristic. Suppose we know finitely many endomorphisms of φ, which generate an A-algebra S. We give a way to determine the saturation of S in $\mathrm{End}_K(\varphi)$ without knowing what the full endomorphism ring is yet.

Let L denote the quotient field of S in $\mathrm{End}_K^0(\varphi)$ and $\tilde{S}$ the integral closure of S in L. Then the saturation of S is $L \cap \mathrm{End}_K(\varphi)$ and we have inclusions $S \subseteq L \cap \mathrm{End}_K(\varphi) \subseteq \tilde{S}$. The idea of the algorithm is to use the fact that S has finite index in $\tilde{S}$, and to check for each coset $x + S \in \tilde{S}/S$ if it lies in $\mathrm{End}_K(\varphi)/S$. Since we are in generic characteristic, we can determine L and $\tilde{S}$ by considering the constant coefficients of the endomorphisms.

Algorithm 4.4.1 (Computing the saturation of a subalgebra of $\mathrm{End}_K(\varphi)$.)**.** Given a Drinfeld module $\varphi : A \to K$ in generic characteristic and $g_1, \ldots, g_n \in \mathrm{End}_K(\varphi)$, the algorithm returns a set of endomorphisms generating the saturation of $A[g_1, \ldots, g_n]$ in $\mathrm{End}_K(\varphi)$ as an algebra over A.

1. For $i = 1, \ldots, n$ let x_i denote the constant coefficient of g_i. Compute the subfield $L = F(x_1, \ldots, x_n)$ of K and let $S := A[x_1, \ldots, x_n]$.
2. Determine the integral closure $\tilde{S}$ of A in L using Algorithm 3.4.4. Let $\gamma_1, \ldots, \gamma_n$ be generators of $\tilde{S}$ as an algebra over A.
3. Since x_i is integral over A, we have $S \subseteq \tilde{S}$. They are finitely generated A-modules of the same rank $[L/K]$. It follows that $\tilde{S}/S$ is finite. Compute a set $\mathcal{S} \subset \tilde{S}$ of representatives for the cosets of S in $\tilde{S}$.
4. Compute $a \in A$ for which $a\tilde{S} \subseteq S$.
5. For each $y \in R$, express $ay \in S$ as a polynomial in $x_1, \ldots, x_n$ with coefficients in A. Let g_{ay} be the endomorphism obtained by replacing each x_i by g_i in the polynomial expression.
6. For each $y \in R$, if the right division of g_{ay} by φ_a in $K[\tau]$ has no remainder, let g_y be the resulting endomorphism. The collection of all g_y that are found in this way generate the saturation of the $A[g_1, \ldots, g_n]$ in $\mathrm{End}_K(\varphi)$.

4.5 Drinfeld modules over finite fields

Let k be a finite field extension of $\mathbb{F}_q$ of degree $d < \infty$ and $\varphi : A \to k[\tau]$ a Drinfeld module over k of rank r. The center of $k[\tau]$ is $\mathbb{F}_q[\tau^d]$. We use the notation $k(\tau) := k[\tau] \otimes_{\mathbb{F}_q[\tau^d]} \mathbb{F}_q(\tau^d)$. One can check that this is a central simple algebra over $\mathbb{F}_q(\tau^d)$ and in fact a division ring. Under the embedding φ, we view A as contained in $k[\tau]$ and, under the unique extension of the embedding, F as contained in $k(\tau)$.

Theorem 4.5.1 (cf. [Gos96], Lemma 4.12.7 and Theorem 4.12.8)**.** *The center of* $\mathrm{End}_k^0(\varphi)$ *is the field* $L = F(\tau^d)$*. Let* a *denote the degree of the field extension* L/F *and* b^2 *the dimension the central simple* L*-algebra* $\mathrm{End}_K^0(\varphi)$*. Then the rank of* φ *is equal to* ab*.*

This result can be used to characterize when the endomorphism ring is commutative.

Theorem 4.5.2. *The following are equivalent:*

(a) $\mathrm{End}_k(\varphi)$ *is commutative.*

(b) $\mathrm{End}_k^0(\varphi) = F(\tau^d)$*.*

(c) $[F(\tau^d)/F] = r$*.*

(d) $[F(\tau^d)/\mathbb{F}_q(\tau^d)] = d$*.*

(e) $\mathrm{End}_k(\varphi)$ *is the saturation as an* $\mathbb{F}_q[\tau^d]$*-module of* $A[\tau^d]$ *inside* $k[\tau]$*.*

Proof. By Theorem 4.5.1, the statements (a),(b) and (c) are equivalent. Since τ^d lies in the center of $k[\tau]$, we have $\mathrm{End}_k(\varphi) = Z_{k[\tau]}(A) = Z_{k[\tau]}(A[\tau^d])$, which implies $\mathrm{End}_k^0(\varphi) = Z_{k(\tau)}(A) = Z_{k(\tau)}(F(\tau^d))$. We also have the inclusion $F(\tau^d) \subseteq \mathrm{End}_k^0(\varphi)$ of $\mathbb{F}_q(\tau^d)$-algebras. Combining this with Theorem 3.5.3 applied to the central simple $\mathbb{F}_q(\tau^d)$-algebra $k(\tau)$ yields:

$$\left(\dim_{\mathbb{F}_q(\tau^d)} F(\tau^d)\right)^2 \leq \dim_{\mathbb{F}_q(\tau^d)} F(\tau^d) \dim_{\mathbb{F}_q(\tau^d)} \mathrm{End}_k^0(\varphi) = d^2,$$

with equality if and only if $F(\tau^d) = \mathrm{End}_k^0(\varphi)$. Hence (b) and (d) are equivalent. Finally, it is straightforward to check that $\mathrm{End}_k(\varphi) = \mathrm{End}_k^0(\varphi) \cap k[\tau]$, from which equivalence of (b) and (e) follows. □

Combining this with the earlier results about the endomorphism ring we also find

Proposition 4.5.3. *If* φ *has height one, then* $\mathrm{End}_k(\varphi) = \mathrm{End}_{\overline{k}}(\varphi)$ *for* $\overline{k}$ *the algebraic closure of* k*.*

Proof. Proposition 4.2.3 tells us that the endomorphism ring over the algebraic closure is commutative and moreover that the degree of the field extension $\mathrm{End}_{\overline{k}}^0(\varphi)/F$ divides r. Since $\mathrm{End}_k^0(\varphi)$, which is contained in $\mathrm{End}_{\overline{k}}^0$, has degree exactly r over F by Theorem 4.5.2, it follows that the $\mathrm{End}_k^0(\varphi) = \mathrm{End}_{\overline{k}}^0(\varphi)$. So for any endomorphism g of φ over $\overline{k}$, there are $a \in A$ and an endomorphism h of φ over k such that $g\varphi_a = h$. That means g is equal to the right division of h by φ_a. Since both h and φ_a have coefficients in k, it follows that $g \in k[\tau]$. □

4.6 The Frobenius endomorphism

Let $k = \mathbb{F}_q[\zeta]$ be a finite field extension of $\mathbb{F}_q$ of degree d. Let $\varphi : A \to k[\tau]$ be a Drinfeld module of rank r and height 1 over k. By Proposition 4.2.3, the endomorphism ring of φ is commutative. As in 4.5, we identify F naturally with a subfield of $k(\tau)$. By Theorem 4.5.2, the Frobenius element τ^d generates a field extension of degree r over F. Since endomorphisms are integral over A, it follows by [AM69], Proposition 5.15, that τ^d is the zero of a monic irreducible polynomial of degree r over A. We will present two methods to compute this polynomial.

