Explicit Description Of Isogeny And Isomorphism Classes Of Drinfeld Modules Of Higher Rank Over Finite Fields.

A Thesis Submitted In Partial Fulfillment For The Requirements For The Academic Degree Doktor der Naturwissenschaften (Dr. rer. nat.)

Submitted in the Faculty of Mathematics and Natural Sciences of the University of Kassel

By

Sedric Nkotto Nkung Assong

Supervisor: Prof.Dr. Hans Georg Rück.

Date of Defence: July 1, 2020

"I herewith give assurance that I completed this dissertation independently without prohibited assistance of third parties or aids other than those identified in this dissertation. All passages that are drawn from published or unpublished writings, either word-for-word or in paraphrase, have been clearly identified as such. Third parties were not involved in the drafting of the content of this dissertation; most specifically, I did not employ the assistance of a dissertation advisor. No part of this thesis has been used in another doctoral or tenure process."

Dedication

To my late mum and the Atheu family.

Acknowledgments

I would like to thank the people without whom this work wouldn't have been achieved.

I am first all grateful to my supervisor Prof.Dr Hans-Georg Rück for his great patience and advise. I learnt a lot from you.

I also owe many thanks to the whole Institut of mathematics of the university of Kassel for the togetherness and the good times spent together.

I have a very special thank to Ines Kana Mebou for her love and all the emotional support. you have been there all the way along.

I am thankful to my family, brothers and sisters for the constant and unconditional support they have been providing.

I am especially grateful to my dad Atheu Denis and my mum Agni Odette for all the sacrifices, love and support. you are my heroes.

Special thanks to my friends Dominik Wulf, Daniel Tcheutia, Merlin Mouafo, Nathalie Wandji, Jean Daniel Djida.

Contents

Abstract/ Zusammenfassung / Résumé

Abstract

When jumping from the number fields theory to the function fields theory, one cannot miss the deep analogy between rank 1 Drinfeld modules and the group of root of unity and the analogy between rank 2 Drinfeld modules and elliptic curves. But so far, there is no known structure in number fields theory that is analogous to the Drinfeld modules of higher rank $r \geq 3$.
In this thesis we investigate the classes of those Drinfeld modules of higher rank $r \geq 3$. We describe the Weil polynomials defining the isogeny classes of rank r Drinfeld modules for any rank $r \geq 3$, which generalizes what Yu already did for $r = 2$. We also provide a necessary and sufficient condition for an order $\mathcal{O}$ in the endomorphism algebra corresponding to some isogeny classes, to be the endomorphism ring of a Drinfeld module. To complete the classification, we define the notion of fine isomorphy invariants for any rank r Drinfeld module and we prove that the fine isomorphy invariants together with the J-invariants describe the L-isomorphism classes of rank r Drinfeld modules defined over the finite field L.

Zusammenfassung

Während der Reise von der Zahlkörper-Theorie nach der Funktionenkörper-Theorie ist es fast unmöglich, dass man die Ähnlichkeit zwischen Drinfeld-Moduln von Rang 1 und die Gruppe der Einheitswurzeln nicht bemerkt und auch die Ähnlichkeit zwischen Drinfeld-Moduln von Rang 2 und elliptische Kurven. Aber bisher gibt es keine Struktur in der Zahlkörper-Theorie, die analog zu Drinfeld-Moduln von Rang $r \geq 3$ ist.
In dieser Doktorarbeit, untersuchen wir die Klassen dieser Drinfeld-Moduln von Rang $r \geq 3$. Wir beschreiben die Weil-Polynome, die Klassen der Isogenien von Drinfeld-Moduln von Rang $r \geq 3$ definieren. Es verallgemeinert die Arbeit, die Yu für $r = 2$ gemacht hat. Wir finden auch eine notwendige und hinreichende Bedingung, so dass eine Ordnung $\mathcal{O}$ in der Endomorphismen-Algebra von manchen Isogenien-Klassen ein Endomorphismus-Ring eines Drinfeld-Moduls ist.

Um die Klassifikation abzuschließen, definieren wir die Fine-Isomorphy-Invarianten für irgendeinen Drinfeld-Modul von Rang r und wir beweisen, dass die Fine-Isomorphy-Invarianten zusammen mit den J-Invarianten die L-Isomorphismus-Klassen der Drinfeld-Moduln von Rang r beschreiben, die über den endlichen Körper L definiert ist.

Résumé

En se baladant de la théorie des corps de nombres *à* la théorie des corps de fonctions, il est difficile de ne pas remarquer la ressemblance frappante qui existe entre les modules de Drinfeld de rang 1 et le group des racines de l'unité et celle qui existe entre les modules de Drinfeld de rang 2 et les courbes élliptiques. Malheureusement il n'existe pas pour le moment de structure de la theorie des corps de nombres analogue aux modules de Drinfeld de rang $r \geq 3$.
Dans ce travail, nous investiguons les classes de ces modules de Drinfeld de rang superieur $r \geq 3$. Nous décrivons les polynomes de Weil définissant les classes d'isogenies des modules de Drinfeld de rang $r \geq 3$. Ce qui généralise le travail déj*à* fait par Yu pour ceux de rang $r = 2$. Nous présentons aussi une condition nécessaire et suffisante pour qu'un ordre $\mathcal{O}$ de l'algèbre d'endomorphisme associée *à* certaines classes d'isogenies, soit l'anneau d'endomorphismes d'un module de Drinfeld donné. Pour compléter la classification, nous définissons la notion d'invariants fins d'isomorphisme associés *à* un module de Drinfeld de rang r et nous démontrons que les invariants fins d'isomorphisme associés aux J-invariants décrivent complètement les L-classes d'isomorphismes des modules de Drinfeld de rang r definis sur le corps fini L.

Introduction

At the beginning of the story (1974), Vladimir Drinfeld wanted to prove the Langlands conjectures for GL_2 over algebraic function fields. On his way to the solution, he came up with the notion of elliptic modules (nowadays called Drinfeld modules). His proof had been later on generalized by Laurent Lafforgue for GL_n (and he got the Fields Medal for that work).

The interest to Drinfeld modules has been increasing more and more because they happen to be useful in factorizing efficiently univariate polynomials over a finite field (Narayanan, 2015) and also are useful in coding theory.

Many attempts to apply Drinfeld modules in cryptography have also been made. This is the case for Gillard *et al.* (in [9], 2003), who proposed a cryptosystem based on Carlitz (rank 1 Drinfeld) modules. But S. Blackburn *et al.* proved later on (in [3]) that the proposed system is unsecured.

More recently, the so-called SIDH (standing for Supersingular Isogeny Diffie-Hellman), which is a cryptosystem based on isogeny graph of supersingular elliptic curves, has been proposed and entered in the very short list of good candidate for post-quantum cryptography because of its resistance to quantum attacks. But Joux and Narayanan proved (in [12], 2019) that the SIDH version of rank 2 Drinfeld modules is not secured.

If there is a common ground to all these attempts to apply Drinfeld modules theory, it is that most of the time only rank 1 and rank 2 Drinfeld modules are used. In fact,

Drinfeld modules of rank 1 are the function-field analogue of the group of roots of unity in number fields theory whereas Drinfeld modules of rank 2 are the function-field analogue of elliptic curves in number fields theory.

In addition, almost everything concerning the classification of rank 1 and rank 2 Drinfeld modules is known.

Yu explicitly described (in [26]) the isogeny classes of rank 2 Drinfeld modules over finite fields by giving the list of all the Weil polynomials (or Weil numbers) defining them. Knowing that the endomorphism algebra of a Drinfeld module is an isogeny invariant, Yu has also described all the orders in the endomorphism algebra corresponding to any isogeny class, occurring as endomorphism ring of a rank 2 Drinfeld module over a finite field in that isogeny class.

Gekeler has described (in [8], 2008) the L-isomorphism classes of rank 2 Drinfeld modules.

Concerning Drinfeld modules of higher rank $r \geq 3$, first of all there is no known analogue structure in number fields theory and very little is known about their classification (in the sense we mentioned before). That is,

1. The Weil polynomials (or Weil numbers) defining the isogeny classes of rank r ($r \geq 3$) Drinfeld modules.

2. The orders in the endomorphism algebra corresponding to a given isogeny class, occurring as endomorphism ring of a Drinfeld module in that isogeny class.

3. The description of the L-isomorphism classes in a given isogeny class of rank r Drinfeld modules defined over the finite field L.

We aim throughout this thesis, to answer those three questions following the below mentioned plan.

We first of all give in the first chapter some preliminaries necessary for our discussions.

In the second chapter, we describe the degree r polynomials defining the isogeny classes of rank r Drinfeld modules over a finite field L and we provide algorithms to check and list all those Weil polynomials.

In the third chapter, we focus on isogeny classes for which the corresponding endomorphism algebra is a field and we describe the orders in that function field, that occur as endomorphism ring of a Drinfeld module in our chosen isogeny class.

In the fourth chapter, we characterize for a Drinfeld module of rank r defined over a finite field L, its L-isomorphism class.

The fifth chapter is booked for the application to Drinfeld modules of rank 3 and rank 4. In this part, we compute given the maximal order of the corresponding (cubic or quartic) function field, all the orders that are endomorphism rings of a (rank 3 or rank 4) Drinfeld module in the chosen isogeny class. We also explain with a concrete example how the computation of the L-isomorphism classes in a fixed isogeny class is made.

CHAPTER 1

Preliminaries

1.1 Function fields

We do not prove the results in this part because all of them are very well known results in function fields theory and any interested reader can find detailed proofs in [22].

Definition 1.1. *An algebraic function field F/k of one variable over a field k is an extension $k \subseteq F$ such that F is a finite algebraic extension of $k(T)$ for some $T \in F$ which is transcendental over k.*

Example 1.1. *Let $k = \mathbb{F}_q$ be the finite field with $q = p^n$ elements (p a prime number). Any finite extension of $k(T) = \mathbb{F}_q(T)$ is an algebraic function field. The field $\mathbb{F}_q(T)$ itself is called the rational function field of one variable over $\mathbb{F}_q$.*

Definition 1.2. *A valuation ring of the function field F/k is a subring $\mathcal{O} \subseteq F$ such that $k \subseteq \mathcal{O} \subseteq F$ and for any $z \in F,\ z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

Example 1.2.

- *Let $P(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial.*

$$\mathcal{O}_1 = \left\{ \frac{f(T)}{g(T)} \mid f(T),\ g(T) \in \mathbb{F}_q[T] \text{ and } P(T) \nmid g(T) \right\}$$

is a valuation ring of the rational function field $\mathbb{F}_q(T)$.

- *The ring*

$$\mathcal{O}_2 = \left\{ \frac{f(T)}{g(T)} \mid f(T),\ g(T) \in \mathbb{F}_q[T] \text{ and } \deg f(T) \leq \deg g(T) \right\}$$

is also a valuation ring of the rational function field $\mathbb{F}_q(T)$.

Proposition 1.1. *Let $\mathcal{O}$ be a valuation ring of the function field F/k. Then*

- *$\mathcal{O}$ is a local ring. i.e. $\mathcal{O}$ has a unique maximal ideal $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^\times$, the set of non-units of $\mathcal{O}$.*
- *For any $0 \neq z \in F$, $z \in \mathfrak{p}$ if and only if $z^{-1} \notin \mathcal{O}$.*

Proposition 1.2. *Let $\mathcal{O}$ be a valuation ring of the function field F/k and let $\mathfrak{p}$ be the corresponding maximal ideal.*

- *$\mathfrak{p}$ is a principal ideal.*
- *Let t be a generator of $\mathfrak{p}$. For any $0 \neq z \in F$ there exists a unique integer $n \in \mathbb{Z}$ such that $z = t^n u$ with $u \in \mathcal{O}^\times$ a unit in $\mathcal{O}$.*
- *$\mathcal{O}$ is a principal ideal domain and if $\mathfrak{p} = t\mathcal{O}$ and $\{0\} \neq I \subseteq \mathcal{O}$ is a non-zero ideal, then $I = t^n\mathcal{O}$ for some $n \in \mathbb{N}$.*

Definition 1.3. *Any ring with the above mentioned properties is called a discrete valuation ring (DVR in short).*

Definition 1.4.

1. *A place $\mathfrak{p}$ of a function field F/k is the maximal ideal of some valuation ring $\mathcal{O}$ of F/k. Any element $t \in \mathfrak{p}$ such that $\mathfrak{p} = t\mathcal{O}$ is called a uniformizer (or uniformizing element or prime element) for $\mathfrak{p}$.*
2. *$\mathbb{P}_F$ denotes the set of all places of F/k.*

Remark 1.1. *If a place $\mathfrak{p} \in \mathbb{P}_F$ is given, the corresponding valuation ring is*

$$\mathcal{O} = \{z \in F \mid z^{-1} \notin \mathfrak{p}\}$$

Definition 1.5. *A discrete valuation of F/k is a map $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ with the following properties:*

1. *$v(z) = \infty \;\Leftrightarrow\; z = 0$*
2. *$v(z_1 z_2) = v(z_1) + v(z_2)$ for all $z_1,\ z_2 \in F$.*
3. *$v(z_1 + z_2) \geq \min\{v(z_1), v(z_2)\}$ for all $z_1,\ z_2 \in F$.*
4. *There exists an element $t \in F$ with $v(t) = 1$.*
5. *$v(a) = 0$ for all $a \in k$.*

Remark 1.2. *The inequality in* 3. *(sometimes called the ultrametric or strict triangular inequality) becomes an equality when $v(z_1) \neq v(z_2)$.*

Remark 1.3. *To a place $\mathfrak{p} \in \mathbb{P}_F$, we associate a map $v_\mathfrak{p} : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ such that*

$$v_\mathfrak{p}(0) = \infty \text{ and for } 0 \neq z \in F,\ v_\mathfrak{p}(z) = n$$

where n is the unique integer (as mentioned before) such that $z = t^n u$ with $u \in \mathcal{O}^\times$. $\mathcal{O}$ is the valuation ring associated to the place $\mathfrak{p}$ and t is the corresponding uniformizer. One easily checks that $v_\mathfrak{p}$ is a discrete valuation.

Proposition 1.3. *Let F/k be a function field.*

1. *Let $\mathfrak{p} \in \mathbb{P}_F$ and $v_\mathfrak{p}$ be the corresponding discrete valuation. We have the following:*
   $\mathcal{O} = \{z \in F \mid v_\mathfrak{p}(z) \geq 0\}$ is the corresponding valuation ring.
   $\mathcal{O}^\times = \{z \in F \mid v_\mathfrak{p}(z) = 0\}$ is the group of units of $\mathcal{O}$.
   $\mathfrak{p} = \{z \in F \mid v_\mathfrak{p}(z) > 0\}$ is the maximal ideal of $\mathcal{O}$.

2. *Conversely, if v is a discrete valuation defined on F/k, we have the following:*
   $\mathfrak{p}_v = \{z \in F \mid v(z) > 0\}$ is a place of F/k.
   $\mathcal{O}_v = \{z \in F \mid v(z) \geq 0\}$ is the corresponding valuation ring.