Variant a): The idea is to first obtain an explicit representation of the ring $A[\tau^d]$. Suppose A is given by generators $\gamma_1, \ldots, \gamma_n$ over $\mathbb{F}_q$. Then we need to determine the kernel of the ring homomorphism

$$\Phi : \mathbb{F}_q[X][Y_1, \ldots, Y_n] \to k[\tau],$$

sending X to τ^d and Y_i to γ_i for $i = 1, \ldots, n$, so the image of Φ is exactly $A[\tau^d]$. The minimal polynomial of τ^d over A can be found from any element of the kernel which is monic of degree r in X by substituting γ_i for Y_i for $i = 1, \ldots, n$. The existence of the minimal polynomial ensures that such an element exists.

Algorithm 4.6.1 (Minimal Polynomial of the Frobenius)**.** Given a finite field k of degree d over $\mathbb{F}_q$ and a Drinfeld A-module φ over k of rank r and height 1, the minimal polynomial f of τ^d over the image of A in $k[\tau]$ is returned.

1. Fix the basis of the $\mathbb{F}_q[\tau^d]$-module $k[\tau]$ given by $(\zeta^i \tau^j)_{0 \le i,j \le d-1}$. The subring $A[\tau^d]$ acts faithfully on $k[\tau]$. For $i = 1, \ldots, n$, determine a monic polynomial of degree d^2 for γ_i over $\mathbb{F}_q[\tau^d]$, which exists by the theorem of Cayley-Hamilton. By replacing τ^d by X and γ_i by Y_i, we obtain an element $g_i \in \mathrm{Ker}(\Phi)$ for each $i = 1, \ldots, n$.

2. Let $\mathcal{J} = (g_1, \ldots, g_n)$. The induced homomorphism

   $$\mathbb{F}_q[X][Y_1, \ldots, Y_n]/\mathcal{J} \to k[\tau]$$

   is a homomorphism of finitely generated free $\mathbb{F}_q[X]$ modules, where X acts on the right hand side by τ^d. A basis of the module on the left is given by $(Y_1^{k_1} \cdots Y_n^{k_n})_{0 \le k_1, \ldots, k_n \le d^2-1}$. Determine explicit generators for its kernel using the elementary divisor theorem. Let $g_{n+1}, \ldots, g_N$ be lifts to $\mathbb{F}_q[X][Y_1, \ldots, Y_n]$. Then $\mathrm{Ker}(\Phi) = (g_1, \ldots, g_N)$.

3. By a Gröbner basis computation determine an element of $g(X, Y_1, \ldots, Y_n) \in \mathrm{Ker}(\Phi)$ which is monic of degree r in X. Then the substitution $f(X) := g(X, \gamma_1, \ldots, \gamma_n) \in A[X]$ gives the minimal polynomial f of τ^d over A.

Variant b): We use the following theoretical result about the eigenvalues of the Frobenius: Let v_∞ denote the normalized valuation at the place of infinity of F and $\overline{v}_\infty$ its continuation to an algebraic closure $\overline{F}$. Let $f = X^r + a_1 X^{r-1} + \cdots + a_{r-1} X + a_r$ denote the minimal polynomial of τ^d over F.

Theorem 4.6.2. *For any zero α of f in $\overline{F}$, we have*

$$\overline{v}_\infty(\alpha) = -\frac{1}{r}\frac{d}{d_\infty}.$$

Proof. This is part (f) in [Yu95], Theorem 1. It can also be seen in the following way: The theorem is equivalent to the statement that the Newton polygon of f has the single slope $-d/(rd_\infty)$. We work inside $k(\tau)$. Let $\tilde{A}$ denote the integral closure of A in $F(\tau^d)$. This is an admissible coefficient ring by Theorem 4.2.1, has rank r as an A-algebra and contains $\mathrm{End}_k(\varphi)$. From the discussion preceding Proposition 3.2.5 this tells us that the Newton Polygon of f has a single slope, which must be equal to $v_\infty(a_r)/r$. We will show that $\deg_{\tilde{A}} \tau^d = d$ (*). The theorem follows from this, since by Proposition 3.2.5, and the formula $\deg_A = -d_\infty v_\infty$ (3.2.2), we have

$$\frac{1}{r}v_\infty(a) = -\frac{1}{r}\frac{\deg_A a}{d_\infty} = -\frac{1}{r}\frac{\deg_{\tilde{A}} \tau^d}{d_\infty} = -\frac{1}{r}\frac{d}{d_\infty}.$$

We will show (*) first in the case that $\mathrm{End}_k(\varphi)$ is integrally closed, which is equivalent to $\mathrm{End}_k(\varphi) = \tilde{A}$. In that case, φ extends to a Drinfeld $\tilde{A}$-module of rank $\tilde{r} = 1$. We have

$$d = \deg_\tau \tau^d = \tilde{r} \deg_{\tilde{A}} \tau^d = \deg_{\tilde{A}} \tau^d.$$

In the general situation we can find an isogeny $g : \varphi \to \varphi'$ of Drinfeld A-modules over k, such that $\mathrm{End}_k(\varphi') = \tilde{A}$. We now have two different ways to view $F(\tau^d) = \mathrm{End}_k^0(\varphi)$ as an A-algebra, induced by φ and φ' respectively, which are related by the isomorphism (4.1.1). Since τ^d commutes with g, by the characterization of (4.1.1), it corresponds to itself. Therefore it has the same minimal polynomial over A regardless of wether we embed A via φ or via φ' . □

By Theorem 4.6.2, the Newton polygon of f has the single slope $-\frac{d}{rd_\infty}$ (which was already used in the proof). With $f(X) = X^r + a_1X^{r-1} + \cdots + a_r$, and the formula $\deg_A(a) = -d_\infty v_\infty(a)$ for $a \in A$, it follows that

$$\deg_A(a_r) = d \text{ and } \deg_A(a_k) \leq \frac{k}{r}d \text{ for } k = 1, \ldots, r-1.$$

This implies also that $\deg_\tau \varphi_{a_i}\tau^{d(r-i)} \leq rd$ for $i = 1, \ldots, r$. For a positive integer k, let $A_{\leq k}$ denote the $\mathbb{F}_q$ vector space of elements of A of degree at most k.

Algorithm 4.6.3 (Minimal Polynomial of the Frobenius, second version)**.** Given a finite field k of degree d over $\mathbb{F}_q$ and a Drinfeld A-module φ over k of rank r and height 1, the minimal polynomial f of τ^d over the image of A in $k[\tau]$ is returned.

1. Use Algorithm 3.3.6 to give a graded basis for the $\mathbb{F}_q$-subspace $A_{\leq d}$ of A of elements with degree at most d.
2. For $k = 1, \ldots, r$ let d_k the biggest positive integer not bigger than $\frac{kd}{r}$.

3. Compute the unique zero of the $\mathbb{F}_q$-affine linear map

$$\begin{array}{ccc} A_{d_1} \oplus \cdots \oplus A_{d_{r-1}} \oplus A_{d_r} & \longrightarrow & k[\tau] \\ (a_1, \ldots, a_{r-1}, a_r) & \longmapsto & \tau^{dr} + a_1\tau^{d(r-1)} + \cdots + a_{r-1}\tau^d + a_r. \end{array}$$

This yields the coefficients $(a_1, \ldots, a_r)$ of f.

4.7 Reduction of Drinfeld modules

Let K be a finite extension of F and $\varphi : A \to K$ a Drinfeld A-module whose characteristic homomorphism is the natural inclusion $A \subseteq K$.

Let v be a place of K with local ring $\mathcal{O}_v$ and residue field k_v.

Definition 4.7.1. (a) We say φ *is defined over* $\mathcal{O}_v$, if for every $a \in A$ the coefficients of φ_a lie in $\mathcal{O}_v$, and if moreover the induced homomorphism $\varphi_v : A \to k_v[\tau]$ defines a Drinfeld module over k_v of the same rank as φ.

(b) We say φ *has good reduction at* v, if φ is isomorphic over K to a Drinfeld module which is defined over $\mathcal{O}_v$.

(c) Suppose φ has good reduction at v. We say φ *has ordinary reduction at* v if it is isomorphic to a Drinfeld module which is defined over $\mathcal{O}_v$ and whose reduction at v has height 1.

Remark 4.7.2. An equivalent condition for φ to be defined over $\mathcal{O}_v$ is that $\varphi(A) \subseteq \mathcal{O}_v[\tau]$ and for every nonzero $a \in A$, the highest coefficient of φ_a is a unit in $\mathcal{O}_v$.

Immediately from this characterization we get

Lemma 4.7.3. *If φ is defined over $\mathcal{O}_v$, then for any nonzero $a \in A$ and for any overfield L of K, every zero of φ_a in L is integral over $\mathcal{O}_v$.*

Proof. Let u be the highest coefficient of φ_a, which by Remark 4.7.2 is a unit in $\mathcal{O}_v$. Then $u^{-1}\varphi_a$ is a monic polynomial with coefficients in $\mathcal{O}_v$ and has the same zeros in L as φ_a. □

The following standard result shows that reduction makes sense for homomorphisms of Drinfeld A-modules defined over $\mathcal{O}_v$:

Proposition 4.7.4. *Suppose φ, φ' are Drinfeld A-modules defined over $\mathcal{O}_v$. Then every isogeny from φ to φ' over K has coefficients in $\mathcal{O}_v$ with leading coefficient a unit. In particular, there is a well-defined injective reduction homomorphism*

$$\mathrm{Hom}_K(\varphi, \varphi') \to \mathrm{Hom}_{k_v}(\varphi_v, \varphi'_v).$$

Definition 4.7.5. We will denote the image of $f \in \mathrm{Hom}_K(\varphi, \varphi')$ under reduction by f_v.

Proof. Let $e \in K[\tau]$ be a dual isogeny to f, such that $ef = \varphi_a$ for some non-zero $a \in A$. Let $\overline{K}$ be an algebraic closure of K. Then we have $\mathrm{Ker}_{\overline{K}} f \subseteq \mathrm{Ker}_{\overline{K}} \varphi_a$. By assumption, φ is defined over $\mathcal{O}_v$, so it follows by Lemma 4.7.3 that all elements of $\mathrm{Ker}_{\overline{K}} \varphi_a$ are integral over $\mathcal{O}_v$. Therefore all zeros of f in $\overline{K}$ are integral over $\mathcal{O}_v$.

Let y denote the highest coefficient of f. For non-constant $b \in A$, comparing the highest coefficient in the relation $\varphi_b f = f\varphi_b$ shows that $y^{(q^k-1)} = u$ for some $k \geq 1$ and some unit $u \in \mathcal{O}_v^*$. Since $\mathcal{O}_v$ is integrally closed in K, it follows that $y \in \mathcal{O}_v$. In any ring, a root of a unit is a unit, so y is a unit in $\mathcal{O}_v$.

Since all zeros of f are integral over $\mathcal{O}_v$, it follows that the monic polynomial $y^{-1}f$ has coefficients which are integral over $\mathcal{O}_v$ and lie in K. The valuation ring $\mathcal{O}_v$ is integrally closed in K, so the coefficients already lie in $\mathcal{O}_v$. Multiplying with y, which we have shown to be a unit in $\mathcal{O}_v$, gives that f has coefficients in $\mathcal{O}_v$ with highest coefficient a unit. The existence and injectivity of the reduction homomorphism follow directly. □

Remark 4.7.6. If φ has good reduction at v one might choose different isomorphic Drinfeld modules φ' and φ'', which are defined over $\mathcal{O}_v$. By Proposition 4.7.4, any isomorphism $\varphi' \to \varphi''$ over K reduces to an isomorphism of their reductions over k_v. Therefore the reduction of φ is well-defined up to isomorphism over k_v.

Proposition 4.7.7. *If a Drinfeld A-module φ over K has good reduction at a place v, then every Drinfeld A-module which is isogenous to φ over K has good reduction at v. The height of the reduction of a Drinfeld module at a place of good reduction is invariant under isogenies.*

Proof. Suppose $f : \varphi \to \varphi'$ is an isogeny between Drinfeld modules over K. After replacing φ by a Drinfeld module which is isomorphic to φ over K, we can assume that φ is defined over $\mathcal{O}_v$. We also replace f by $u^{-1}f$ and φ' by the Drinfeld module given by $a \mapsto u^{-1}\varphi' u$, whereby we can assume that the highest coefficient of f is equal to one. Then by the same argument as in the proof of Proposition 4.7.4, all coefficients of f lie in $\mathcal{O}_v$.

For any $a \in A$ we have the relation $\varphi'_a f = f\varphi_a$. This shows that φ'_a is the result of applying the right division by f in $K[\tau]$ to a certain $\mathbb{F}_q$-linear polynomial with coefficients in $\mathcal{O}_v$. Since f is monic with coefficients in $\mathcal{O}_v$, it follows that φ'_a has coefficients in $\mathcal{O}_v$. Comparing the highest coefficients in $\varphi'_a f = f\varphi_a$ shows that the leading coefficient of φ'_a is a unit in $\mathcal{O}_v$. Hence φ' is defined over $\mathcal{O}_v$, in particular it has good reduction at v.

Concerning the heights, note that by reducing the coefficients of f we obtain an isogeny between the reductions of φ and φ'. By Proposition 2.2.7, isogenous Drinfeld modules have the same height. □

We are interested in places of ordinary reduction because they guarantee us that the reduction will have a commutative endomorphism ring. The following theorem tells us, when we can find a place with ordinary reduction. It is a direct consequence of [Pin97, Theorem 0.3] and the fact that all endomorphisms of a Drinfeld module are already defined over some separable extension of its field of definition.

Theorem 4.7.8. *The Drinfeld module φ has good and ordinary reduction at some place of K if and only if $\mathrm{End}_K(\varphi)$ is separable over A. In this case, there are infinitely many places of K, where φ has good and ordinary reduction.*

4.8 Image of End under reduction

Let K be a finite extension of F and let $\varphi : A \to K[\tau]$ be a Drinfeld module over K whose characteristic morphism is the inclusion $A \subseteq K$. We prepare for the proof of Proposition 4.8.9, which will be an important tool for computing the endomorphism ring.

Let v be a place of K and suppose that φ is defined over $\mathcal{O}_v$. Let $\mathfrak{p}_0$ be the characteristic ideal and h the height of φ_v. By Proposition 4.7.4, we have a canonical embedding $\mathrm{End}_K(\varphi) \to \mathrm{End}_{k_v}(\varphi_v)$. Let $\overline{K}$ denote an algebraic closure of K and let $\overline{\mathcal{O}_v}$ denote the integral closure of $\mathcal{O}_v$ in $\overline{K}$. Fix a maximal ideal $\overline{\mathfrak{m}_v}$ of $\overline{\mathcal{O}_v}$ lying over $\mathfrak{m}_v$. The residue field $\overline{k_v} := \overline{\mathcal{O}_v}/\overline{\mathfrak{m}_v}$ is naturally an algebraic closure of k_v. We let $\mathcal{R} : \overline{\mathcal{O}_v} \to \overline{k_v}$ be the quotient map. This gives a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_v & \longrightarrow & k_v \\ \downarrow & & \downarrow \\ \overline{\mathcal{O}_v} & \longrightarrow & \overline{k_v} \end{array}$$

In fact, this is a diagram of A-modules, where A acts via φ on the objects on the left half and via φ_v on those of the right half of the diagram.

By Proposition 4.7.4, for any nonzero $f \in \mathrm{End}_K(\varphi)$ the zeros of f in $\overline{K}$ are integral over $\mathcal{O}_v$ and therefore lie in $\overline{\mathcal{O}_v}$.

Lemma 4.8.1. *The restriction of $\mathcal{R}$ to*

$$\mathrm{Ker}_{\overline{K}} f \to \mathrm{Ker}_{\overline{k_v}} f_v$$

is surjective. In the case $f = \varphi_a$, with $a \notin \mathfrak{p}_0$ it is an isomorphism.