Remark 1.4. *We can therefore deduce from the previous proposition that a place of a function field F/k is entirely defined by giving either a valuation ring $\mathcal{O}$ of F/k, a maximal ideal of a valuation ring $\mathcal{O}$ of F/k or a discrete valuation v defined on F.*

Definition 1.6. *Let $\mathfrak{p}$ be a maximal ideal of a valuation ring $\mathcal{O}_\mathfrak{p}$ of the function field F/k.*

- $\mathbb{F}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ *is a field called the residue field associated to the place $\mathfrak{p}$.*

- *For $z \in \mathcal{O}_\mathfrak{p}$, $z(\mathfrak{p})$ denotes the residue class of z modulo $\mathfrak{p}$.*
  When $z \in \mathfrak{p}$ we have $z(\mathfrak{p}) = 0$. that is the reason why the place $\mathfrak{p}$ in this case is called a zero of the element z.
  When $z \in F \setminus \mathcal{O}_\mathfrak{p}$, $v_\mathfrak{p}(z) < 0$ and $\mathfrak{p}$ is called a pole of z.

- $\deg \mathfrak{p} = [\mathbb{F}_\mathfrak{p} : k]$ *is called the degree of the place $\mathfrak{p}$.*

1.2 Algebraic function fields extensions

Definition 1.7. *An algebraic function field F'/k' is called an algebraic extension of F/k if $F' \supseteq F$ is an algebraic field extension and $k' \supseteq k$.*
The extension is said to be finite if $[F' : F] < \infty$.

Definition 1.8. *We consider an algebraic extension F'/k' of F/k. A place $\mathfrak{p}' \in \mathbb{P}_{F'}$ is said to lie over the place $\mathfrak{p} \in \mathbb{P}_F$ if $\mathfrak{p} \subseteq \mathfrak{p}'$. We also say that $\mathfrak{p}'$ is an extension of $\mathfrak{p}$ or $\mathfrak{p}$ lies under $\mathfrak{p}'$ and we write $\mathfrak{p}' \mid \mathfrak{p}$.*

Proposition 1.4. *Let F'/k' be a function field extension of F/k. $\mathfrak{p} \in \mathbb{P}_F$ and $\mathfrak{p}' \in \mathbb{P}_{F'}$. $\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}_{\mathfrak{p}'}$ denote the corresponding discrete valuation rings. $v_\mathfrak{p}$ and $v_{\mathfrak{p}'}$ denote the corresponding discrete valuations. The followings are equivalent:*

1. $\mathfrak{p}' \mid \mathfrak{p}$.

2. $\mathcal{O}_\mathfrak{p} \subseteq \mathcal{O}_{\mathfrak{p}'}$.

3. *There exists an integer $e \geq 1$ such that $v_\mathfrak{p}(z) = ev_{\mathfrak{p}'}(z)$ for all $z \in F$. Moreover $\mathfrak{p} = \mathfrak{p}' \cap F$ and $\mathcal{O}_\mathfrak{p} = \mathcal{O}_{\mathfrak{p}'} \cap F$.*

Remark 1.5. *As a consequence of the previous proposition, if $\mathfrak{p}' \mid \mathfrak{p}$ then the residue field $\mathbb{F}_{\mathfrak{p}'} = \mathcal{O}_{\mathfrak{p}'}/\mathfrak{p}'$ is a field extension of the residue field $\mathbb{F}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$.*

Definition 1.9. *Let F'/k' be an algebraic extension of F/k, and let $\mathfrak{p}' \in \mathbb{P}_{F'}$ be a place of F'/k' lying over $\mathfrak{p} \in \mathbb{P}_F$.*

a) The integer $e\,(\mathfrak{p}' \mid \mathfrak{p}) := e$, with $v_\mathfrak{p}(z) = ev_{\mathfrak{p}'}(z)\ \forall z \in F$, is called the ramification index of $\mathfrak{p}'$ over $\mathfrak{p}$.
$\mathfrak{p}' \mid \mathfrak{p}$ is said to be ramified if $e\,(\mathfrak{p}' \mid \mathfrak{p}) > 1$ and unramified if $e\,(\mathfrak{p}' \mid \mathfrak{p}) = 1$.

b) $f\,(\mathfrak{p}' \mid \mathfrak{p}) := [\mathbb{F}_{\mathfrak{p}'} : \mathbb{F}_\mathfrak{p}]$ is called the relative (or residual) degree of $\mathfrak{p}'$ over $\mathfrak{p}$.

Remark 1.6.

- $e\,(\mathfrak{p}' \mid \mathfrak{p}) \in \mathbb{N}$.

- $f\,(\mathfrak{p}' \mid \mathfrak{p}) < \infty \;\Leftrightarrow\; [F' : F] < \infty$.

- *If F"$/k$" is an algebraic extension of F'/k' and $\mathfrak{p}$" is a place of F"$/k$" lying over $\mathfrak{p}'$ then*
  $e\,(\mathfrak{p}\text{"} \mid \mathfrak{p}) = e\,(\mathfrak{p}\text{"} \mid \mathfrak{p}') \cdot e\,(\mathfrak{p}' \mid \mathfrak{p})$.
  $f\,(\mathfrak{p}\text{"} \mid \mathfrak{p}) = f\,(\mathfrak{p}\text{"} \mid \mathfrak{p}') \cdot f\,(\mathfrak{p}' \mid \mathfrak{p})$.

Proposition 1.5. *Let F'/k' be an algebraic function field extension of F/k.*

a) For each place $\mathfrak{p}' \in \mathbb{P}_{F'}$, the exists exactly one place $\mathfrak{p} \in \mathbb{P}_F$ such that $\mathfrak{p}' \mid \mathfrak{p}$.

b) Conversely, every place $\mathfrak{p} \in \mathbb{P}_F$ has at least one (and at most finitely many) extension $\mathfrak{p}' \in \mathbb{P}_{F'}$.

Theorem 1.1 (Fundamental equality).
Let F'/k' be a finite algebraic function field extension of F/k. Let $\mathfrak{p} \in \mathbb{P}_F$ and $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ be all the places of F'/k' lying over $\mathfrak{p}$. Let $e_i = e(\mathfrak{p}_i \mid \mathfrak{p})$ be the ramification index and $f_i = f(\mathfrak{p}_i \mid \mathfrak{p})$ be the residual degree of $\mathfrak{p}_i \mid \mathfrak{p}$. We have then

$$\sum_{i=1}^{m} e_i f_i = [F' : F]$$

Remark 1.7. *Let $\mathfrak{p}$ be as in the previous theorem.*

a) $\mathfrak{p}$ is said to split completely in the extension F'/F if there are exactly $n = [F' : F]$ distinct places of F'/k' lying over $\mathfrak{p}$.

b) $\mathfrak{p}$ is said to be ramified if there exists $i \in \{1, \cdots, m\}$ such that $e_i > 1$. Otherwise $\mathfrak{p}$ is said to be unramified.

c) $\mathfrak{p}$ is said to be totally ramified if there is only one place $\mathfrak{p}' \in \mathbb{P}_{F'}$ lying over $\mathfrak{p}$ with ramification index $e(\mathfrak{p}' \mid \mathfrak{p}) = n = [F' : F]$.

1.3 Orders in function fields extensions

From now on we will be mostly working with algebraic function fields extensions of the rational function field $\mathbb{F}_q(T)$.
Let $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$. Let F be a finite field extension of k.

Definition 1.10. *An order $\mathcal{O}$ of F is a finitely generated A-submodule of F such that $\mathcal{O}$ is a subring of F and $\mathcal{O}$ spans F over k. That means $k \cdot \mathcal{O} = F$.*

Example 1.3. *Let π be an algebraic element over k which is also integral over A. We consider the function field extension $k(\pi)/k$. $\mathcal{O} = A[\pi]$ is an order of $k(\pi)$.*

Remark 1.8. *If an order $\mathcal{O}$ of F is not properly contained in any other order, then $\mathcal{O}$ is called a maximal order.*
An example of maximal order is the integral closure of A in F. In addition, this is the unique maximal order of the function field F. This maximal order is usually called the ring of integers of the function field F.
Arbitrary orders and maximal orders share some properties but also have differences. One of the main differences is that maximal orders are Dedekind domains. Which is not the case for arbitrary orders. That means, any proper

ideal of a maximal order factors uniquely (up to units) as a product of prime ideals. This is the main feature that allows to do arithmetic in maximal orders. We also recall that prime ideals in Dedekind domains are also maximal.

Definition 1.11 (Norm of an ideal)**.**
We consider again our function field F. Let $\mathcal{O}_{max}$ be the ring of integers of F. The norm $N_{F/k}(?)$ of ideals in $\mathcal{O}_{max}$ is defined as follows:

- *If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{max}$ lying above a prime ideal $\mathfrak{p}_0$ of A, then the norm $N_{F/k}(\mathfrak{p})$ is defined as*
$$N_{F/k}(\mathfrak{p}) = \mathfrak{p}_0^{\mathfrak{f}_0}$$
where $\mathfrak{f}_0$ is the residual degree of $\mathfrak{p} \mid \mathfrak{p}_0$.
- *If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals (not necessarily distinct) of $\mathcal{O}_{max}$ then*
$$N_{F/k}(\mathfrak{p}_1 \cdot \mathfrak{p}_2) = N_{F/k}(\mathfrak{p}_1) \cdot N_{F/k}(\mathfrak{p}_2)$$

Remark 1.9. *The unique prime factorization of ideals in the Dedekind domain $\mathcal{O}_{max}$ completes the definition above to that of the norm of any ideal I of $\mathcal{O}_{max}$.*

There is something that measures at which extend a given order $\mathcal{O}$ of a function field F is far from the maximal order $\mathcal{O}_{max}$ of F. It is called the conductor of $\mathcal{O}$ in $\mathcal{O}_{max}$ and it is defined as follows:

Definition 1.12. *Let $\mathfrak{c}_{\mathcal{O}}$ (or simply $\mathfrak{c}$ if there is no confusion on the order $\mathcal{O}$) denotes the conductor of an order $\mathcal{O}$ in the maximal order $\mathcal{O}_{max}$.*
$$\mathfrak{c} = \{x \in F \mid x\mathcal{O}_{max} \subseteq \mathcal{O}\}$$
$\mathfrak{c}$ is the largest ideal of $\mathcal{O}_{max}$ contained in $\mathcal{O}$.

Remark 1.10. *It is a very well known fact that*
$$disc(\mathcal{O}) = N_{F/k}(\mathfrak{c})\, disc(\mathcal{O}_{max})$$
Where disc(?) denotes the discriminant of an A-basis of the order in argument. Also if the discriminant of the order $\mathcal{O}$ is (up to a unit) the same as the discriminant of the maximal order, then the order $\mathcal{O}$ is also maximal. Thus $N_{F/k}(\mathfrak{c})$ can be used to measure to which extend $\mathcal{O}$ is far from $\mathcal{O}_{max}$.

We want now to talk about Drinfeld modules but before, let us discuss the notion of additive polynomials which is important in Drinfeld modules theory.

1.4 Additive polynomials

[10] is a good reference for all the results mentioned in this part.
Let L be a field with $p = char(L)$. $\overline{L}$ denotes an algebraic closure of L.

Definition 1.13. *A polynomial $P(x) \in L[x]$ is said to be additive if $P(x + y) = P(x) + P(y)$ as polynomial in x and y or equivalently if $\forall \alpha,\ \beta \in \overline{L},\ P(\alpha + \beta) = P(\alpha) + P(\beta)$.*

Example 1.4. *Some trivial examples are the polynomials $P(x) = ax,\ a \in L$ and $Q(x) = x^q$ for any $q = p^n,\ n \in \mathbb{N}$.*

Proposition 1.6. *Let $P(x),\ Q(x) \in L[x]$ be two additive polynomials over L.*

- *$P(x) + Q(x)$ is additive.*
- *$aP(x)$ is additive $\forall a \in L$.*
- *$P(Q(x))$ is additive.*

The proof follows straightforwardly from the definition.
The proposition above shows that the set $\mathcal{A}(L)$ of additive polynomials over L forms a ring under polynomials addition and composition.
From now on we denote τ_p the additive polynomial defined by $\tau_p(x) = x^p$. We denote $L\{\tau_p\}$ the subring of $\mathcal{A}(L)$ spanned by $\{\tau_p^i,\ i = 0, 1, 2, \cdots\}$
We recall that τ_p^0 is the additive polynomial defined by $\tau_p^0(x) = x$.
$L\{\tau_p\}$ is a non-commutative ring and one checks that $\forall \alpha \in L,\ \ \tau_p \cdot \alpha = \alpha^p \cdot \tau_p$.
It follows from the definition of additive polynomials that

Proposition 1.7. *$\mathcal{A}(L) = L\{\tau_p\}$.*

In general, one can also set $q = p^n,\ n \in \mathbb{N}$ such that $\mathbb{F}_q \subseteq L$. And consider then the ring $L\{\tau\}$ of $\mathbb{F}_q$-linear additive polynomials spanned by $\{\tau^i,\ i = 0, 1, 2, \cdots\}$. Where τ is the $\mathbb{F}_q$-linear additive polynomial defined by $\tau(x) = x^q$ and $\tau^0(x) = x$.
As a consequence, the ring $L\{\tau\}$ is an $\mathbb{F}_q$-algebra. Where $\tau \cdot \alpha = \alpha^q \cdot \tau\ \ \forall \alpha \in L$.
$L\{\tau\}$ is sometimes called the ring of Ore polynomials.

Proposition 1.8 (Fundamental theorem of additive polynomials)**.**
We assume that the field L is algebraically closed. Let $P(x) \in L[x]$ be a separable polynomial and $\Lambda = \{\lambda_1, \cdots, \lambda_m\} \subset L$ be the set of roots of $P(x)$. $P(x)$ is additive if and only if Λ is a subgroup of L.

Proof:[10, theorem 1.2.1] $\Diamond$

Corollary 1.1. *Let $P(x)$ be as in the previous proposition.*
$P(x)$ is $\mathbb{F}_q$-linear if and only if the set of roots Λ is an $\mathbb{F}_q$-vector subspace of L.

Proof:[10, Corollary 1.2.1] $\lozenge$

Remark 1.11. *A polynomial $f(\tau) \in L\{\tau\}$ is said to be separable if its constant coefficient is non-zero.*

1.5 Drinfeld modules

1.5.1 Definition and some properties

Let us now give the definition and some properties of Drinfeld modules.
Let $A = \mathbb{F}_q[T]$ be the ring of polynomials in the variable T over the finite field $\mathbb{F}_q$. Let L be an A-field. That is, a field equipped with an $\mathbb{F}_q$-algebras homomorphism $\gamma : A \longrightarrow L$. τ and $L\{\tau\}$ are as defined in the previous section.

Definition 1.14. *A Drinfeld module ϕ over L is an $\mathbb{F}_q$-algebra homomorphism $\phi : A \longrightarrow L\{\tau\}$ such that*

- *$\phi(A) \nsubseteq L$. In other word $\exists a \in A$ such that $\deg_\tau \phi(a) \geq 1$.*
- *$\forall a \in A, \;\; \phi(a) \equiv \gamma(a)\tau^0 \mod \tau$. In other words the constant coefficient (w.r.t τ) of $\phi(a)$ is $\gamma(a)\tau^0$.*

Remark 1.12. *Most of the time one omits τ^0 and simply write α instead of $\alpha\tau^0$ for any $\alpha \in L$. We also usually simply write ϕ_a instead of $\phi(a)$.*
Since $A = \mathbb{F}_q[T]$, ϕ is entirely defined by giving only the image ϕ_T of T.