Proof. The factorization in $\overline{\mathcal{O}_v}[X] \subseteq \overline{K}[X]$ into linear factors reduces to a factorization in $\overline{k_v}[X]$. This shows surjectivity. If $f = \varphi_a$ and $a \notin \mathfrak{p}_0$, then $\mathrm{ord}_\tau \varphi_{v,a} = 0$, which means $\varphi_{v,a}$ is separable. It follows that φ_a and $\varphi_{v,a}$ have the same number of zeros, which implies that the restriction of $\mathcal{R}$ is bijective, since we already know it is surjective. □

Lemma 4.8.2. *For any maximal ideal $\mathfrak{p}$ of A and any $n \geq 0$, the restriction of $\mathcal{R}$ gives a surjective A-module homomorphism*

$$\mathcal{R}|_{\varphi[\mathfrak{p}^n](\overline{K})} : \varphi[\mathfrak{p}^n](\overline{K}) \to \varphi_v[\mathfrak{p}^n](\overline{k_v}).$$

(a) If $\mathfrak{p} \neq \mathfrak{p}_0$, this is an isomorphism.

(b) For $\mathfrak{p} = \mathfrak{p}_0$, the kernel of $\mathcal{R}|_{\varphi[\mathfrak{p}_0^n](\overline{K})}$ is isomorphic to $(A/\mathfrak{p}_0^n)^{\oplus h}$ and is a direct summand of $\varphi[\mathfrak{p}^n](\overline{K})$.

Proof. Pick any nonzero $a \in \mathfrak{p}^n$. We have $\varphi[\mathfrak{p}^n](\overline{K}) \subseteq \mathrm{Ker}_{\overline{K}}\, \varphi_a \subseteq \overline{\mathcal{O}_v}$, so it makes sense to speak of the restriction of $\mathcal{R}$.

Suppose first that for some $b \in A$ we have $\mathfrak{p}^n = (b)$. Then surjectivity follows from Lemma 4.8.1 for $f = \varphi_b$. In general, we can find $N \geq n$, such that $\mathfrak{p}^N = (b)$ for some $b \in A$, due to the fact that A has finite class number. Pick $c \in A$ with $\mathrm{ord}_{\mathfrak{p}}\, c = N - n$. Then we have a commutative diagram

$$\begin{array}{ccc} \varphi[\mathfrak{p}^N](\overline{K}) & \xrightarrow{\mathcal{R}|} & \varphi_v[\mathfrak{p}^N](\overline{k_v}) \\ \downarrow{\scriptstyle \varphi_c} & & \downarrow{\scriptstyle \varphi_{v,c}} \\ \varphi[\mathfrak{p}^n](\overline{K}) & \xrightarrow{\mathcal{R}|} & \varphi_v[\mathfrak{p}^n](\overline{k_v}) \end{array}.$$

We have already shown that the top arrow is a surjection. The arrow on the right is surjective by Proposition 2.2.15, (b). It follows that the bottom arrow is also surjective, which is what we wanted to show.

Now (a) directly follows from the surjectivity since domain and range of the map in consideration are both isomorphic to $(A/\mathfrak{p}^n)^{\oplus r}$ by Proposition 2.2.15, (a) and therefore have the same finite cardinality.
It is left to show (b). Again by Proposition 2.2.15,the restriction of $\mathcal{R}$ is up to isomorphisms a homomorphism of $A/\mathfrak{p}_0^n$-modules of the form

$$(A/\mathfrak{p}_0^n)^{\oplus r} \to (A/\mathfrak{p}_0^n)^{\oplus (r-h)}.$$

We already know it is surjective. Since the image is free, it is split surjective. The kernel is of the form $\bigoplus_{i=1}^{k} A/\mathfrak{p}_0^{n_k}$ for $k \geq 0$ and $1 \leq n_1, \ldots, n_k \leq n$, and we must have

$$(A/\mathfrak{p}_0)^n \cong \bigoplus_{i=1}^{k} A/\mathfrak{p}_0^{n_k} \oplus (A/\mathfrak{p}_0^n)^{\oplus (r-h)}.$$

Comparing the submodules of both sides, which are annihilated by $\mathfrak{p}$ shows that $k = h$. Next we compare the lengths of both sides of the equality and find

$$nr = n_1 + \cdots + n_h + n(r-h) \leq nh + n(r-h) = nr.$$

The inequality here cannot be strict. Since all n_i are bounded above by n, they must all be equal to n. This shows the kernel is of the desired form. □

Now let $g \in \mathrm{End}_k(\varphi)$ be an endomorphism whose image g_v under reduction can be written as a product $g_v = \varphi_{v,a} h_v = h_v \varphi_{v,a}$ for some $a \in A$, and $h_v \in \mathrm{End}_{k_v}(\varphi_v)$ (we do *not* assume that h_v is actually the reduction of an element of $\mathrm{End}_K(\varphi)$). Let $\mathfrak{p}$ be a maximal ideal of A. For any A-module M let ${}_{\mathfrak{p}}M$ denote the $\mathfrak{p}$-power torsion submodule of M, which is made up of those elements of M that are annihilated by a power of $\mathfrak{p}$.

Lemma 4.8.3. *If $\mathfrak{p} \neq \mathfrak{p}_0$, we have*

$$ {}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{K}}(\varphi_a)\right) \subseteq {}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{K}}(g)\right). \tag{4.8.4} $$

Proof. By the assumption $g_v = h_v \varphi_{v,a}$, we have the inclusion

$$ \mathrm{Ker}_{\overline{k_v}}(\varphi_{v,a}) \subseteq \mathrm{Ker}_{\overline{k_v}}(g_v), $$

which implies

$$ {}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{k_v}} \varphi_{v,a}\right) \subseteq {}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{k_v}} g_v\right). \tag{4.8.5} $$

Choose a nonzero $b \in A$, such that both φ_a and g divide φ_b in $\mathrm{End}_K(\varphi)$. Both $\mathrm{Ker}_{\overline{K}} \varphi_a$ and $\mathrm{Ker}_{\overline{K}} g$ are A-submodules of $\mathrm{Ker}_{\overline{K}} \varphi_b$, and hence their $\mathfrak{p}$-power torsion submodules are contained in ${}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{K}} \varphi_b\right) = \varphi[\mathfrak{p}^n](\overline{K})$, where $n = \mathrm{ord}_{\mathfrak{p}}(b)$. By Lemma 4.8.2, the restriction of $\mathcal{R}$ to $\varphi[\mathfrak{p}^n](\overline{K})$ is injective. Therefore the inclusion (4.8.4) is equivalent to

$$ \mathcal{R}\left({}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{K}} \varphi_a\right)\right) \subseteq \mathcal{R}\left({}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{K}} g\right)\right). \tag{4.8.6} $$

We claim this is exactly inclusion (4.8.5), which we know to be true. Showing this finishes the proof. It is generally true that for a torsion A-module M and an A-module homomorphism $\theta : M \to N$, we have ${}_{\mathfrak{p}}\theta(M) = \theta({}_{\mathfrak{p}}M)$. This follows from the fact that any torsion module decomposes as a direct sum of its prime power torsion modules for the different prime ideals of A. Now we combine this with Lemma 4.8.1 and find that for any endomorphism $f \in \mathrm{End}_K(\varphi)$, we have

$$ \mathcal{R}\left({}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{K}} f\right)\right) = {}_{\mathfrak{p}}\left(\mathcal{R}\left(\mathrm{Ker}_{\overline{K}} f\right)\right) = {}_{\mathfrak{p}}\left(\mathrm{Ker}_{\overline{k_v}} f_v\right). $$

It remains to use this on both sides of (4.8.6). □

Proposition 4.8.7. *The torsion submodule of the cokernel of the embedding $\mathrm{End}_K(\varphi) \hookrightarrow \mathrm{End}_{k_v}(\varphi_v)$ is annihilated by a power of $\mathfrak{p}_0$.*

Proof. Suppose $h_v \in \mathrm{End}_{\overline{k_v}}(\varphi_v)$ represents a torsion element of the cokernel of $\mathrm{End}_{\overline{K}}(\varphi) \hookrightarrow \mathrm{End}_{\overline{k_v}}(\varphi_v)$, i.e. there are nonzero $a \in A$ and $g \in \mathrm{End}_K(\varphi)$ such that $g_v = \varphi_{v,a} h_v = h_v \varphi_{a,v}$. Let $N \geq \mathrm{ord}_{\mathfrak{p}_0}(a)$, such that $\mathfrak{p}_0^N = (b)$ for some $b \in A$. We claim that

$$ \mathrm{Ker}_{\overline{K}} \varphi_a \subseteq \mathrm{Ker}_{\overline{K}}(g \varphi_b). \tag{4.8.8} $$

By the Chinese remainder theorem it is enough to check that the inclusion holds for all $\mathfrak{p}$-power torsion parts where $\mathfrak{p}$ runs through the maximal ideals of A. For $\mathfrak{p} \neq \mathfrak{p}_0$, this follows directly from Lemma 4.8.3, since $\varphi_{v,a}$ divides g_v. For $\mathfrak{p}_0$, we have

$$_{\mathfrak{p}_0}(\mathrm{Ker}_{\overline{K}}\,\varphi_a) = \varphi[\mathfrak{p}_0^{\mathrm{ord}_{\mathfrak{p}_0}(a)}](\overline{K}) \subseteq \varphi[\mathfrak{p}_0^N](\overline{K}) = \mathrm{Ker}_{\overline{K}}(\varphi_b).$$

Since φ_a is separable, 4.8.8 implies that it divides $g\varphi_b$ from the right in $K[\tau]$, say $g\varphi_b = \tilde{h}\varphi_a \in \mathrm{End}_K(\varphi)$. It follows that $\varphi_a\tilde{h}\varphi_a = \tilde{h}\varphi_a^2$. Right-division by φ_a shows that $\tilde{h}$ commutes with φ_a, which implies $\tilde{h} \in \mathrm{End}_K(\varphi)$, since we are in generic characteristic. Now we pass to the reduction and find

$$\tilde{h}_v\varphi_{v,a} = g_v\varphi_{v,b} = \varphi_{v,a}h_v\varphi_{v,b} = \varphi_{v,b}h_v\varphi_{v,a}.$$

Right-division by $\varphi_{v,a}$ in $k_v[\tau]$ shows that $\varphi_{v,b}h_v$ lies in the image of $\mathrm{End}_K(\varphi)$. This shows that the image of h_v in the cokernel is annihilated by a power of $\mathfrak{p}_0$. □

Proposition 4.8.9. *Let v and w be places of K. Suppose φ is defined over both $\mathcal{O}_v$ and $\mathcal{O}_w$ and let $\mathfrak{p}_v$ be the maximal ideal of A lying under v and $\mathfrak{p}_w$ the one lying under w. Suppose further that $\mathfrak{p}_v \neq \mathfrak{p}_w$. Then the image of the combined reduction homomorphism*

$$\begin{aligned} \mathrm{End}_K(\varphi) &\to \mathrm{End}_{k_v}(\varphi_v) \oplus \mathrm{End}_{k_w}(\varphi_w) \\ g &\mapsto (g_v, g_w) \end{aligned}$$

is a saturated A-submodule of $\mathrm{End}_{k_v}(\varphi_v) \oplus \mathrm{End}_{k_w}(\varphi_w)$.

Proof. By Proposition 4.8.7, we are in the following situation: We have torsion-free A-modules M, M_1 and M_2 with injective homomorphisms $j_1 : M \hookrightarrow M_1$ and $j_2 : M \hookrightarrow M_2$, such that the torsion submodule T_1 of $M_1/j_1(M)$ is annihilated by a power of $\mathfrak{p}_v$ and the torsion submodule T_2 of $M_2/j_2(M)$ by a power of $\mathfrak{p}_w$. We want to show that the image of $j : M \to M_1 \oplus M_2, m \mapsto (j_1(m), j_2(m))$ is saturated in $M_1 \oplus M_2$.

Suppose $\mathfrak{p}_v^{k_1}T_1 = 0$ and $\mathfrak{p}_w^{k_2}T_2 = 0$. By the Chinese remainder theorem, there is $b \in A$ with $b \in \mathfrak{p}_v^{k_1}$ and $b \notin \mathfrak{p}_w$. Since b is contained in only finitely many maximal ideals of A, there exists $c \in A$ with $c \in \mathfrak{p}_w^{k_2}$ and such that b and c are relatively prime, say $xb+yc = 1$ for $x, y \in A$.

Now suppose we have $m_1 \in M_1$, $m_2 \in M_2$ and nonzero $a \in A$, such that $a(m_1, m_2) = j(m)$ for some $m \in M$. It follows that $m_1 + j_1(M) \in T_1$ and, since by construction $bT_1 = 0$, that $bm_1 = j_1(n)$ for some $n \in M$. Similarly, there is $l \in M$ with $cm_2 = j_2(l)$. Now we compute

$$j_1(an) = abm_1 = j_1(bm).$$

Since j_1 is injective, we have $an = bm$. This implies $aj_2(n) = bj_2(m) = abm_2$ and since M_2 is torsion free that $j_2(n) = bm_2$. Let $\tilde{m} = xn + yl$. Then

$$j_2(\tilde{m}) = xbm_2 + ycm_2 = (xb + yc)m_2 = m_2.$$

By symmetry of the argument we also have $j_1(\tilde{m}) = m_1$. This shows that indeed the image of j is saturated.

□

The following example shows that when we consider a single place v, the image of $\mathrm{End}_K(\varphi)$ in $\mathrm{End}_{k_v}(\varphi_v)$ need not be saturated.

Example 4.8.10. Let $A = \mathbb{F}_q[t]$ with field of fractions $F = \mathbb{F}_q(t)$. Let K be the field extension obtained by first adjoining a $2(q-1)$-st root s of t and then a solution ξ of the equation $X^q - s^{q-1}X - s = 0$, which is irreducible by the Eisenstein criterion. Let v be the valuation on F associated to the prime ideal (t) of A and normalized by $v(t) = 1$. This v extends uniquely to a valuation on K, which we also denote by v. We then have

$$v(s) = \frac{1}{2(q-1)},\ v(\xi) = \frac{1}{2q(q-1)}.$$

To see this, one considers the Newton polygons: The minimal polynomial $X^{2(q-1)} - t$ of s over F has a Newton polygon with unique slope $1/(2(q-1))$, so there is a unique way to extend v to $F(s)$. Similarly the minimal polynomial $X^q - s^{q-1}X - s$ of ξ over $F(s)$ has the unique slope $1/(2q(q-1))$, so there is also only one way to extend v further from $F(s)$ to all of K. The claimed values of s and ξ can also be read off from this.

We define a Drinfeld A-module over K by

$$\varphi_t = \tau^2 - (\xi^{q-1} + t^q \xi^{q(1-q)})\tau + t.$$

We claim that φ has good reduction at v but that $\mathrm{End}_K(\varphi)$ is not saturated in $\mathrm{End}_{k_v}(\varphi_v)$:

The reduction of φ is given by $\varphi_{v,t} = \tau^2$. Therefore φ has good, but not ordinary reduction at v. The endomorphism ring of the reduction $\varphi_v : A \to \mathbb{F}_q[\tau]$ contains both τ and τ^3 and in $\mathbb{F}_q[\tau]$ we have the relation $\tau^3 = \varphi_{v,t}\tau$.

Claim 4.8.11. The endomorphism τ of φ_v does not lie in the image of $\mathrm{End}_K(\varphi)$.