Definition 1.15. *The rank of the Drinfeld module ϕ is defined as*
$r = rank\phi = \deg_\tau \phi_T$.

Example 1.5. *$A = \mathbb{F}_5[T], \;\; L = \mathbb{F}_5$ is an A-field defined by*
$\gamma : A \longrightarrow L, \; f(T) \longmapsto f(0)$.
$\phi_T = \tau^2 + \tau$ defines a rank 2 Drinfeld module.
$\psi_T = \tau$ defines a rank 1 Drinfeld module (usually called Carlitz module).

Remark 1.13. *Let $\phi : A \longrightarrow L\{\tau\}$ be a Drinfeld module.*

1. *The term “module” is due to the non-trivial A-module structure induced by the map ϕ on L as follows:*

$$\forall a \in A \text{ and } \alpha \in L, \quad a \cdot \alpha := \phi_a(\alpha)$$

2. *We denote $\phi[a] = \{\alpha \in \overline{L} \mid \phi_a(\alpha) = 0\}$ the group of a-torsion points. If I is an ideal of A, $\phi[I] := \bigcap_{a \in I} \phi[a] = \phi[b]$ where b is a generator of the ideal I of A.*

3. *The map ϕ is injective by definition.*

4. *The kernel of the $\mathbb{F}_q$-algebras homomorphism $\gamma : A \longrightarrow L$ defining the A-field L is called the A-characteristic of L (or the characteristic of the Drinfeld module ϕ).*
   When $Ker\gamma = \{0\}$, the Drinfeld modules over L are said to have generic characteristic. Otherwise the Drinfeld modules over L are said to have a special characteristic.
   For instance when L is finite, any Drinfeld module defined over L must have a special characteristic.

Since we will be dealing with Drinfeld module over a finite field L, let us assume from now on that L has a special A-characteristic we denote $\langle \mathfrak{p}_v \rangle = Ker\gamma$. We recall that $Ker\gamma$ is by definition a maximal ideal of A.
v will denote the valuation (or place) of A (or k) associated to that maximal ideal.

Definition 1.16. *Let $f(\tau) \in L\{\tau\}$.*
The weight of $f(\tau)$ denoted $wgt\,(f(\tau))$ is defined as the sub-degree of the polynomial $f(\tau)$. i.e. $f(\tau) = \alpha\tau^{wgt(f)} +$ monomials in τ of higher degrees . with $\alpha \neq 0$.

Proposition 1.9. *[10, lemma 4.5.6]*
There exists a positive integer h such that for all $a \in A$, $wgt\,(\phi_a) = hv(a)\deg \mathfrak{p}_v$. We recall that v denotes the valuation defined over k associated to the place $\mathfrak{p}_v$.

Remark 1.14. *For $a = \mathfrak{p}_v$ we have then $wgt\,(\phi_{\mathfrak{p}_v}) = h \deg \mathfrak{p}_v$.*
We take this opportunity to recall that since the ideal $\mathfrak{p}_v$ is principal in A, we will sometime abuse the language by keeping the same notation for the ideal and its generator. But at each time the reader could easily guess which one we will be talking about.

Definition 1.17. *The positive integer h is called the height of the Drinfeld module ϕ.*

Remark 1.15. *It is a well known fact that for any $a \in A$, if a is relatively prime to $\mathfrak{p}_v$ then $\phi[a] \simeq (A/aA)^r$. Otherwise $\phi[a] \simeq (A/aA)^{r-h}$. In particular $\phi[\mathfrak{p}_v] \simeq (A/\mathfrak{p}_v A)^{r-h}$. Where $r = rank\phi$ and h is the height of ϕ.*

1.5.2 Morphisms of Drinfeld modules

As it has always been the case in mathematics, each time one defines a new structure, one should also define the notion of morphism between two such structures in order to complete the definition of that category.

Definition 1.18. *Let ϕ and ψ be two Drinfeld modules over the A-field L. a morphism from ϕ to ψ is an element $f \in L\{\tau\}$ such that*

$$f \cdot \phi_a = \psi_a \cdot f \quad \forall a \in A$$

which is equivalent to $f \cdot \phi_T = \psi_T \cdot f$.

Remark 1.16.

- *One can straightforwardly see that f is an isomorphism if and only if $\deg_\tau f(\tau) = 0$.*
  When such an isomorphism exists, ϕ and ψ are said to be isomorphic or lie in the same isomorphism class (as equivalence relation).
- *A non-zero morphism is called an isogeny.*

Proposition 1.10. *Let ϕ and ψ be Drinfeld modules over the A-field L such that there exists an isogeny $f(\tau) \in L\{\tau\}$ from $\phi \longrightarrow \psi$. Then there exists also an isogeny $g \in L\{\tau\}$ from $\psi \longrightarrow \phi$ such that*

$$f \cdot g = \psi_a \text{ and } g \cdot f = \phi_a \text{ for some } a \in A.$$

Proof:[10, proposition 4.7.13] $\Diamond$

Remark 1.17.

1. *One clearly sees from the previous proposition that the isogeny relation is an equivalence relation.*
   ϕ and ψ are therefore said to be isogenous or lie in the same isogeny class (as equivalence relation).
2. *It is a well known fact that only Drinfeld modules with the same rank can be isogenous.*
   One easily sees it by comparing the degrees (in τ) of the polynomials involved in the equation $f \cdot \phi_T = \psi_T \cdot f$.

Remark 1.18. *Let $f(\tau) : \phi \longrightarrow \psi$ be an isogeny and $H = Spec\left(L[x]/\langle f(x)\rangle\right)$ be the so-called scheme-theoretic kernel of f.*
The Drinfeld module ψ is called the quotient Drinfeld module of ϕ by H and it is denoted $\psi = \phi/H$. In other words, given a Drinfeld module ϕ, an isogenous Drinfeld module ψ is entirely defined by giving the corresponding scheme-theoretic kernel.
The following result provide a necessary and sufficient condition for a group scheme H to be a scheme-theoretic kernel of an isogeny.

Proposition 1.11. *[10, proposition 4.7.11]*
Let ϕ be a fixed Drinfeld module of rank r over the finite A-field L. Let $H \subseteq \mathbb{G}_a/L = Spec(L[x])$ be a finite affine subgroup scheme. We have the following:
H is the scheme theoretic kernel of an isogeny $f : \phi \longrightarrow \psi$ if and only if H is invariant under the action of A (via ϕ) and the local (or connected) part H_{loc} of the group scheme H is of the form

$$H_{loc} = Spec\left(L[x]/\langle x^{q^{t \deg \mathfrak{p}_v}}\rangle\right) \quad \textit{for some integer } t \geq 0$$

Corollary 1.2. *Any étale affine subgroup scheme $H \subseteq \mathbb{G}_a/L = Spec(L[x])$ which is A-invariant (via ϕ) is the scheme-theoretic kernel of an isogeny f from ϕ to another Drinfeld module $\psi := \phi/H$.*

Proof: This corollary follows from the fact that in such a case the local part H_{loc} of H is trivial and we have then

$$H_{loc} = \{0\} = Spec(L) = Spec\left(L[x]/\langle x\rangle\right) = Spec\left(L[x]/\langle x^{q^{0 \cdot \deg \mathfrak{p}_v}}\rangle\right)$$

One applies then the previous proposition with $t = 0$. ◊

Remark 1.19. *The former proposition basically says (as shown in [23, proposition 2.5]) that*
H is given as the kernel of an additive polynomial $f \in L\{\tau\}$ and
f is an isogeny if and only if
H is A-invariant (via ϕ) and height$(f) \equiv 0 \mod \deg \mathfrak{p}_v$.

Definition 1.19. *An isogeny f from a Drinfeld module ϕ to itself is called an endomorphism.*

Remark 1.20. *The set of endomorphism of ϕ over L together with the zero morphism form a ring denoted $End_L\phi$ (or simply $End\phi$ if there is no confusion on the field L) and it is called the endomorphism ring of ϕ.*

Proposition 1.12. *Let ϕ and ψ be two Drinfeld modules.*
If ϕ and ψ are isogenous then

- *The endomorphism k-algebras $End\phi \otimes_A k$ and $End\psi \otimes_A k$ are isomorphic. In other words the endomorphism k-algebra is an isogeny invariant.*
- *$End\phi$ and $End\psi$ have the same rank over A.*

Theorem 1.2. *Let ϕ be a Drinfeld module over a finite A-field L*
and $s = [L : \mathbb{F}_q]$.
There is a special endomorphism of ϕ defined by $\pi = \tau^s$. This endomorphism is called the Frobenius endomorphism of ϕ.
The following are known facts (see [26]):

- *π is an algebraic integer and the function field $k(\pi)$ is the center of the k-algebra $End\phi \otimes_A k$.*
- *$r = rank\phi = [k(\pi) : k]\sqrt{rank_{k(\pi)} End\phi \otimes_A k}$.*

For the special case when $End\phi \otimes_A k$ is a field, we have
$r = rank\phi = [k(\pi) : \; k]$ and $End\phi$ is an A-order in the function field $k(\pi)$.

CHAPTER 2

Isogeny classes of rank r Drinfeld modules

The aim of this part is to describe in detail and provide a complete list of rank r Weil numbers for a fixed positive integer r. The description of rank 2 Weil numbers has already been done by Yu in [26]. We want to extend it to higher ranks. Before starting let us fix some notations. Throughout this part, we denote $A = \mathbb{F}_q[T]$ the ring of polynomial in T over a finite field $\mathbb{F}_q$. L is a finite A-field defined by an $\mathbb{F}_q$-algebras homomorphism $\gamma : A \longrightarrow L$. $\mathfrak{p}_v = Ker(\gamma)$ and $m = \left[L : {}^{A}\!/_{\mathfrak{p}_v}\right]$. $k = \mathbb{F}_q(T)$ denotes the fraction field of A and $Q(T)$ is the monic generator of the principal ideal $\mathfrak{p}_v^m$ i.e. $\mathfrak{p}_v^m = \langle Q \rangle = Q(T) \cdot A$.

2.1 Definitions and potential Weil polynomials

Let us first define what a Weil number is.

Definition 2.1. *[26] Weil numbers]*
An element $\pi \in \overline{k}$ is called a degree r Weil number over a finite A-field L if the following conditions hold.

(c1) π is integral over A.

(c2) There is only one place of $k(\pi)$ which is a zero of π and this place lies above the A-characteristic v of L.

(c3) There is only one place of $k(\pi)$ lying over the place ∞ of k.

(c4) $|\pi|_\infty = l^{1/r}$ where $l = |L|$ and $|.|_\infty$ is the unique extension to $k(\pi)$ of the normalized absolute value of k corresponding to the place ∞.

(c5) $[k(\pi) : k]$ divides r

Remark 2.1. *We recall that the place at* ∞ *in* k *is defined via the valuation* $v_\infty : k \longrightarrow \mathbb{Z} \cup \{\infty\}$ *such that*
$v_\infty\left(\frac{f(T)}{g(T)}\right) = \deg g(T) - \deg f(T)$ *for* $0 \neq \frac{f(T)}{g(T)} \in k$ *and* $v_\infty(0) = \infty$.
That means concerning condition $(c4)$ *of definition 2.1 that the place at* ∞ *in* k *is normalized in such a way that the absolute value of the uniformizer* $\frac{1}{T}$ *is* $\left|\frac{1}{T}\right|_\infty = q^{-1}$. *This absolute value is then extended to* $k(\pi)$ *using the unique extension (for which we keep the same notation unless otherwise mentioned)* ∞ *in* $k(\pi)$.

Definition 2.2. *[Weil polynomial]*
We will call throughout this part Weil polynomial, the minimal polynomial over the field k *of a Weil number.*

Remark 2.2. *From now on, we denote by* $M(x)$ *the minimal polynomial associated to the algebraic number* π. *We set* $r_1 = [k(\pi) : k]$ *the degree of* $M(x)$. *The condition* $(c5)$ *of definition 2.1 imposes that* r_1 *divides* r. *So we also set* $r_2 = \frac{r}{r_1}$ *i.e.* $r = r_1 \cdot r_2$.

Now let us take a Weil number π and the corresponding Weil polynomial $M(x)$. We want to investigate how $M(x)$ looks like, having in mind all the required conditions provided by the above mentioned definition 2.1.
The first condition $(c1)$ is that π is integral over A. Therefore the minimal polynomial is of the form

$$M(x) = x^{r_1} + a_1 x^{r_1 - 1} + \cdots + a_{r_1 - 1}x + a_{r_1} \in A[x].$$

Also $a_{r_1} = M(0) = (-1)^{r_1} N_{k(\pi)/k}(\pi)$. But π has a unique zero in $k(\pi)$ which lies over $\mathfrak{p}_v$ according to the condition $(c2)$. Thus $\mathfrak{p}_v$ is the unique prime of A dividing a_{r_1}. That is

$$a_{r_1} = \mu \mathfrak{p}_v^\alpha \qquad (\star)$$

where $\alpha \in \mathbb{N}$, $\mu \in \mathbb{F}_q^*$
Moreover, we know from condition $(c4)$ that $|\pi|_\infty = l^{1/r} = q^{\frac{m \deg \mathfrak{p}_v}{r}}$. That means $v_\infty(\pi) = v_\infty(\pi_i) = -\frac{m \cdot \deg \mathfrak{p}_v}{r}$ $\forall i$, where $\pi_{i's}$ denote the roots of $M(x)$.
We also know that $a_{r_1} = (-1)^{r_1} \prod_{i=1}^{r_1} \pi_i$. Hence $v_\infty(a_{r_1}) = r_1 v_\infty(\pi) = -\frac{m \cdot \deg \mathfrak{p}_v}{r_2}$.
From $(\star)$ we have $-\alpha \deg \mathfrak{p}_v = v_\infty(a_{r_1}) = -\frac{m \cdot \deg \mathfrak{p}_v}{r_2}$ and therefore $\mathbb{N} \ni \alpha = \frac{m}{r_2}$.

$$\text{Thus } r_2 \mid m \text{ and } a_{r_1} = \mu \mathfrak{p}_v^{\frac{m}{r_2}} = \mu Q^{\frac{1}{r_2}}$$

where $Q = \mathfrak{p}_v^m$ is the monic generator of the ideal $\mathfrak{p}_v^m$. Therefore

$$M(x) = x^{r_1} + a_1 x^{r_1 - 1} + \cdots + a_{r_1 - 1} x + \mu Q^{\frac{1}{r_2}} \in A[x],\ \mu \in \mathbb{F}_q^*.$$

Let us consider again the roots $\pi_1, \cdots, \pi_{r_1}$ of $M(x)$ in $\overline{k}$. One knows that $a_n = (-1)^n \sum\limits_{i_1, \cdots, i_n} \pi_{i_1} \pi_{i_2} \cdots \pi_{i_n}$. That is

$$v_\infty(a_n) = v_\infty\left(\sum_{i_1, \cdots, i_n} \pi_{i_1}\pi_{i_2}\cdots\pi_{i_n}\right) \geq \min_{i_1, \cdots, i_n}\left\{v_\infty(\pi_{i_1}\pi_{i_2}\cdots\pi_{i_n})\right\}$$

But

$$\min_{i_1, \cdots, i_n}\left\{v_\infty(\pi_{i_1}\pi_{i_2}\cdots\pi_{i_n})\right\} = v_\infty(\pi_{j_1}\pi_{j_2}\cdots\pi_{j_n}) = v_\infty(\pi_{j_1}) + v_\infty(\pi_{j_2}) + \cdots + v_\infty(\pi_{j_n})$$

for some $(j_1, \cdots, j_n)$

Again as we mentioned before, one draws from condition $(c4)$ that $v_\infty(\pi_{j_1}) = v_\infty(\pi_{j_2}) = \cdots = v_\infty(\pi_{j_n}) = v_\infty(\pi) = -\frac{m \deg \mathfrak{p}_v}{r} = -\frac{\deg Q}{r}$.
Hence $v_\infty(a_n) \geq v_\infty(\pi_{j_1}) + v_\infty(\pi_{j_2}) + \cdots + v_\infty(\pi_{j_n}) = n \cdot v_\infty(\pi) = -\frac{n \cdot \deg Q}{r}$.
Thus $-\deg a_n \geq -\frac{n \cdot \deg Q}{r}$ that is

$$\deg a_n \leq \frac{n \cdot \deg Q}{r}.$$

Therefore the coefficients a_i of $M(x)$ satisfy the boundary condition

$$\deg a_i \leq \frac{i \cdot \deg Q}{r} = \frac{i \cdot \deg Q^{\frac{1}{r_2}}}{r_1}$$

.