Proof. Suppose τ is the image of some $g \in \mathrm{End}_K(\varphi)$. By injectivity of the reduction map we would then have $g^2 = \varphi_t$. By comparing highest and lowest coefficient in this equality, g must be of the form $g = \tau + \sqrt{t}$ for some square root of t in K. Comparing the τ-coefficient in $g^2 = \varphi_t$ then gives $\sqrt{t} + \sqrt{t}^q = -(\xi^{q-1} + t^q \xi^{q(1-q)})$. This is a contradiction, since the valuations of the respective sides of this equation are different. □

Claim 4.8.12. The endomorphism τ^3 of φ_v lies in the image of $\mathrm{End}_K(\varphi)$.

Proof. The additive polynomial

$$g = (\tau - \xi^{q-1})(\tau - s^{q-1})(\tau - t\xi^{1-q})$$

is an endomorphism of φ and its reduction is equal to τ^3. This can be seen by hand in the following way. Let π, $\tilde{g}$ and σ denote the first, second and third factor on the right hand side of this equality. Then one checks that $\pi\sigma = \varphi_t$ and that $\sigma\pi = \tilde{g}^2$. From this it follows that

$$g\varphi_t = \pi\tilde{g}\sigma\pi\sigma = \pi\tilde{g}^3\sigma = \pi\sigma\pi\tilde{g}\sigma = \varphi_t g.$$

The statement about the reduction follows from the fact that each factor reduces to τ. □

5 Main algorithm

We now put the preceding results together. Throughout this section K denotes a finite extension of F and φ a Drinfeld A-module over K of rank r. By Theorem 4.7.8, exactly one of the following must be true: Either there is a place v of K at which φ has good and ordinary reduction, or $\mathrm{End}_K(\varphi)$ is inseparable over A.

If the endomorphism ring is separable over A, we can therefore use our results, in particular Proposition 4.8.9 relating the endomorphism ring to its reductions, to compute $\mathrm{End}_K(\varphi)$, which is done in 5.1. If instead, there is an endomorphism of φ which is inseparable over A, we can use it to pass to a bigger coefficient ring and reduce to the computation of the endomorphism ring of a Drinfeld module over K of degree r/p whose coefficient ring is isomorphic to A. This is done in 5.2. Finally, we present a total algorithm in 5.3, which computes the endomorphism ring of φ by deciding which case we are in and calling the corresponding algorithm. In the inseparable case this gives a recursion, since the algorithm for the inseparable case calls the total algorithm. Each time this happens the rank of the Drinfeld module that is passed is strictly smaller than before, so the total algorithm still terminates.

5.1 The separable case

Algorithm

Algorithm 5.1.1 (Determining the endomorphism ring from the reduction at two places.)**.** Given a Drinfeld module $\varphi : A \to K[\tau]$ of rank r over a finite extension K of F and places v_1, v_2 of K which fulfil the premise of Proposition 4.8.9 and at which φ has ordinary reduction, this algorithm computes a finite list of elements of $K[\tau]$, which generate the endomorphism ring $\mathrm{End}_K(\varphi)$ as an A-algebra.

1. Compute the residue fields k_{v_i} and the reductions φ_{v_i} of φ for $i = 1, 2$.
2. For $i = 1, 2$ determine the minimal polynomial m_i of the Frobenius element $\tau^{d_{v_i}}$ over $\varphi_{v_i}(A)$ in $k_{v_i}[\tau]$ with Algorithm 4.6.3 for $i = 1, 2$. Let m_i^{sep} be the unique

separable irreducible polynomial over F for which $m_i(X) = m_i^{sep}(X^{p^{e_i}})$ for some $e_i \geq 0$.

3. For $i = 1, 2$ set $E_i = F[X]/(m_i^{sep})$. Use Algorithm 3.1.2 to obtain a list `IntFields` of intermediate fields of the field extension E_1/F. For each L in `IntFields`, compute a primitive element α_L over F and the minimal polynomial m_L of α_L over F.

4. Create a new list `Embeddings`. For L running through `IntFields`, determine all zeros of m_L in E_2 and for every such zero $\beta \in E_2$ add the pair (α_L, β) to `Embeddings`.

5. For every pair (α, β) in `Embeddings` determine a nonzero $a \in A$ such that both $a\alpha \in A[X]/(m_1^s) \subseteq E_1$ and $a\beta \in A[X]/(m_2^s) \subseteq E_2$. Replace (α, β) by $(a\alpha, a\beta)$.

6. Iterating over (α, β) in `Embeddings`, compute the minimal polynomial m of α over F and the zeros $\varepsilon_1, \ldots, \varepsilon_k$ of m in K. Collect all the elements of K found in this way in the list `Constants`.

7. For every ε in `Constants` use Algorithm 4.3.7 to find an endomorphism $g_\varepsilon \in K[\tau]$ with constant coefficient ε, if it exists. Let $\mathcal{S}$ be the set of all those g_ε.

8. Using Algorithm 4.4.1, determine the saturation as an A-module of the subalgebra generated by $\mathcal{S}$ in the endomorphism ring. This returns generators for $\mathrm{End}_K(\varphi)$.

Correctness

To simplify the notation, we identify F with its image in any arising F-algebra. First we collect some observations about the algorithm, which are straightforward to check.

- By Proposition 4.2.3, the endomorphism ring of φ_{v_i} is commutative for $i = 1, 2$.
- It follows that $\mathrm{End}^0_{k_{v_i}}(\varphi_{v_i}) = F(\tau^{d_{v_i}})$, and that it is a field of degree r over F.
- For $i = 1, 2$ the field E_i maps bijectively onto the maximal separable subfield of $\mathrm{End}^0_{k_{v_i}}(\varphi_{v_i})$ over F by identifying the image of X with $\left(\tau^{d_{v_i}}\right)^{e_i}$. We identify it for the following considerations with this subfield.
- Under this identification $A[X]/(m_i^{sep})$ is contained in the endomorphism ring of φ_{v_i}.
- The list `IntFields` lists all intermediate fields of E_1/F, hence all intermediate fields of $\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1})/F$ which are separable over F.
- The list `Embeddings` corresponds bijectively to the set of pairs (L, ι), where L is an intermediate field of E_1/F and $\iota : L \to E_2$ is an F-homomorphism. Hence it corresponds bijectively to the set of pairs (L, ι), where L is an intermediate field of $\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1})/F$ which is separable over F and $\iota : L \to \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$ is an F-homomorphism.

- In steps 6 and 7, exactly those endomorphisms of φ over K are computed which have the same minimal polynomial over F as some α which appears in a pair (α, β) of `Embeddings`.

Lemma 5.1.2. *After or before step 5, the set of entries in* `Embeddings` *corresponds bijectively to the set of F-subalgebras of $\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$, which are separable field extensions of F. A bijection is given by associating to a pair (α, β) the field generated by (α, β) over F in $\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$. Here F is identified with $\{(x, x) | x \in F\} \subseteq \mathrm{End}^0_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$.*

Proof. By the universal property of the direct product, the data of an F-subalgebra of $\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$ which is a separable field extension of F is equivalent to the data of separable subfield L of $\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1})$ containing F, together with an F-homomorphism $L \to \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$. The set of those corresponds bijectively to `Embeddings` by the remarks above. □

Abbreviate $E := \mathrm{End}^0_K(\varphi)$. Algorithm 4.4.1 allows us to determine the full endomorphism ring from any A-subalgebra $S \subseteq \mathrm{End}_K(\varphi)$ which has finite index in $\mathrm{End}_K(\varphi)$, or equivalently, which has also quotient field E. This happens in step 8 under the assumption that the set of endomorphisms $\mathcal{S}$ computed in step 7 generates E over F.

Therefore correctness of the algorithm follows from the

Claim 5.1.3. The set $\mathcal{S}$ contains some $g_0 \in \mathrm{End}_K(\varphi)$, which is a primitive element for E/F.