Remark 2.3. *As conclusion of our above discussion, we will be working from now on with polynomials of the form*

$$M(x) = x^{r_1} + a_1 x^{r_1 - 1} + \cdots + a_{r_1 - 1} x + \mu Q^{1/r_2} \in A[x]$$

such that $r_2 \mid m$ *and* $\deg a_i \leq \frac{i \cdot \deg Q^{1/r_2}}{r_1}$.

Lemma 2.1. *Let Q be a given monic polynomial in $A = \mathbb{F}_q[T]$ whose degree is a multiple of a positive integer r with $gcd(r, q) = 1$. Then Q is an r^{th} power in k_∞ where $k = \mathbb{F}_q(T)$.*

Proof: $v_\infty\left(\frac{Q}{T^{\deg Q}}\right) = 0$. Thus $\frac{Q}{T^{\deg Q}} \in \mathcal{O}_\infty$. where $\mathcal{O}_\infty$ denotes the valuation ring associated to the place ∞. Q is a monic polynomial. Therefore,

$\frac{Q}{T^{\deg Q}} \equiv 1 \mod \left(\frac{1}{T}.\mathcal{O}_\infty\right)$. We consider the polynomial $f(Y) = Y^r - \frac{Q}{T^{\deg Q}}$. Since $f(1) = 1 - \frac{Q}{T^{\deg Q}} \equiv 0 \mod \left(\frac{1}{T}.\mathcal{O}_\infty\right)$, $f'(1) = r.1 \equiv r.1 \mod \left(\frac{1}{T}.\mathcal{O}_\infty\right)$ and $\gcd(r, char(k)) = 1$ that is $r.1 \neq 0$. We can apply the Hensel lemma and conclude that $\frac{Q}{T^{\deg Q}}$ is an r-th power in $\mathcal{O}_\infty$. Since $\deg Q$ is a multiple of r, Q is also an r-th power in k_∞. ◊

Remark 2.4. *[Some assumptions]*
Before moving forward, let us make two major assumptions. From now till otherwise mention,

A1 we assume that r is a prime number. That is
$r_1 = r,\ r_2 = 1$ and therefore $M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q$
or $r_1 = 1,\ r_2 = r$ and therefore $M(x) = x + \mu Q^{1/r}$

A2 we also consider r to be coprime with the characteristic $char(k)$. $gcd(r, char(k)) = 1$. This assumption is made so that the minimal polynomial $M(x)$ is separable.

We will later on generalize our results by getting rid of those assumptions one after the other. The assumption A1 on the primality of r will be dropped first and we will therefore list all the "separable" Weil polynomials. After then we will drop also the assumption A2 about the separability and show how one can without loss of generality assume that $M(x)$ is separable.

Proposition 2.1. *Let $\pi \in \overline{k}$ be a Weil number and $M(x)$ be its the minimal polynomial over k which is (as we mentioned in remark 2.4) of the form*

$$M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q \text{ or } M(x) = x + \mu Q^{1/r}.$$

Since π satisfies the condition (c3) of definition 2.1, $M(x)$ must have one of the below mentioned forms.

1. *$M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q$ such that the polynomial $M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$ is irreducible in $k_\infty[x]$. Where $s = \left\lceil\frac{m \deg \mathfrak{p}_v}{r}\right\rceil = \left\lceil\frac{\deg Q}{r}\right\rceil = \left\lceil\frac{\deg Q^{1/r_2}}{r_1}\right\rceil$.*

2. *$M(x) = x + \mu Q^{1/r}$ with $r \mid m$ and $\mu \in \mathbb{F}_q^*$*

Proof: First of all one can clearly notice from remark 2.3 that $\deg a_i \leq is\ \ \forall i$. That means the polynomial $M_0(x) \in \mathcal{O}_\infty[x]$.
$M(x)$ has just two possible forms as consequence of the assumption $A1$ of remark 2.4.

If $M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + \mu Q$ then the minimal polynomial of $\frac{\pi}{T^s}$ is $M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$.
If $M(x) = x + \mu Q^{1/r}$ then the minimal polynomial of $\frac{\pi}{T^s}$ is $M_0(x) = x - \mu\frac{Q^{1/r}}{T^s}$.
In addition $k(\pi) = k(\frac{\pi}{T^s})$.
We also know that there is a unique extension of the place at ∞ in $k(\pi)$ if and only if $M_0(x)$ is irreducible over the completion k_∞ or $M_0(x)$ is a power of an irreducible polynomial over k_∞ (see [18, proposition 8.2, page 163]).
For the first case, $\deg M_0(x)$ is a prime number. So $M_0(x)$ must be irreducible since it cannot be a power of a polynomial of degree ≥ 2.
For the second case, $M_0(x) = x - \mu\frac{Q^{1/r}}{T^s}$ is a degree 1 polynomial and therefore already irreducible. Also, $\pi \in k$, π is integral over A and A is integrally closed. Thus $\pi \in A$. $\pi^r = \alpha Q$ for some $\alpha \in \mathbb{F}_q$. $Q = \mathfrak{p}_v^m$. In addition $\mathfrak{p}_v$ is a prime element in the UFD A. Thus $\mathfrak{p}_v$ is the unique prime element dividing π. That is $\pi = \beta \cdot \mathfrak{p}_v^n$ for some $n \in \mathbb{N}$ and $\beta \in \mathbb{F}_q$. Hence $\beta^r \cdot \mathfrak{p}_v^{nr} = \alpha \cdot \mathfrak{p}_v^m$. i.e. $nr = m$ and then $r \mid m$.
Therefore we have the expected result. $\diamondsuit$

Remark 2.5. *A natural question one can ask after a look at our proposition 2.1 above is how one can actually check that*

$$M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$$

is irreducible over the completion field k_∞. Before answering that question, let us remind for the convenience of the reader the following well known fact in algebraic number theory.
Let k be a global field, $M(x) \in k[x]$ be an irreducible polynomial over k with integer coefficients (i.e. the coefficients of $M(x)$ lie in the ring of integers of k) and v a given place of k. Let $n \in \mathbb{N}$ with $n > v(discriminant(M(x)))$. As a direct consequence of the Hensel lemma, the irreducible decomposition $M(x) = \bar{f}_1(x)\cdots\bar{f}_s(x) \mod \mathfrak{p}_v^n$ completely encodes the irreducible decomposition $M(x) = f_1(x)\cdots f_s(x) \in k_v[x]$ of $M(x)$ over the completion field k_v (see [4, III.4.3, theorem 1] or [1, theorem 7.3]).

Here is therefore an answer for the above mentioned question.

Proposition 2.2. *Let $h = v_\infty(disc(M_0(x))) + 1$.*
$M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$ is irreducible in $k_\infty[x]$ if and only if $M_0(x) \mod \frac{1}{T^h}\mathcal{O}_\infty$ is irreducible.

Proof: The proof follows from remark 2.5. $\diamondsuit$

Remark 2.6.

- *One can notice that $M_0(x)$ is defined over $\mathbb{F}_q\left[\frac{1}{T}\right]$. So checking the irreducibility of $M_0(x) \mod \frac{1}{T^h}\mathcal{O}_\infty$ is equivalent to checking the one of $M_0(x) \mod \frac{1}{T^h}\mathbb{F}_q\left[\frac{1}{T}\right]$. Since ${}^{\mathbb{F}_q\left[\frac{1}{T}\right]}\!\big/_{\frac{1}{T^h}\mathbb{F}_q\left[\frac{1}{T}\right]} \cong {}^{A}\!\big/_{T^h A}$ is finite, one can then check (using proposition 2.2) in finitely many steps, whether $M_0(x)$ is irreducible over k_∞ or not.*

- *One can also compute $h = v_\infty\left(disc\left(M_0(x)\right)\right) + 1$ directly from $M(x)$ by noticing that $disc\left(M_0(x)\right) = \frac{1}{T^{sr(r-1)}} disc\left(M(x)\right)$.*
  Therefore $h = v_\infty\left(disc\left(M(x)\right)\right) + sr(r-1) + 1$.

After our investigation, we can say so far that any element $\pi \in \overline{k}$ which is a degree r Weil number (r prime) must have a minimal polynomial of one of the below mentioned forms.

(1) $x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q$ such that $\deg a_i \leq \frac{i \deg Q}{r}$ and the polynomial $M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$ is irreducible in $k_\infty[x]$ where $s = \lceil\frac{\deg Q}{r}\rceil$.

(2) $x - \mu Q^{\frac{1}{r}}$ with $r \mid m$ and $\mu \in \mathbb{F}_q$

Conversely, let us pick π a root of the polynomials (1) or (2). We want to check whether π is a Weil number. Let us have a look at each condition from ($c1$) to ($c5$).

- The condition ($c1$) is obvious in both cases since the polynomials (1) and (2) are in $A[x]$

- The condition ($c3$) follows from the definition of those polynomials. For the polynomial (1), we clearly have the condition that it is irreducible over the completion k_∞ of k at the place ∞.
  For the polynomial (2), it is irreducible over k_∞ as degree 1 polynomial.

- Concerning the condition ($c4$), one can just notice that
$$N_{k(\pi)/k}\left(\pi\right) = \begin{cases} (-1)^r\mu Q & \text{for polynomials of the form} \\ & x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q \\ \mu Q^{1/r} & \text{for polynomials of the second form } x - \mu Q^{1/r} \end{cases}$$
  To avoid any ambiguity, let us denote ∞' the place in $k(\pi)$ above ∞ in k. $v_{\infty'}\left(\pi\right) := \frac{1}{[k(\pi):k]}v_\infty\left(N_{k(\pi)/k}\left(\pi\right)\right) = -\frac{1}{r}\deg Q$ (in both cases).
  Therefore $|\pi|_{\infty'} = q^{-v_{\infty'}(\pi)} = q^{\frac{1}{r}\deg Q} = l^{1/r}$.

- The condition ($c5$) is also straightforward since
$$[K(\pi):K]=\begin{cases} r & \text{for polynomials of the form} \\ & x^r+a_1x^{r-1}+\cdots+a_{r-1}x+\mu Q \\ 1 & \text{for polynomials of the second form } x-\mu Q^{1/r}\end{cases}$$
In any case $[K(\pi):K]$ divides r.

- The condition ($c2$) is also fulfil for the polynomial (2) because there is (in this case) a unique prime above $\mathfrak{p}_v$ in $k(\pi)$ and A fortiori a unique zero of π above $\mathfrak{p}_v$.

Therefore the only missing condition is the condition ($c2$) for the polynomials of the first form (1).
Let us then investigate the places above $\mathfrak{p}_v$. π denotes here a root of a polynomial of the first form (1). It is a trivial fact from the properties of the polynomial (1) that π has at least one zero in $k(\pi)$ and any zero $\mathfrak{p}_\pi$ of π lies above $\mathfrak{p}_v$.

Proposition 2.3. *Let $n=v\,(disc\,(M(x)))+1$. Where*
$M(x)=x^r+a_1x^{r-1}+\cdots+a_{r-1}x+\mu Q$ is a polynomial of the first form (1). $M(x)=f_1(x)\cdot f_2(x)\cdots f_s(x)$ (for some $s\in\mathbb{N}$) is the irreducible decomposition of $M(x)$ over the completion k_v of k at the place $\mathfrak{p}_v$ if and only if $\overline{M}(x)=\overline{f_1}(x)\cdot\overline{f_2}(x)\cdots\overline{f_s}(x)$ is an irreducible decomposition of
$\overline{M}(x)=M(x) \mod \mathfrak{p}_v^n$. Where $f_j(x)$ is the lifting of $\overline{f_j}(x)$ in $k_v[x]$ i.e. $\overline{f_j}(x)=f_j(x) \mod \mathfrak{p}_v^n$.

Proof: Direct consequence of Hensel lemma as mentioned in remark 2.5.

$\diamondsuit$

Remark 2.7. *Let us remind some other well known facts in algebraic number theory.*

- *If $\mathfrak{p}$ is a place of k and $M(x)$ is the minimal polynomial over k of a given $\pi\in\overline{k}$, and if $M(x)=\bar{f}_1(x)\cdots\bar{f}_s(x) \mod \mathfrak{p}^n$ is an irreducible decomposition of $M(x) \mod \mathfrak{p}^n$ (with n as in remark 2.5) then $\mathfrak{p}=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s}$ in $k(\pi)$. If $\mathfrak{f}_i$ denotes the residual degree of $\mathfrak{p}_i|\mathfrak{p}$ then we have in addition, $e_i\mathfrak{f}_i=\deg\bar{f}_i(x)$. (see [13, theorem 2.C]). Each $\mathfrak{p}_i$ is described by the polynomial $f_i(x)$ through the valuation v_i defined by $v_i=\bar{v}\circ\tau_i$ with $\bar{v}$ the unique extension of v to $\overline{k}_v$ and*
$$\begin{array}{rcl}\tau_i:k(\pi) & \longrightarrow & \overline{k}_v \\ \pi & \longmapsto & \pi_i\end{array}$$
for some root π_i of $f_i(x)$.