By Proposition 4.7.4 the reduction homomorphisms $\mathrm{End}_K(\varphi) \to \mathrm{End}_{k_{v_i}}(\varphi_{v_i})$ extend to embeddings $j_i : E \to \mathrm{End}^0_{k_{v_i}}(\varphi_{v_i})$ for $i = 1, 2$. Let $j := (j_1, j_2) : \mathrm{End}^0_K(\varphi) \to \mathrm{End}^0_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$. The A-submodule $j(\mathrm{End}_K(\varphi))$ is saturated in $\mathrm{End}_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}_{k_{v_2}}(\varphi_{v_2})$ by Proposition 4.8.9 . This implies

$$j(\mathrm{End}_K(\varphi)) = j(E) \cap \left(\mathrm{End}_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}_{k_{v_2}}(\varphi_{v_2})\right).$$

Now by Lemma 5.1.2, after step 5 there is (α_0, β_0) in `Embeddings`, which generates $j(E)$ over $j(F)$. Moreover, α_0 is an endomorphism of φ_{v_1} over k_{v_1} and β_0 of φ_{v_2} over k_{v_2}. Hence $(\alpha_0, \beta_0) \in j(\mathrm{End}_K(\varphi))$, say $(\alpha_0, \beta_0) = j(g_0)$ for some $g_0 \in \mathrm{End}_K(\varphi)$. Now g_0 has the same minimal polynomial over F as α and β. This implies that it will be found as an element of $\mathcal{S}$ in step 7. Since j induces a field isomorphism $E \to j(E)$, it follows that g_0 generates E over F. This shows Claim 5.1.3.

Over the algebraic closure

In order to compute the Endomorphism ring of φ over the algebraic closure $\overline{K}$ one replaces step 6 in Algorithm 5.1.1 by the following variation:

6'. Iterating over (α, β) in `Embeddings`, compute the minimal polynomial m of α over F, *extend K to a splitting field of m* and compute the zeros $\varepsilon_1, \ldots, \varepsilon_k$ of m in the new K. Collect all the zeros found in this way in the list `Constants`.

To see why this works let K' be a minimal finite separable extension of K, such that all endomorphisms of φ over an algebraic closure of K are already defined over K' and let v_i' be an extension of v_i to K' for $i = 1, 2$. Let $E' := \mathrm{End}^0_{K'}(\varphi)$, which is again a separable field extension of F.

By Proposition 4.5.3 we have $\mathrm{End}_{k_{v_i}}(\varphi_{v_i}) = \mathrm{End}_{k_{v_i'}}(\varphi_{v_i'})$. In particular E' embeds naturally as an F-algebra into

$$\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2}).$$

We can again apply Lemma 5.1.2 to see that after step 5 there is a pair (α, β) in `Embeddings` that generates the image of E' over F in $\mathrm{End}^0_{k_{v_1}}(\varphi_{v_1}) \oplus \mathrm{End}^0_{k_{v_2}}(\varphi_{v_2})$ and such that α and β are actually endomorphisms. By saturatedness, it follows that there exists an endomorphism g of φ over K' which maps to α under reduction. It follows that g has the same minimal polynomial m over F as α and that g generates E' over F. Let $\varepsilon' \in K'$ denote the constant coefficient of g, which is also a zero of m. Then by Proposition 4.3.6, g is already defined over $K[\epsilon']$. It follows that the endomorphism ring over K' is the same as over $K[\epsilon']$ and hence that $K' = K[\epsilon']$ by minimality of K'.

Let K'' be the field obtained by repeatedly extending K as in in step 6'. Since (α, β) is contained in `Embeddings` after step 5, in step 6' it is arranged that m has a zero in K'' which is contained in the list `Constants`. It follows that K' embeds in K'' and that the image of g in $K''[\tau]$ is added to $\mathcal{S}$ in step 7.

5.2 The inseparable case

Now we consider the case, where we know the endomorphism ring has elements that are inseparable over A and we assume we are given one such element explicitly. The algorithm assumes that we can compute the endomorphism ring for Drinfeld modules of rank strictly smaller than that of φ.

Algorithm 5.2.1 (Dealing with inseparability)**.** Given a Drinfeld module $\varphi : A \to K[\tau]$ of rank r over a finite extension K of F and an element $g \in K[\tau]$, whose constant coefficient is inseparable of degree p over F, this algorithm returns generators for the endomorphism ring $\mathrm{End}_K(\varphi)$ as an A-algebra.

1. Apply Algorithm 4.1.3 to the subalgebra $A[g]$ of $\mathrm{End}_K(\varphi)$ with the maximal order being the subring $A^{1/p}$ of p-th roots of elements of A in $A[g] \otimes_A F$. This yields a Drinfeld A-module φ' and an isogeny $f : \varphi \to \varphi'$ – all defined over K – such that the endomorphism ring of φ' contains $A^{1/p}$, in the sense that every element of $\varphi'(A)$ has a p-th root in the endomorphism ring.

2. Let e be a dual isogeny to f. Then $g' := fge$ is an endomorphism of φ' and we have $F(g') = F^{1/p}$ in $\mathrm{End}_K^0(\varphi')$. Apply Algorithm 4.4.1 to compute generators for $F^{1/p} \cap \mathrm{End}_K^0(\varphi)$. This way we extend φ' to a Drinfeld $A^{1/p}$-module over K of rank r/p, which we denote $\varphi^{1/p}$.

3. Call Algorithm 5.3.1 to compute generators $g'_1, \ldots, g'_n$ for $\mathrm{End}_K(\varphi^{1/p})$ as an $A^{1/p}$ algebra. Note that $\mathrm{End}_K^0(\varphi') = F(g', g'_1, \ldots, g'_n)$.

4. For $i = 1, \ldots, n$ compute $g_i = eg'_i f$. We have $\mathrm{End}_K^0(\varphi) = F(g, g_1, \ldots, g_n)$.

5. We obtain generators for $\mathrm{End}_K(\varphi)$ by applying Algorithm 4.4.1 to the A-algebra generated by the endomorphisms $g, g_1, \ldots, g_n$.

5.3 Synthesis

Algorithm 5.3.1. Given a Drinfeld module $\varphi : A \to K[\tau]$ of rank r over a finite extension K of F, this algorithm returns generators for the endomorphism ring $\mathrm{End}_K(\varphi)$ as an A-algebra. Let $\mathcal{P}$ be a list of the places of K and $\mathcal{A}$ a list of the elements of A, which are not p-th powers in A.

1. Take the next place v of $\mathcal{P}$. Check if φ is defined over $\mathcal{O}_v$ and has ordinary reduction at v. If yes, search through $\mathcal{P}$ until another such place w is found which lies over another prime ideal of A than V. Call Algorithm 5.1.1 to compute generators for $\mathrm{End}_K(\varphi)$, return those and finish the algorithm. If not, continue with step 2.

2. Take the next a in $\mathcal{A}$. Check if a has a p-th root $a^{1/p}$ in K, and if so call Algorithm 4.3.7 to find an endomorphism g of φ with constant coefficient $a^{1/p}$ if it exists. If such a g is found, call Algorithm 5.2.1, return the generators for $\mathrm{End}_K(\varphi)$ and finish. If a has no p-th root in $K \backslash A$ or if no endomorphism with constant coefficient a p-th root of a exists go to step 1.

6 Generalization to finitely generated extensions

In section 5 we have described how to compute the endomorphism ring of a Drinfeld module $\varphi : A \to K[\tau]$ if K is a finite extension of F. We will analyse how the algorithm can be generalized when we allow K to be transcendental over F. It turns out that we can use basically the same method as before, once we have dealt with the question how one can form reductions of φ in this situation.

6.1 Reductions

Let A be an admissible coefficient ring, R a commutative ring, and K a field which all contain a finite field $\mathbb{F}_q$. Let $r \geq 1$ be an integer. Similarly as in 4.7 we define

Definition 6.1.1. (a) A *Drinfeld A-module of rank r over R* is a ring homomorphism $\varphi : A \to R[\tau]$, such that for every $a \in A$ the highest coefficient of φ_a is a unit in R and we have $\deg_\tau \varphi_a = r \deg_A a$. We also say *$\varphi$ is defined over R.*

(b) Let $\varphi : A \to K[\tau]$ be a Drinfeld A-module over K, and suppose $R \subseteq K$. We say *φ has coefficients in R*, if $\varphi(A) \subseteq R[\tau]$.