- *One can also wonder why we consider the irreducible decomposition of $M(x)$ to be of the form $M(x) = f_1(x) \cdot f_2(x) \cdots f_s(x)$ instead of $M(x) = f_1(x)^{m_1} \cdot f_2(x)^{m_2} \cdots f_s(x)^{m_s}$ with $m_i \geq 1$. This is due to the simple reason that $M(x)$ has been assumed to be separable. We will come back later on to case where $M(x)$ is not separable.*

Proposition 2.4. *As before $M(x) = f_1(x) \cdot f_2(x) \cdots f_s(x)$ is the irreducible decomposition of $M(x)$ over k_v. If $f_{i_0}(x)$ describes a zero $\mathfrak{p}_{i_0}$ of π in $k(\pi)$, then π has a unique zero in $k(\pi)$ if and only if $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \mod \mathfrak{p}_v \neq 0$. $Res(?,?)$ denotes the resultant function.*

Proof: Let us assume that π has a unique zero $\mathfrak{p}_{i_0}$ in $k(\pi)$ described by the factor $f_{i_0}(x)$. If $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \equiv 0 \mod \mathfrak{p}_v$ then we have the following:
We recall that $\mathfrak{p}_v$ can be seen here as the unique place of the completion field k_v.
$\mathfrak{p}_v \mid Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right)$ i.e. $\mathfrak{p}_v \mid Res\left(f_{i_0}(x), f_j(x)\right)$ for some $j \in \{1, \cdots, s\}$ $j \neq i_0$. That means $\mathfrak{p}_i \mid Res\left(f_{i_0}(x), f_j(x)\right)$ for all $i = 1, \cdots, s$.
Where $\mathfrak{p}_v = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$ is the prime decomposition of $\mathfrak{p}_v$ in $k(\pi)$.
$\mathfrak{p}_i$ can be seen as the unique extension of $\mathfrak{p}_v$ in the completion field $(k(\pi))_{\mathfrak{p}_i} \simeq k_v(\pi_i)$. Where π_i is a root of the irreducible factor $f_i(x) \in k_v[x]$ of $M(x)$ defining the place $\mathfrak{p}_i$.
In particular $\mathfrak{p}_{i_0}$ divides $Res\left(f_{i_0}(x), f_j(x)\right)$.
Let $\tilde{\mathfrak{p}}_{i_0}$ be a prime of F above $\mathfrak{p}_{i_0}$. $F = Gal\left(k(\pi)\right)$ denotes the Galois closure of $k(\pi)$ (i.e. the splitting field of $M(x)$).
$\mathfrak{p}_{i_0} \mid Res\left(f_{i_0}(x), f_j(x)\right)$ implies that $\tilde{\mathfrak{p}}_{i_0} \mid Res\left(f_{i_0}(x), f_j(x)\right)$. In other words $\tilde{\mathfrak{p}}_{i_0}$ divides $\pi_{i_0} - \pi_j$ for some root π_{i_0} of $f_{i_0}(x)$ and π_j of $f_j(x)$.
$\tilde{\mathfrak{p}}_{i_0}$ divides π. π and π_{i_0} are both, roots of $f_{i_0}(x)$. The corresponding valuation v_{i_0} is defined by $v_{i_0} = \overline{v} \circ \tau_0$ with

$$\begin{array}{rcl} \tau_0 : k(\pi) & \hookrightarrow & \overline{k_v} \\ \pi & \longmapsto & \pi_{i_0} \end{array}$$

$\overline{v}$ is the valuation defined over $\overline{k_v}$ (extending v).
By definition, $\mathfrak{p}_{i_0}$ divides π i.e. $v_{i_0}(\pi) > 0$. In addition, $\pi = \sigma(\pi_{i_0})$ for some $\sigma \in Gal(F/k)$. That is $v_{i_0} \circ \sigma(\pi_{i_0}) > 0$.
But $v_{i_0} \circ \sigma$ and v_{i_0} define the same place of $k(\pi)$ because π and π_{i_0} are roots of the same irreducible factor $f_{i_0}(x)$. Thus $\tilde{\mathfrak{p}}_{i_0}$ divides π_{i_0}.
$\tilde{\mathfrak{p}}_{i_0}$ divides $\pi_{i_0} - \pi_j$ and $\tilde{\mathfrak{p}}_{i_0}$ divides π_{i_0} implies that $\tilde{\mathfrak{p}}_{i_0}$ divides π_j.
But $\pi_j = \sigma_j(\pi)$ for some $\sigma_j \in Gal(F/k)$. That means $\tilde{\mathfrak{p}}_{i_0} \mid \pi_j$ i.e. $\tilde{\mathfrak{p}}_{i_0} \mid \sigma_j(\pi)$. In other word $\sigma_j^{-1}\left(\tilde{\mathfrak{p}}_{i_0}\right) \mid \pi$.
$\sigma_j^{-1}\left(\tilde{\mathfrak{p}}_{i_0}\right)$ is a place of F above the place $\mathfrak{p}_j$ of $k(\pi)$ defined by $f_j(x)$.

We have then $\pi \in \sigma_j^{-1}(\tilde{\mathfrak{p}}_{i_0}) \cap k(\pi) = \mathfrak{p}_j$.
Therefore π possesses at least two zeros and it contradicts our initial hypothesis.
Let us assume conversely that $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \mod \mathfrak{p}_v \neq 0$.
If there are more than a zero of π above $\mathfrak{p}_v$ in $k(\pi)$, then we have the following:
$M(x) = f_1(x) \cdots f_s(x) \in k_v[x]$. Suppose that $f_{i_0}(x)$ and $f_{i_1}(x)$ describe zeros of π above $\mathfrak{p}_v$ in $k(\pi)$. Let $\tilde{\mathfrak{p}}_{i_0}$ and $\tilde{\mathfrak{p}}_{i_1}$ be primes of F above $\mathfrak{p}_{i_0}$ and $\mathfrak{p}_{i_1}$ respectively. There exists $\sigma \in Gal(F/k)$ such that $\tilde{\mathfrak{p}}_{i_1} = \sigma(\tilde{\mathfrak{p}}_{i_0})$. Since $\tilde{\mathfrak{p}}_{i_0}$ and $\tilde{\mathfrak{p}}_{i_1}$ both divide π we have $\sigma(\tilde{\mathfrak{p}}_{i_0})$ divides π and $\tilde{\mathfrak{p}}_{i_0}$ divides π. That is, $\tilde{\mathfrak{p}}_{i_0}$ divides $\sigma^{-1}(\pi)$ and $\tilde{\mathfrak{p}}_{i_0}$ divides π.
$\sigma^{-1}(\pi)$ is a conjugate of π which is not a root of $f_{i_0}(x)$. Otherwise it would describe the same place of $k(\pi)$. Which is not the case since $\tilde{\mathfrak{p}}_{i_0}$ and $\tilde{\mathfrak{p}}_{i_1}$ are primes of F above two distinct primes $\mathfrak{p}_{i_0}$ and $\mathfrak{p}_{i_1}$ of $k(\pi)$.
Thus $\tilde{\mathfrak{p}}_{i_0}$ divides $\sigma^{-1}(\pi) - \pi$. i.e. $\tilde{\mathfrak{p}}_{i_0}$ divides $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right)$. But $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \in A_v$. That is $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \in A_v \cap \tilde{\mathfrak{p}}_{i_0} = \mathfrak{p}_v$.
Therefore $\mathfrak{p}_v \mid Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right)$ i.e. $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \equiv 0 \mod \mathfrak{p}_v$.
It contradicts our initial hypothesis.
Hence there is a unique zero of π above $\mathfrak{p}_v$ in $k(\pi)$.

$\Diamond$

Remark 2.8. *We know by definition that the conjugate of a Weil number π is also a Weil number. So any characterization of Weil numbers one provides must not depend on π but on its minimal polynomial $M(x)$ over k.*
Based on that fact, two questions emerge from the previous proposition 2.4. First of all how does one identify which factor $f_{i_0}(x)$ describes a zero of π? Secondly one can notice at the first glance that the condition

$$\text{“}Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \mod \mathfrak{p}_v \neq 0\text{”}$$

depends on the factor $f_{i_0}(x)$ describing a zero of π. So even if one succeeds in identifying $f_{i_0}(x)$, how sure are we that the statement remains true for any other conjugate of π? The following proposition handle that issue.

Proposition 2.5. *$M(x)$ is the minimal polynomial of $\pi \in \overline{k}$. $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ denote the primes of $k(\pi)$ above $\mathfrak{p}_v$. If there is a unique prime containing π i.e.*

$$\exists!\ i_0 \in \{1, \cdots, s\} \text{such that } \pi \in \mathfrak{p}_{i_0} \text{ but } \pi \notin \mathfrak{p}_j\ \forall j \neq i_0.$$

then so is it for any other conjugate $\tilde{\pi}$ of π.

Proof: As mentioned before, F denotes the splitting field of $M(x)$. π and $\tilde{\pi}$ are conjugate. that means one can find $\alpha \in Gal\left(F/k\right)$ such that $\tilde{\pi} = \alpha\left(\pi\right)$. $\pi \in \mathfrak{p}_{i_0}$ and $\pi \notin \mathfrak{p}_j\ \forall j \neq i_0$. Let $\mathfrak{p}_{1j}, \cdots, \mathfrak{p}_{l_j j}$ be the primes of F above $\mathfrak{p}_j$. $\pi \in \mathfrak{p}_{i_0}$ means $\pi \in \mathfrak{p}_{ii_0}\ \forall i = 1, \cdots, l_{i_0}$. i.e. $\alpha(\pi) \in \alpha(\mathfrak{p}_{ii_0})\ \forall i = 1, \cdots, l_{i_0}$. In other words $\tilde{\pi} \in \alpha(\mathfrak{p}_{i_0})$.
$\forall j \neq i_0\ \pi \notin \mathfrak{p}_j$. That means $\pi \notin \mathfrak{p}_{ij}$ for some $i \in \{1, \cdots, l_j\}$. Equivalently, $\alpha(\pi) \notin \alpha(\mathfrak{p}_{ij})$ for some i. In other words $\tilde{\pi} \notin \alpha(\mathfrak{p}_j)$.
Therefore $\tilde{\pi} \in \alpha\left(\mathfrak{p}_{i_0}\right)$ and $\tilde{\pi} \notin \alpha\left(\mathfrak{p}_j\right)\ \forall j \neq i_0$. Since α acts as a permutation on the set of primes, we can conclude that $\tilde{\pi}$ belongs to some prime
$\mathfrak{q}_{k_0} = \alpha\left(\mathfrak{p}_{i_0}\right)$ of $k(\tilde{\pi})$ above $\mathfrak{p}_v$ and $\tilde{\pi}$ does not belong to any other prime $\mathfrak{q}_j\ j \neq k_0$ of $k(\tilde{\pi})$ above $\mathfrak{p}_v$.

$\diamondsuit$

Corollary 2.1. *$M(x) = f_1(x) \cdot f_2(x) \cdots f_s(x) \in k_v[x]$ is the irreducible decomposition in $k_v[x]$ of a polynomial of the first form (1).*
There is a unique zero of π in $k(\pi)$ lying over the place v of k if and only if $Res\left(f_j(x), \frac{M(x)}{f_j(x)}\right) \mod \mathfrak{p}_v \neq 0\ \forall j \in \{1, \cdots, s\}$.

Proof: Let us assume that there is a unique zero of π in $k(\pi)$. Let $f_{i_0}(x)$ be the irreducible factor of $M(x)$ in $k_v[x]$ describing that zero of π. That means $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \mod \mathfrak{p}_v \neq 0$. If for some other $i_1 \in \{1, \cdots, s\}$ $i_1 \neq i_0$, $Res\left(f_{i_1}(x), \frac{M(x)}{f_{i_1}(x)}\right) \mod \mathfrak{p}_v = 0$, then we have the following:
$f_{i_1}(x)$ also describes a zero in $k(\tilde{\pi})$ of some root $\tilde{\pi}$ of $M(x)$. Let F be the splitting field of $M(x)$. Since $M(x)$ is irreducible and separable over k, $Gal(F/k)$ acts transitively on the set of roots. That means π and $\tilde{\pi}$ are conjugate. In other words there exists $\alpha \in Gal(F/k)$ such that
$\tilde{\pi} = \alpha\left(\pi\right)$. $Res\left(f_{i_1}(x), \frac{M(x)}{f_{i_1}(x)}\right) \mod \mathfrak{p}_v = 0$ means that $\tilde{\pi}$ has more than a zero in $k(\tilde{\pi})$ above $\mathfrak{p}_v$ (see proposition 2.4). This is (based on proposition 2.5) a contradiction.
Hence we also have $Res\left(f_j(x), \frac{M(x)}{f_j(x)}\right) \mod \mathfrak{p}_v \neq 0$ for any other $j \neq i_0$.
Conversely if $Res\left(f_j(x), \frac{M(x)}{f_j(x)}\right) \mod \mathfrak{p}_v \neq 0$ for all $j \in \{1, \cdots, s\}$ then we have in particular $Res\left(f_{i_0}(x), \frac{M(x)}{f_{i_0}(x)}\right) \mod \mathfrak{p}_v \neq 0$. Where $f_{i_0}(x)$ denotes an irreducible factor of $M(x)$ in $k_v[x]$ describing a zero of π. Hence π has a unique zero in $k(\pi)$ above the place v of k (see proposition 2.4).

$\diamondsuit$

We summarize our discussion in the following theorem.

Theorem 2.1. *Let $M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + \mu Q \in A[x]$ be a potential Weil polynomial. i.e. $\deg a_i \leq \frac{i \deg Q}{r}$ and $M(x)$ is irreducible over k. Let D*

be the discriminant of the polynomial $M(x)$. $k(\pi) = k[x]/M(x)\cdot k[x]$.

1. *Let* $n = v(D)+1$ *and* $\overline{M(x)} \equiv \overline{f_1}(x)\cdot\overline{f_2}(x)\cdots\overline{f_{\mathfrak{s}}}(x) \mod \mathfrak{p}_v^n$ *be an irreducible decomposition of* $M(x) \mod \mathfrak{p}_v^n$.
   There is a unique zero of π *in* $k(\pi)$ *lying over the place* v *of* k *if and only if* $Res\left(\overline{f_i}(x), \frac{\overline{M(x)}}{\overline{f_i}(x)}\right) \not\equiv 0 \mod \mathfrak{p}_v \quad \forall i = 1,\cdots,\mathfrak{s}$.

2. *Let* $s = \lceil\frac{\deg Q}{r}\rceil$ *and* $h = v_\infty(D) + sr(r-1)+1$.
   $M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$.
   There is a unique place of $k(\pi)$ *lying over the place at* ∞ *of* k *if and only if* $\overline{M_0(x)} \equiv M_0(x) \mod \frac{1}{T^h}$ *is irreducible.*

2.2 Algorithm - Weil polynomials

In this part we provide an algorithm that takes as input a polynomial of the form $M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q$ with $\deg a_i \le \frac{i\deg Q}{r}$ and $s = \lceil\frac{\deg Q}{r}\rceil$ (r prime).

The algorithm outputs a "True" if the polynomial is a Weil polynomial and a "False" otherwise.

Before giving the algorithm, let us draw the attention of the reader on the fact that from the results we provided so far, all the conditions ($c1$ to $c5$) of definition 2.1 can be checked using only the coefficients of the given polynomial.

Algorithm 2.1. ***Input***: $M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q$

1. *Compute* $D = disc\,(M(x))$.

2. *Compute* $h = v_\infty\,(D) + sr(r-1)+1$

3. *Set* $M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \frac{a_2}{T^{2s}}x^{r-2} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{r.s}}$.
   If $M_0(x)$ *is not irreducible modulo* $\frac{1}{T^h}$ *then* ***output*** *False and exit.*
   else move to the next step.

4. *Compute* $n = v(D)+1$ *where* v *is the valuation associated to the prime* $\mathfrak{p}_v$ *A-characteristic of* L.

5. *Compute* $\overline{M}(x) \equiv M(x) \mod \mathfrak{p}_v^n$ *and decompose (irreducibly)*
   $\overline{M}(x) = \bar{f}_1(x)\cdot\bar{f}_2(x)\cdots\bar{f}_{\mathfrak{s}}(x)$.
   If for all $j \in \{1,\cdots,\mathfrak{s}\}$ *Res* $\left(\bar{f}_j(x), \frac{\overline{M}(x)}{\bar{f}_j(x)}\right) \not\equiv 0 \mod \mathfrak{p}_v$ *then*
   output *True and exit.*
   Else: then ***output*** *False and exit.*
   $Res(\cdot,\cdot)$ *denotes the resultant function.*

Remark 2.9.

1. *Each step of algorithm 2.1 requires to know only the coefficients of the polynomial $M(x)$ and can be achieved in finitely many computations.*

2. *If $r \mid \deg Q$ and $h = 1$ then $s = \frac{\deg Q}{r}$, and the step 2 is done by simply checking that the polynomial*
   $M_0(x) = x^r + \sum_{i \in I} a_{i,0} x^{r-i} + \mu$ *is irreducible over $\mathbb{F}_q$.*
   Where $I = \left\{ i = 1, \cdots, r-1;\ \deg a_i = \frac{i \deg Q}{r} \right\}$ and $a_{i,0}$ denotes the leading coefficient of a_i.
   Indeed, for $h = 1$,

   $$\frac{a_i}{T^{is}} \equiv \begin{cases} 0 \mod \frac{1}{T} & if \deg a_i < \frac{i \deg Q}{r} \\ a_{i,0} \mod \frac{1}{T} & if \deg a_i = \frac{i \deg Q}{r} \end{cases}$$

   One can also remark that the residue field associated to the place ∞ is $\mathbb{F}_q$.
   One may also notice that $h = 1$ if and only if $disc\,(M_0(x)) \neq 0$ where $M_0(x) = x^r + \sum_{i \in I} a_{i,0} x^{r-i} + \mu$.
   Indeed, The discriminant of the polynomial

   $$M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1} x + \mu Q$$

   is a homogeneous polynomial of degree $2r - 2$ in its coefficients. One of the monomials is $\mu^{r-1} Q^{r-1}$ whose degree (in T) is $(r-1) \deg Q$. Also, all the monomials of the form $a_{i_1}^{\alpha_1} \cdots a_{i_l}^{\alpha_l}$ with $i_k \in I$, have degree (in T) $(r-1) \deg Q$. Therefore $v_\infty\,(disc\,(M(x))) := -\deg_T\,(disc\,(M(x))) = -(r-1) \deg Q$ iff $disc\,(M_0(x)) \neq 0$. In such a case $h = 1$.

3. *A priori, the algorithm only tells us for a given polynomial whether the polynomial is a Weil polynomial or not. But one can also use that algorithm to provide the complete list of degree r Weil polynomials.*
   Indeed, the coefficients a_i of the polynomial

   $$M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1} x + \mu Q$$

   are bounded by $\deg a_i \leq \frac{i \deg Q}{r}$ and $a_i \in \mathbb{F}_q[T]$. So there are finitely many such polynomials. One can then check for each polynomial (using the algorithm) whether the polynomial is a rank r Weil polynomial or not.

In fact the number of polynomials $a_i \in \mathbb{F}_q[T]$ of degree atmost $\frac{i \deg Q}{r}$ is $q^{\frac{i \deg Q}{r}+1}$. Thus for polynomials of the form

$$M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + \mu Q \in A[x],$$

we have a total number of $\prod_{i=1}^{r-1} q^{\frac{i \deg Q}{r}+1} = q^{(r-1)\left[1+\frac{\deg Q}{2}\right]}$ *polynomials to be checked. This number can be reduced if one takes into account the following result.*

Proposition 2.6. *We consider the same polynomial $M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + \mu Q \in A[x]$, whose root π generates the fields extension $k(\pi)/k$. If $\mathfrak{p}_v$ does not divide a_{r-1}, then π satisfies the condition $(c2)$ of the definition 2.1. That is, there is a unique zero of π in $k(\pi)$ over the place v.*

Proof: We get to prove the contraposition of the statement above. That is, if π has more than a zero over the place v then $\mathfrak{p}_v$ divides a_{r-1}.
Let $\mathfrak{p}_1$ be a zero of π above v in $k(\pi)$. If π has another zero say $\mathfrak{p}_2$, then we have the following.
Let F be the splitting field of $M(x)$. F/k is a Galois extension and $k(\pi)$ is an intermediate field. Let $\mathfrak{p}_1'$ and $\mathfrak{p}_2'$ be extensions of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively in F. Let B be the integral closure of A in $k(\pi)$. $\mathfrak{p}_1' \cap A = \mathfrak{p}_1' \cap B \cap A = \mathfrak{p}_1 \cap A = \mathfrak{p}_v$. Same for $\mathfrak{p}_2'$. So $\mathfrak{p}_1'$ and $\mathfrak{p}_2'$ are primes of F above $\mathfrak{p}_v$. Since $Gal(F/k)$ acts transitively on the sets of primes above $\mathfrak{p}_v$, there exists $\sigma \in Gal(F/k)$ such that $\mathfrak{p}_2' = \sigma(\mathfrak{p}_1')$. $\mathfrak{p}_2' \big| \pi$ then $\sigma(\mathfrak{p}_1') \big| \pi$. That is $\mathfrak{p}_1' \big| \sigma^{-1}(\pi)$. Moreover, $\sigma^{-1}(\pi) \neq \pi$ otherwise σ would be in $Gal(F/k(\pi))$ that is
$\mathfrak{p}_1 = \sigma(\mathfrak{p}_1) = \sigma(\mathfrak{p}_1' \cap B) = \sigma(\mathfrak{p}_1') \cap \sigma(B) = \mathfrak{p}_2' \cap B = \mathfrak{p}_2$. Which is not possible since $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Also, $a_{r-1} = \sum_{j=1}^{r} \prod_{i=1, i\neq j}^{r} \tau_i(\pi)$, $\mathfrak{p}_1' \big| \pi$ and $\mathfrak{p}_1' \big| \sigma^{-1}(\pi)$. Therefore $\mathfrak{p}_1' \big| a_{r-1}$. That is $a_{r-1} \in \mathfrak{p}_1'$ but $a_{r-1} \in A$. Hence $a_{r-1} \in \mathfrak{p}_1' \cap A = \mathfrak{p}_v$ i.e. $\mathfrak{p}_v \big| a_{r-1}$. $\diamondsuit$

Remark 2.10. *As we mentioned in remark 2.9, if one takes into account the above mentioned result, the number of polynomials to be checked (using the whole algorithm 2.1) can be reduced to*

$$q^{1+\frac{(r-1)\deg Q}{r} - \deg \mathfrak{p}_v} \times \prod_{i=1}^{r-2} q^{1+\frac{i \deg Q}{r}} = q^{(r-1)\left[\frac{\deg Q}{2}+1\right] - \deg \mathfrak{p}_v}$$

For other polynomials for which $\mathfrak{p}_v \nmid a_{r-1}$, one can just check the step 2 of our algorithm.

2.3 Generalization to any positive degree r.

As we promised in remark 2.4, we are going to drop the primality property of r and just consider any positive integer r. But we still keep the assumption $A2$ of remark 2.4 concerning the separability of the extension $k(\pi)/k$.
One can notice that, the only condition which has really involved the primality property of r is the last condition $(c5)$ of definition 2.1. Once we get rid of that primality hypothesis, instead of polynomials (1) and (2) as we got before, we now have the below mentioned polynomials:

Theorem 2.2 (General potential Weil polynomials).
Let r be a positive integer and $s = \left\lceil \frac{\deg Q}{r} \right\rceil$. A degree r Weil polynomial must have one of the below mentioned forms:

(1) $M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + \mu Q$ such that the polynomial $M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$ is irreducible in $k_\infty[x]$

(2) $M(x) = x^{r_1} + a_1 x^{r_1-1} + \cdots + a_{r_1-1}x + \mu Q^{1/r_2}$ such that the polynomial $M_0(x) = x^{r_1} + \frac{a_1}{T^s}x^{r_1-1} + \cdots + \frac{a_{r_1-1}}{T^{s(r_1-1)}}x + \mu\frac{Q^{1/r_2}}{T^{sr_1}}$ is irreducible in $k_\infty[x]$. Where r_1 and r_2 are positive integers (≥ 2) such that $r = r_1 \cdot r_2$ and r_2 divides m. The coefficients $a_{i's}$ follow the same boundary condition $\deg a_i \leq \frac{i \deg Q}{r} = \frac{i \deg Q^{1/r_2}}{r_1} \leq is$.

(3) $x - \mu Q^{1/r}$ with $r \mid m$ and $\mu \in \mathbb{F}_q^*$

Proof: Let π be a rank r Weil number and $M(x)$ the corresponding Weil polynomial (i.e. the minimal polynomial of π over k). The condition $(c5)$ requires $\deg M(x)$ to be a divisor of r. Let $r_1 = \deg M(x)$ and $r_2 = \frac{r}{r_1}$. Remark 2.3 (which does not require the primality hypothesis on r) informs us that $M(x)$ has the form

$$M(x) = x^{r_1} + a_1 x^{r_1-1} + \cdots + a_{r_1-1}x + \mu Q^{1/r_2}$$

with $r_2 \mid m$, $\deg a_i \leq \frac{i \deg Q}{r} \leq is$ with $s = \left\lceil \frac{\deg Q}{r} \right\rceil$.

If $r_1 = r$ then $M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + \mu Q$.
π is a rank r Weil number. Thus the place at ∞ has a unique extension in $k(\pi) = k\left(\frac{\pi}{T^s}\right)$. That is, the minimal polynomial of $\frac{\pi}{T^s}$ which is

$$M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$$

must be irreducible or a power of an irreducible polynomial in $k_\infty[x]$; but since $M_0(x)$ is separable, $M_0(x)$ must be irreducible in $k_\infty[x]$.

If r_1 =1 then $M(x) = x + \mu Q^{1/r}$, $\mu \in \mathbb{F}_q^*$ and for the same reason as for the case r prime, r must divide m.

If $r_1 \neq 1,\ r$ then we have the following:

$$M(x) = x^{r_1} + a_1 x^{r_1 - 1} + \cdots + a_{r_1 - 1} x + \mu Q^{1/r_2}$$

with $r_2 \mid m$, $\deg a_i \leq \frac{i \deg Q}{r}$ as mentioned in remark 2.3. Since there is a unique place above the place at ∞ in $k(\pi) = k\left(\frac{\pi}{T^s}\right)$, the minimal polynomial of $\frac{\pi}{T^s}$ which is

$$M_0(x) = x^{r_1} + \frac{a_1}{T^s} x^{r_1 - 1} + \cdots + \frac{a_{r_1 - 1}}{T^{s(r_1 - 1)}} x + \mu \frac{Q^{1/r_2}}{T^{s r_1}}$$

must be either irreducible or a power of an irreducible polynomial over k_∞. But $M_0(x)$ is separable. Therefore it must be irreducible in $k_\infty[x]$.

Hence we have the expected result. ◊

Conversely, let us now pick π a root of the above mentioned polynomials (1), (2) or (3) in theorem 2.2.

- The condition $(c1)$ is obvious for each case since the polynomials (1), (2) and (3) are in $A[x]$.
- The condition $(c3)$ follows from the condition imposed to the polynomial $M_0(x)$ for the cases (1) and (2). $M_0(x)$ is irreducible over the completion field k_∞ of k at the place ∞. i.e. there is a unique place of $k(\pi)$ over ∞. Same thing for the corresponding polynomial in (3) since it is a degree 1 polynomial.
- The condition $(c4)$ is obtained from the value of $N_{k(\pi)/k}(\pi)$ in each case.
  For the polynomial (1), $N_{k(\pi)/k}(\pi) = (-1)^r \mu Q$. i.e.
  $v_{\infty'}(\pi) := \frac{1}{[k(\pi):k]} v_\infty\left(N_{k(\pi)/k}(\pi)\right) = -\frac{1}{r} \deg Q$.
  Likewise for the third polynomial (3).
  Concerning the polynomial (2), we have $N_{k(\pi)/k}(\pi) = (-1)^{r_1} \mu Q^{1/r_2}$ and then $v_{\infty'}(\pi) = \frac{1}{[k(\pi):k]} v_\infty\left(N_{k(\pi)/k}(\pi)\right) = -\frac{1}{r_1 \cdot r_2} \deg Q = -\frac{1}{r} \deg Q$.
  ∞' here denotes (to avoid any confusion) the unique extension of ∞ in $k(\pi)$.
  Therefore in each case $|\pi|_{\infty'} = q^{-v_{\infty'}(\pi)} = q^{\frac{1}{r}\deg Q} = l^{1/r}$ where $l = |L|$.
- Condition $(c5)$ is also straightforward from the hypothesis since
  in case (1) $[k(\pi) : k] = r$ divides r,

in case (2) $[k(\pi):k] = r_1$ which is assumed to be a divisor of r,
and in case (3) $[k(\pi):k] = 1$ divides r.

Therefore the only condition missing to the bunch of requirements is the condition ($c2$).

Corollary 2.2. *If m and r are coprime, then the only potential Weil polynomials are the one of the form*

$$M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu Q$$

such that the polynomial $M_0(x) = x^r + \frac{a_1}{T^s}x^{r-1} + \cdots + \frac{a_{r-1}}{T^{s(r-1)}}x + \mu\frac{Q}{T^{sr}}$ is irreducible in $k_\infty[x]$.

Proof: If m and r are coprime, then no divisor of r other than 1 divides m. Thus the cases (2) and (3) of theorem 2.2 cannot occur. $\Diamond$

Remark 2.11. *The algorithm 2.1 can also be used here (without any further modification) to list the rank r Weil polynomials where r denotes any positive integer. The only thing that changes is the list of potential Weil polynomials. In addition to the set of polynomials we had before, one must also check (using the algorithm 2.1) each polynomial of the form*

$$x^{r_1} + a_1x^{r_1-1} + \cdots + a_{r_1-1}x + \mu Q^{1/r_2}.$$

Where r_2 runs through the set $\mathcal{D}(r,m)$ of common divisors of r and m, and $r_1 = \frac{r}{r_2}$.

2.4 Generalization for inseparable Weil polynomials

As mentioned in remark 2.4, we are going to drop the last remaining assumption A2.