If φ is a Drinfeld A-module of rank r over R, it naturally induces a Drinfeld A-module of rank r over every nonzero commutative R-algebra. In particular, if λ is a prime ideal of R with residue field k_λ, we obtain a Drinfeld module φ_λ of rank r over k_λ through the ring homomorphism $R \to k_\lambda$ associated to λ.

From now on we suppose R is a finitely generated integral $\mathbb{F}_q$-algebra and integrally closed with quotient field K. Let $\varphi : A \to K[\tau]$ be a Drinfeld module in generic characteristic, which is already defined over R. Via the characteristic homomorphism of φ, we view R as an overring of A. Let λ be a maximal ideal of R. Then by Hilbert's Nullstellensatz the residue field k_λ is a finite extension of $\mathbb{F}_q$. As a Drinfeld module over a finite field, the reduction φ_λ has special characteristic, which implies that λ contracts to a maximal ideal of A.

Definition 6.1.2. We say φ has *ordinary reduction* at λ if φ_λ has height one.

Now we formulate the results from earlier in this more general setting. Replacing $\mathcal{O}_v$ by R in the proofs of Lemma 4.7.3 and Proposition 4.7.4 respectively, we obtain

Lemma 6.1.3. *If φ is defined over R, then for any nonzero $a \in A$ and for any overfield L of K, every zero of φ_a in L is integral over R.*

Proposition 6.1.4. *Suppose φ, φ' are Drinfeld A-modules over R. Then every isogeny $f : \varphi \to \varphi'$ which is defined over K has coefficients in R with leading coefficient a unit. In particular, for every prime ideal λ of R we have an injective reduction homomorphism of A-modules*

$$\mathrm{Hom}_K(\varphi, \varphi') \to \mathrm{Hom}_{k_\lambda}(\varphi_\lambda, \varphi'_\lambda).$$

The discussion from subsection 4.8 also carries over directly when we consider maximal ideals of R instead of places of a function field and make the obvious modifications in the proofs. In particular

Proposition 6.1.5. *Let λ, μ be maximal ideals of R and let $\mathfrak{p}_\lambda$ and $\mathfrak{p}_\mu$ be the maximal ideals of A lying under λ and μ respectively. Suppose that $\mathfrak{p}_\lambda \neq \mathfrak{p}_\mu$. Then the image of*

$$\mathrm{End}_K(\varphi) \to \mathrm{End}_{k_\lambda}(\varphi_\lambda) \oplus \mathrm{End}_{k_\mu}(\varphi_\mu)$$

is a saturated A-submodule of $\mathrm{End}_{k_\lambda}(\varphi_\lambda) \oplus \mathrm{End}_{k_\mu}(\varphi_\mu)$.

Finally, the source from [Pin97, Theorem 0.3] we cited for Theorem 4.7.8 also applies to this more general case:

Theorem 6.1.6. *There is a maximal ideal of R at which φ has ordinary reduction if and only if $\mathrm{End}_K(\varphi)$ is separable over A. In this case the set of maximal ideals of R at which φ has ordinary reduction is a Zariski-dense subset of the prime spectrum of R.*

6.2 Finitely generated models

Let K be a finitely generated field containing $\mathbb{F}_q$ and $\varphi : A \to K[\tau]$ a Drinfeld module over K of rank r. We give a proof that there always is a ring R such that Proposition 6.1.5 is applicable.

Proposition 6.2.1. *There exists a finitely generated $\mathbb{F}_q$-subalgebra R of K, such that*

(a) the quotient field of R is K,

(b) R is integrally closed,

(c) φ is defined over R.

Proof. Choose nonzero generators $\gamma_1, \ldots, \gamma_n$ of A over $\mathbb{F}_q$. Let $\tilde{R} \subseteq K$ be the $\mathbb{F}_q$-algebra obtained by starting from $\mathbb{F}_q$ and adjoining all coefficients of φ_{γ_i} as well as the inverse of the top coefficient for $i = 1, \ldots, n$. It is clear that $\varphi(A) \subset \tilde{R}$. Suppose for contradiction that there exists $a \in A$ such that the top coefficient y of φ_a is not a unit in $\tilde{R}$. Then there exists a maximal ideal λ of $\tilde{R}$ containing y and we have $\deg_\tau \varphi_{\lambda,a} < \deg_\tau \varphi_a = r \deg_A a$. However, by looking at the reduction of φ_{γ_i} for any nonconstant γ_i, we find that φ_λ is a Drinfeld module of rank r over k_λ. So $\deg_\tau \varphi_{\lambda,a} = r \deg_A a$ and we have a contradiction.

We have shown that φ is defined over the finitely generated $\mathbb{F}_q$-algebra $\tilde{R}$ and hence over any overring. By adjoining a finite generating set of K, we can assume the quotient field of $\tilde{R}$ is K. Let R be the integral closure of $\tilde{R}$ in K. By Theorem 6.2.2 below, R is finitely generated as an $\tilde{R}$-module, so it is a finitely generated $\mathbb{F}_q$ algebra, which has all the properties specified in the proposition. □

Theorem 6.2.2. *Let B be an integral domain, which is a finitely generated algebra over a field and let K be the quotient field of B. Then for any finite field extension L/K, the integral closure of B in L is a finitely generated B-module.*

Proof. An integral domain for which the conclusion of the theorem holds is called a *Japanese ring*. According to Chapter 12 in Nagata's "Commutative algebra" ([Mat70]), every finitely generated algebra over a field is Japanese. More precisely, this is Theorem 72 in [Mat70] together with the definitions in the beginning of Chapter 12 there. □

6.3 Generalization of the Algorithm

We have pointed out how the necessary tools from the case where K is finite over F generalize to the general. Indeed the algorithms from section 5 can be adapted directly with the following modifications.

1.) Before computing anything else, one first computes an integrally closed, finitely generated $\mathbb{F}_q$ subalgebra R of K whose quotient field is K and such that φ is defined over R.

2.) In Algorithm 5.1.1 for the separable case, instead of places v, w one expects as input maximal ideals λ, μ of R at which φ has ordinary reduction and works with those instead. This also works for the variant to compute the endomorphism ring over the algebraic closure.

3.) The algorithm for the inseparable case works as stated.

4.) To adapt the total Algorithm 5.3.1 treating the general case, one has to replace $\mathcal{P}$ by a function which enumerates the maximal ideals of R instead of places of a global function field.

References

[AM69] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[BJ89] Stanisaw Balcerzyk and Tadeusz Jzefiak. *Commutative Noetherian and Krull Rings*. Ellis Horwood, 1989.

[DH] Pierre Deligne and Dale Husemller. Survey of Drinfeld modules. *Contemp Math.*, 67.

[Dri74] V G Drinfel'd. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561, 1974.

[Fli13] Yuval Z. Flicker. *Drinfeld Moduli Schemes and Automorphic Forms*. Springer, 2013.

[Gos96] David Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1996.

[GS06] Philippe Gille and Tams Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge University Press, 2006.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Science Publications, 2002.

[Mat70] Hideyuki Matsumura. *Commutative Algebra*. W.A. Benjamin, Inc., 1970.

[Neu90] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1990.

[PD12] Richard Pink and Anna Devic. Adelic openness for Drinfeld modules in special characteristic. *J. Number Theory*, 132(7):1583 1625, 2012.

[Pin97] Richard Pink. The Mumford-Tate conjecture for Drinfeld-modules. *Publ. Res. Inst. Math. Sci.*, 33(3):393–425, 1997.

[Ros02] Michael Rosen. *Number Theory in Function Fields*. Springer, 2002.

[Yu95] Jiu-Kang Yu. Isogenies of Drinfeld modules over finite fields. *J. Number Theory*, 54(1):161–171, 1995.