Remark 2.12. *Before going further, let us draw the attention of the reader on the following fact:*
The only sprain to the generality is how to check the conditions (c2) and (c3) when $M(x)$ is inseparable. In other words how to get the irreducible factorization of $M(x)$ over the completion field $k_* \in \{k_\infty,\ k_v\}$. In the previous case, the factorization was entirely determine by the irreducible decomposition of $M(x) \mod \mathfrak{p}_v^n$ and $M(x) \mod \frac{1}{T^h}$ for k_v and k_∞ respectively. Where $n = v\left(disc\left(M(x)\right)\right) + 1$ and $h = v_\infty\left(disc\left(M(x)\right)\right) + sr(r-1) + 1$.

That argument is not valid anymore in this case because disc $(M(x)) = 0$. *But at least one knows that if* $M(x)$ *is an inseparable irreducible polynomial over a field* k *of characteristic* $p > 0$, *then there exists a separable polynomial* $f(x) \in k[x]$ *such that* $M(x) = f\left(x^{p^d}\right)$ *for some* $d \in \mathbb{N}$. *We will use the separable polynomial* $f(x)$ *to overcome the difficulties encountered when* $M(x)$ *is inseparable.*

2.4.1 Some properties of monic irreducible polynomials over a field k of characteristic $p > 0$

We provide in this part, as mentioned in the title, some important properties of irreducible polynomials over a field k, with $char(k) = p > 0$. These properties will be very helpful later on.

Proposition 2.7. *[6, theorem A6, page 11]*
Let k *be a field of characteristic* $p > 0$ *and* $f(x)$ *be a monic irreducible polynomial in* $k[x]$. *Then* $f(x^p)$ *is either irreducible or a* p*-th power of an irreducible polynomial in* $k[x]$.

Proof:[6] Let k be a field of characteristic $p > 0$ as mentioned above and $f(x)$ be a monic irreducible polynomial in $k[x]$. Let $g(x)$ be a monic irreducible factor of $f(x^p)$. So $f(x^p) = g(x)^n \cdot h(x)$ for some $n \in \mathbb{N}$ and $h(x) \in k[x]$ such that $g(x)$ does not divide $h(x)$. Differentiating both sides of the equation gives:
$0 = ng'(x) \cdot g(x)^{n-1} \cdot h(x) + g(x)^n \cdot h'(x) = g(x)^{n-1}\left(ng'(x) \cdot h(x) + g(x) \cdot h'(x)\right)$.
Thus $ng'(x) \cdot h(x) = -g(x) \cdot h'(x)$ i.e. $g(x) \mid ng'(x) \cdot h(x)$. But $k[x]$ is a UFD, $g(x)$ is irreducible (hence prime) in $k[x]$ and $g(x) \nmid h(x)$. Therefore $g(x) \mid ng'(x)$. But $\deg g(x) > \deg g'(x)$. So $ng'(x)$ must be 0. i.e.

$$n = 0 \text{ in } k \text{ or } g'(x) = 0.$$

- If $g'(x) = 0$ then
  $g(x) = \tilde{g}(x^p)$ for some monic polynomial $\tilde{g}(x) \in k[x]$.
  Thus $f(x^p) = g(x)^n \cdot h(x) = \tilde{g}(x^p)^n \cdot h(x)$. By differentiating both sides of the equation $f(x^p) = \tilde{g}(x^p)^n \cdot h(x)$, one can also see that $h(x)$ must be a polynomial in x^p. That is $h(x) = \tilde{h}(x^p)$ for some monic polynomial $\tilde{h}(x) \in k[x]$.
  So one obtains $f(x^p) = \tilde{g}(x^p)^n \cdot \tilde{h}(x^p)$. In other words $f(x) = \tilde{g}(x)^n \cdot \tilde{h}(x)$.
  But $f(x)$ is a monic irreducible polynomial over k.
  Since $n \geq 1$ we must therefore have $n = 1$ and $\tilde{h}(x) = 1$.
  Hence $f(x^p) = \tilde{g}(x^p) = g(x)$ is irreducible.

- If $n = 0$ in k then $n = ps$ for some $s \in \mathbb{N}$.
  So $f(x^p) = g(x)^n \cdot h(x) = g(x)^{ps} \cdot h(x)$. By differentiating both sides of the equation $f(x^p) = g(x)^{ps} \cdot h(x)$, one can see that $h(x)$ must be a polynomial in x^p since $h'(x) = 0$. So $f(x^p) = g(x)^{ps} \cdot \tilde{h}(x^p)$ where $h(x) = \tilde{h}(x^p)$.
  $g(x)^p$ is of course a polynomial in x^p. Let us set $g(x)^p = \tilde{g}(x^p)$. Thus $f(x^p) = \tilde{g}(x^p)^s \cdot \tilde{h}(x^p)$ that is $f(x) = \tilde{g}(x)^s \cdot \tilde{h}(x)$.
  But $f(x)$ is a monic irreducible polynomial in $k[x]$. Therefore we must have $\tilde{h}(x) = 1$ and $s = 1$. That is $f(x^p) = \tilde{g}(x^p) = g(x)^p$.
  Hence $f(x^p)$ is a p-th power of an irreducible polynomial in $k[x]$.

$\diamondsuit$

Corollary 2.3. *[6, Corollary A8]*
Let k be a field of characteristic $p > 0$ and $f(x)$ be a monic irreducible polynomial in $k[x]$. The following statements are equivalent.

(i) *$f(x^{p^n})$ is irreducible in $k[x]$ $\forall n \in \mathbb{N}$.*

(ii) *$f(x) \notin k^p[x]$*

One should keep in mind that we mean by $k^p = \{a^p,\ a \in k\}$.

Proof:[6]

(i) $\Rightarrow$ (ii) If $f(x) \in k^p[x]$ then $f(x^p) \in k^p[x^p]$.
That is $f(x^{p^n}) = x^{p^n} + a_1^p x^{p^{n-1}} + \cdots + a_{n-1}^p x^p + a_n^p, \quad a_i \in k$.
Thus $f(x^{p^n}) = \left(x^{p^{n-1}} + a_1 x^{p^{n-2}} + \cdots + a_{n-1}x + a_n\right)^p$ is reducible.
In other words, $f(x) \in k^p[x]$ implies $f(x^{p^n})$ reducible in $k[x]$. Therefore by contrapositive, $f(x^{p^n})$ irreducible implies $f(x) \notin k^p[x]$.

(ii) $\Rightarrow$ (i) We proceed by induction on n. $f(x)$ is a monic irreducible polynomial in $k[x]$. One can then get from the proposition 2.7 that $f(x^p)$ is either irreducible or a p-th power of an irreducible polynomial in $k[x]$.
If $f(x^p)$ were a p-th power of an irreducible polynomial in $k[x]$, then $f(x)$ would be in $k^p[x]$ which is not possible according to our hypothesis (ii).
Therefore $f(x^p)$ is irreducible.
Let us assume that $f(x^{p^{n_0}})$ is irreducible for some fixed $n_0 \in \mathbb{N}$ and let us prove that $f(x^{p^{n_0+1}})$ is also irreducible.
We set $g(x) = f(x^{p^{n_0}})$.
$g(x)$ is a monic irreducible polynomial in $k[x]$. So from proposition 2.7, one can say that either $g(x^p)$ is irreducible or $g(x^p)$ is a p-th power

of an irreducible polynomial in $k[x]$. $f(x^{p^{n_0}})$ and $f(x)$ have the same coefficients in k. Thus since $f(x) \notin k^p[x]$, $g(x) = f(x^{p^{n_0}}) \notin k^p[x]$.
If $g(x^p)$ were a p-th power of an irreducible polynomial in $k[x]$ then $g(x)$ would be in $k^p[x]$. That is not possible because of our hypothesis (ii).
Therefore $g(x^p)$ must be irreducible in $k[x]$. That is $f(x^{p^{n_0+1}})$ is irreducible in $k[x]$.
Hence $\forall n \in \mathbb{N}$ $f(x^{p^n})$ is irreducible in $k[x]$.

$\diamondsuit$

Corollary 2.4. *Let k be a field of characteristic $p > 0$ and $f(x)$ be a monic irreducible polynomial in $k[x]$. Let $n \in \mathbb{N}$.*
$f(x^{p^n})$ is either irreducible or a p^{n_0}-th power of an irreducible polynomial in $k[x]$ for some $n_0 \in \mathbb{N}$.

Proof: Let $f(x)$ be a monic irreducible polynomial in $k[x]$ as mentioned in the corollary above. We know from corollary 2.3 that if $f(x) \notin k^p[x]$ then $f(x^{p^n})$ is irreducible.
Now if $f(x) \in k^p[x]$ then,
Let $f(x) = x^d + a_1^p x^{d-1} + \cdots + a_{d-1}^p x + a_d^p$.
We set $n_0 = \min\left\{\nu_p(a_i^p),\ i = 1, \cdots, d\right\}$ where $\nu_p(a_i^p)$ denotes the positive integer t such that $a_i^p = b_i^{p^t}$ and $b_i \in k \setminus k^p$. Let $a_{i_0}^p$ be the coefficient for which $n_0 = \nu_p(a_{i_0}^p)$.

$$f(x) = x^d + b_1^{p^{n_0+r_1}} x^{d-1} + b_2^{p^{n_0+r_2}} x^{d-2} + \cdots + b_{i_0}^{p^{n_0}} x^{d-i_0} + \cdots + b_{d-1}^{p^{n_0+r_{d-1}}} x + b_d^{p^{n_0+r_d}}$$

If $n \geq n_0$ then we have the following

$$\begin{aligned} f(x^{p^n}) &= x^{dp^n} + b_1^{p^{n_0+r_1}} x^{(d-1)p^n} + \cdots + b_{i_0}^{p^{n_0}} x^{(d-i_0)p^n} + \cdots + \\ &\quad + b_{d-1}^{p^{n_0+r_{d-1}}} x^{p^n} + b_d^{p^{n_0+r_d}} \\ &= \Big(x^{dp^{n-n_0}} + b_1^{p^{r_1}} x^{(d-1)p^{n-n_0}} + \cdots + b_{i_0} x^{(d-i_0)p^{n-n_0}} + \cdots + \\ &\quad + b_{d-1}^{p^{r_{d-1}}} x^{p^{n-n_0}} + b_d^{p^{r_d}} \Big)^{p^{n_0}} \\ &= \left(g_0\left(x^{p^{n-n_0}} \right) \right)^{p^{n_0}} \end{aligned}$$

with $g_0(x) = x^d + b_1^{p^{r_1}} x^{d-1} + \cdots + b_{i_0} x^{d-i_0} + \cdots + b_{d-1}^{p^{r_{d-1}}} x + b_d^{p^{r_d}}$
$g_0(x)$ must be irreducible in $k[x]$. Indeed,
If $g_0(x)$ is reducible in $k[x]$, that is $g_0(x) = h_1(x) \cdot h_2(x)$ with $h_1(x)$ and $h_2(x)$ in $k[x]$, then we have the following:
$g_0\left(x^{p^{n-n_0}}\right) = h_1\left(x^{p^{n-n_0}}\right) \cdot h_2\left(x^{p^{n-n_0}}\right)$. That is,

$$\begin{aligned} f(x^{p^n}) = \left(g_0\left(x^{p^{n-n_0}}\right)\right)^{p^{n_0}} &= \left(h_1\left(x^{p^{n-n_0}}\right)\right)^{p^{n_0}} \cdot \left(h_2\left(x^{p^{n-n_0}}\right)\right)^{p^{n_0}} \\ &= h_1^{p^{n_0}}\left(x^{p^n}\right) \cdot h_2^{p^{n_0}}\left(x^{p^n}\right) \end{aligned}$$

Where $h_i^{p^{n_0}}(x)$ denotes the polynomial obtained from $h_i(x)$ by raising all its coefficients to the power p^{n_0}.
Thus $f(x^{p^n}) = h_1^{p^{n_0}}\left(x^{p^n}\right) \cdot h_2^{p^{n_0}}\left(x^{p^n}\right)$ i.e. $f(x) = h_1^{p^{n_0}}(x) \cdot h_2^{p^{n_0}}(x)$ which contradicts the fact that $f(x)$ is irreducible.
Hence $g_0(x)$ must be irreducible in $k[x]$.
In addition, since $b_{i_0} \notin k^p$, we also have $g_0\left(x^{p^{n-n_0}}\right)$ is irreducible (see corollary 2.3).

If $n < n_0$ then one can write down $f(x^{p^n})$ as follows

$$F(x) := f(x^{p^n}) = \ (g(x))^{p^n}$$

with $g(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0 \in k^p[x]$.
<u>Claim 1</u>: If $f(x)$ is separable then so is $g(x)$.
We know that $f(x)$ is a separable polynomial and $d = \deg f(x)$. We also know that for each root α of $f(x)$, the p^n-th root $\alpha^{\frac{1}{p^n}}$ of α is a root of $F(x)$. So $F(x)$ has at least d distinct roots ①.
Also $F(x) = f(x^{p^n}) = (g(x))^{p^n}$ and $\deg g(x) = d$. Thus $F(x)$ has a maximum of d distinct roots ②.
① and ② imply that $F(x)$ must have exactly d distinct roots.
Therefore $g(x)$ is separable.
<u>Claim 2</u>: $g(x)$ is irreducible over k.
Indeed, Let us assume that $g(x)$ is reducible over k.
That is $g(x) = h_1(x) \cdot h_2(x)$.
Therefore $(g(x))^{p^n} = (h_1(x))^{p^n} \cdot (h_2(x))^{p^n} = h_1^{p^n}\left(x^{p^n}\right) \cdot h_2^{p^n}\left(x^{p^n}\right)$. Where $h_i^{p^n}(x)$ denotes the polynomial obtained from $h_i(x)$ by raising all its coefficients to the power p^n.
Thus $f(x^{p^n}) = (g(x))^{p^n} = h_1^{p^n}\left(x^{p^n}\right) \cdot h_2^{p^n}\left(x^{p^n}\right)$ That is $f(x) = h_1^{p^n}(x) \cdot h_2^{p^n}(x)$ which is impossible since $f(x)$ is irreducible over k.
Hence $g(x)$ must be irreducible.
So for this special case, if in addition to the hypothesis of the corollary $f(x)$ is separable, then $f(x^{p^n})$ would be a p^n-th power of an irreducible separable polynomial.

Therefore in any case $f(x^{p^n})$ is either irreducible or a p^{n_0}-th power of an irreducible polynomial in $k[x]$. $\Diamond$

2.4.2 Inseparable Weil polynomials

Let us come back to our Weil number π with all the notations we have set at the beginning and $k = \mathbb{F}_q(T)$. We now assume that the extension $k(\pi)/k$ is not separable. That is the minimal polynomial $M(x)$ of π is an irreducible inseparable polynomial in $k[x]$. We know that if it is the case, then there exists a separable irreducible polynomial $f(x) \in k[x]$ such that

$$M(x) = \ f(x^{p^n}) \text{ for some } n \in \mathbb{N}.$$

Let us first discuss the case where $n = 1$. i.e. $M(x) = f(x^p)$.
Let $f(x) = f_1(x) \cdots f_{\mathfrak{s}}(x)$ be the irreducible decomposition of $f(x)$ over the completion field k_* (where $k_* \in \{k_v,\ k_\infty\}$).
So $M(x) = f(x^p) = f_1(x^p) \cdots f_{\mathfrak{s}}(x^p)$. According to the proposition 2.7, each polynomial $f_i(x^p)$ is either irreducible or a p-th power of an irreducible polynomial $h_i(x) \in k_*[x]$ i.e. $f_i(x^p) = (h_i(x))^p$. In any case, the irreducible decomposition of $f(x)$ encodes all the irreducible factors of $M(x)$ in $k_*[x]$ and is enough to decide about the conditions $(c2)$ and $(c3)$ of definition 2.1. Indeed,
π satisfies condition $(c3)$ if and only if $M(x)$ is irreducible or a power of an irreducible polynomial over k_∞.
But we can say from our above discussion that $M(x)$ is irreducible or a power of an irreducible polynomial over k_∞ if and only if the separable polynomial $f(x)$ is irreducible over k_∞
Likewise, one can properly check in this case the condition $(c2)$ of definition 2.1 using proposition 2.4 where $M(x)$ is replaced by the irreducible separable polynomial $f(x)$. In other words the condition $(c2)$ is satisfied by the polynomial $M(x)$ if and only if it is satisfied by the polynomial $f(x)$. That is $Res\left(f_i(x), \frac{f(x)}{f_i(x)}\right) \neq 0 \mod \mathfrak{p}_v\ \forall i \in \{1, \cdots, \mathfrak{s}\}$. Thanks to corollary 2.1.

Now if $M(x) = f(x^{p^n})$ with $n > 1$ then the same idea holds. That is, the irreducible decomposition of $f(x) = f_1(x) \cdots f_s(x)$ over the completion field k_* encodes the irreducible decomposition of $M(x)$ over k_*.

$$M(x) = f(x^{p^n}) = f_1(x^{p^n}) \cdots f_{\mathfrak{s}}(x^{p^n})$$

From corollary 2.4, one can draw that each $f_i(x^{p^n})$ is either irreducible or a p^{n_0}-th power of an irreducible polynomial in $k_*[x]$ for some $n_0 \in \mathbb{N}$.
Therefore one can use the irreducible decomposition of $f(x)$ in $k_*[x]$ to check the conditions $(c2)$ and $(c3)$ of definition 2.1. Exactly as it happened for the case $n = 1$,
π satisfies condition $(c3)$ if and only if $M(x)$ is irreducible or a power of an

irreducible polynomial over k_∞.
$M(x) = f(x^{p^n})$ is irreducible or a power of an irreducible polynomial over k_∞ if and only if the separable polynomial $f(x)$ is irreducible over k_∞. Thanks to corollary 2.4.
Following the same idea, the polynomial (or a root π of the polynomial) $M(x)$ satisfies the condition $(c2)$ of definition 2.1 if and only if $Res\left(f_i(x^{p^n}), \frac{M(x)}{f_i(x^{p^n})}\right) \neq 0 \mod \mathfrak{p}_v$ $\forall i \in \{1, \cdots, \mathfrak{s}\}$. Thanks once more to proposition 2.4 and also to corollary 2.1.

Remark 2.13. *A conclusion one can draw from our discussion above is that, modulo some slight changes, one can use the same algorithm 2.1 in the case where the polynomial $M(x)$ is inseparable. After those minor changes, we get the following algorithm.*

Algorithm 2.2. $\left(r = p^n r_0,\ s = \left\lceil \frac{\deg Q}{r} \right\rceil = \left\lceil \frac{\deg Q}{p^n r_0} \right\rceil\right)$
Input : $M(x) = x^{p^n r_0} + a_1 x^{p^n(r_0-1)} + \cdots + a_{r_0-1} x^{p^n} + \mu Q = f(x^{p^n})$.
Where $f(x) = x^{r_0} + a_1 x^{r_0-1} + \cdots + a_{r_0-1} x + \mu Q$.

1. *Compute* $h = v_\infty\left(disc\left(f(x)\right)\right) + s r_0(r_0 - 1) + 1$

2. *Set* $f_0(x) = x^{r_0} + \frac{a_1}{T^{p^n s}} x^{r_0-1} + \frac{a_2}{T^{2p^n s}} x^{r_0-2} + \cdots + \frac{a_{r_0-1}}{T^{p^n(r_0-1)s}} x + \mu \frac{Q}{T^{p^n r_0 \cdot s}}$.
   If $f_0(x)$ *is not irreducible modulo* $\frac{1}{T^h}$ *then* ***output*** *False and exit.*
   else move to the next step.

3. *Compute* $u = v(disc\left(f(x)\right)) + 1$ *where* v *is the valuation associated to the prime* $\mathfrak{p}_v$ *A-characteristic of* L.

4. *Compute* $\overline{f}(x) \equiv f(x) \mod \mathfrak{p}_v^u$ *and provide the irreducible decomposition* $\overline{f}(x) = \bar{f}_1(x) \cdot \bar{f}_2(x) \cdots \bar{f}_{\mathfrak{s}}(x)$. *That is the irreducible decomposition of* $\overline{M}(x)$ *is given by* $\overline{M}(x) = \overline{f}(x^{p^n}) = \bar{f}_1(x^{p^n}) \cdot \bar{f}_2(x^{p^n}) \cdots \bar{f}_{\mathfrak{s}}(x^{p^n})$
   If for all $j \in \{1, \cdots \mathfrak{s}\}$ $Res\left(\bar{f}_j(x), \frac{\bar{f}(x)}{\bar{f}_j(x)}\right) \neq 0 \mod \mathfrak{p}_v$
   then ***output*** *True and exit.*
   Else: ***output*** *False and exit.*

Remark 2.14. *The above mentioned algorithm is based on the fact that the irreducible decomposition of the separable polynomial $f(x)$ in $k_*[x]$ encodes the irreducible decomposition of $M(x) = f(x^{p^n})$ in $k_*[x]$. We mean that one can get a 1-to-1 map between the irreducible factors of $f(x)$ and those of $M(x) = f(x^{p^n})$ in $k_*[x]$.*

CHAPTER 3

Description of the endomorphism rings of Drinfeld modules in a given isogeny class

We know that the endomorphism algebra is an isogeny invariant. We consider here isogeny classes of Drinfeld modules whereby endomorphism algebras are field i.e. $End\phi \otimes k = k(\pi)$ where π is the Frobenius endomorphism of Drinfeld modules ϕ in the chosen isogeny class.
A natural question that arises and that we aim to answer in this chapter is: Which orders of $End\phi \otimes k = k(\pi)$ occur as endomorphism rings of Drinfeld modules in our chosen isogeny class?
Let us clearly point out that this question is different from the one answered by Kuhn and Pink in [14] and by Garai and Papikian in [7]. The previously mentioned authors provided efficient algorithms which compute, given a Drinfeld module ϕ the endomorphism ring $End\phi$.
As we have seen before, a general Weil polynomial has the form

$$M(x) = x^{r_1} + a_1 x^{r_1 - 1} + \cdots + a_{r_1 - 1} x + \mu \mathfrak{p}_v^{\frac{m}{r_2}}$$

where $r_1 = [k(\pi) : k]$ and $r_2 = \sqrt{\dim_{k(\pi)} End\phi \otimes_A k}$.
Therefore our restriction on the endomorphism algebra (that must be a field) leads to the restriction to isogeny classes defined by Weil polynomials of the form

$$M(x) = x^{r} + a_1 x^{r-1} + \cdots + a_{r-1} x + \mu \mathfrak{p}_v^{m}$$

Before answering our question, let us recall the notions of Tate modules and Dieudonné modules which are very important to answer the question.

3.1 Tate module of a Drinfeld module

Let ψ be a Drinfeld module over the A-field L with A-characteristic $\mathfrak{p}_v$. v denotes the place of k associated to the prime $\mathfrak{p}_v$. Let ω be a place of k

different from v and $\mathfrak{p}_\omega$ denotes the corresponding prime. $\psi[\mathfrak{p}_\omega^n]$ denotes the group of $\mathfrak{p}_\omega^n$-torsion points of ψ.

Definition 3.1. *The Tate module of ψ at ω is defined by the inverse limit $T_\omega\psi := \varprojlim \psi[\mathfrak{p}_\omega^n] = Hom_{A_\omega}(k_\omega/A_\omega, \psi[\mathfrak{p}_\omega^\infty])$ where $\psi[\mathfrak{p}_\omega^\infty] = \bigcup_{n\geq 1} \psi[\mathfrak{p}_\omega^n]$*

Remark 3.1. *(Recall)*
Let ϕ and ψ be two isogenous Drinfeld modules defined over the A-field L. $Hom_L(\phi,\psi)$ denotes the group of isogenies from ϕ to ψ. Let $u : \phi \longrightarrow \psi$ be an isogeny. If $y \in \phi[\mathfrak{p}_\omega^n]$ then $u(y) \in \psi[\mathfrak{p}_\omega^n]$.
To $u \in Hom_L(\phi,\psi) \otimes A_\omega$, corresponds therefore a canonical morphism of A_ω-modules $u^* \in Hom_{A_\omega}(T_\omega\phi, T_\omega\psi)$.

Theorem 3.1. *[Tate, [10, see theorem 4.12.12]]*
Let ϕ and ψ be two isogenous Drinfeld modules over the finite A-field L as mentioned in the previous remark. Let $G = Gal(\overline{L}/L)$. The canonical map

$$Hom_L(\phi,\psi) \otimes A_\omega \xrightarrow{\sim} Hom_{A_\omega[G]}(T_\omega\phi, T_\omega\psi)$$

is a bijection (as morphism of A_ω-modules).

Corollary 3.1.

- *If $\phi = \psi$ then we have the bijection*

$$End_L\phi \otimes A_\omega \xrightarrow{\sim} End_{A_\omega[G]}T_\omega\phi$$

- *We denote $V_\omega\phi := T_\omega\phi \otimes k_\omega$.*

$$End_L\phi \otimes k_\omega \cong End_{k_\omega[G]}V_\omega\phi$$

as k_ω-algebras.

Remark 3.2. *Let π be the Frobenius endomorphism of the Drinfeld module ϕ. We denote $M(x)$ the minimal polynomial of π over k.*
The characteristic polynomial of the action of π on the Tate module $T_\omega\phi$ is $M(x)^t$ where $t = \dim_{k(\pi)} End\phi \otimes k$. If $t = 1$ as it will be the case in the sequel, then $M(x)$ is the characteristic polynomial of the action of π on $T_\omega\phi$
.

3.2 Dieudonné module of a Drinfeld module

We want now to discuss what the so-called Tate's theory says when one works at the place v defined by the A-characteristic of the Drinfeld module ϕ defined over the finite A-field L.

Let us recall that the Tate's theory at the other places ω, strongly relies on the fact that the polynomial $\phi_{\mathfrak{p}_\omega^n}(x)$ is separable. That means $\phi[\mathfrak{p}_\omega^n]$ (as group scheme) is étale. This is not true anymore at the place v. That difficulty is overcome by considering the notion of Dieudonné modules. Before moving forward, let us recall the following theorem known as Dieudonné-Cartier-Oda theorem.

Theorem 3.2. *Let $m \in \mathbb{N}$ and L be a degree m field extension of $A/\mathfrak{p}_v$. Let K_v be the unique degree m unramified extension of the completion field k_v of k at the place v. Let W be the ring of integers of K_v. Let F and V be indeterminates such that*
$FV = VF = \mathfrak{p}_v$
$F\lambda = \sigma(\lambda)F$ *and* $\lambda V = V\sigma(\lambda) \quad \forall \lambda \in W$
where $\sigma : W \longrightarrow W$ is the unique automorphism induced by the Frobenius $\tau^{\deg \mathfrak{p}_v}$ of L.
There is an anti-equivalence of categories between the category of finite commutative group scheme over L of finite $A/\mathfrak{p}_v$-rank and the category of left $W[F,V]$-modules of finite W-length.

Remark 3.3.

- *Given a finite commutative L-group scheme S of finite $A/\mathfrak{p}_v$-rank, we denote $D(S)$ the corresponding left $W[F,V]$-module of finite W-length.*
- *$D(S)$ is W-free and $rank_{A/\mathfrak{p}_v} S = rank_W D(S)$.*
- *W is also known as the ring of Witt vectors over the field L and since L is finite (and therefore perfect), W is a discrete valuation ring and L is its residue field.*

Definition 3.2 (Dieudonné module at the place v).
Let ψ be a Drinfeld module over the finite A-field L with $m = [L : A/\mathfrak{p}_v]$. The Dieudonné module of ψ is defined by the direct limit

$$T_v\psi := \varinjlim D(\psi[\mathfrak{p}_v^n])$$

where $D(\psi[\mathfrak{p}_v^n])$ is the left $W[F,V]$-module associated to the L-group scheme $\psi[\mathfrak{p}_v^n]$ as mentioned in the previous remark.

The corresponding Tate theorem is given below.

Theorem 3.3. *[Serre-Tate, [11, proposition8.2, corollary 8.3, theorem 8.4]] The canonical map*

$$Hom_L(\phi, \psi) \otimes A_v \xrightarrow{\sim} Hom_{W[F,V]}(T_v\psi, T_v\phi)$$

is a bijection (as morphism of A_v-modules).

Remark 3.4. *[see [11]]*

- *If $\phi = \psi$ then we have $End\psi \otimes A_v \xrightarrow{\sim} End_{W[F,V]}T_v\psi$*
- *We denote $V_v\psi = T_v\psi \otimes K_v$. We have $End\psi \otimes k_v \xrightarrow{\sim} End_{K_v[F,F^{-1}]}V_v\psi$.*
- *$T_v\psi/\mathfrak{p}_v^n T_v\psi$ can be identified to $D(\psi[\mathfrak{p}_v^n])$.*
- *The $W[F,V]$-module $D(\psi[\mathfrak{p}_v^n])$ can be decomposed into its étale and local parts. $D(\psi[\mathfrak{p}_v^n]) = D(\psi[\mathfrak{p}_v^n])_{loc} \oplus D(\psi[\mathfrak{p}_v^n])_{ét}$.*
  Actually the polynomial $\psi_{\mathfrak{p}_v^n}(x) = x^{nh \deg \mathfrak{p}_v} \cdot g_n(x)$ where $g_n(x)$ is a separable polynomial.
  $D(\psi[\mathfrak{p}_v^n])_{loc} = D(\psi[\mathfrak{p}_v^n]_{loc})$ and $D(\psi[\mathfrak{p}_v^n])_{ét} = D(\psi[\mathfrak{p}_v^n]_{ét})$
  where $\psi[\mathfrak{p}_v^n]_{loc} = Spec\left(\overline{L}[x]/\langle x^{nh \deg \mathfrak{p}_v}\rangle\right)$ and $\psi[\mathfrak{p}_v^n]_{ét} = Spec\left(\overline{L}[x]/\langle g_n(x)\rangle\right)$.
  That means the Dieudonné module can also be decomposed as
  $T_v\psi = (T_v\psi)_{loc} \oplus (T_v\psi)_{ét}$.
- *The Frobenius π of ψ acts on $T_v\psi$ via $\pi = F^m$.*
- *F (and therefore $\pi = F^m$) acts on the local part $D(\psi[\mathfrak{p}_v])_{loc}$ as a nilpotent element and acts on the étale part $D(\psi[\mathfrak{p}_v])_{ét}$ as an isomorphism.*

For more details on this part, one can follow [11, §6, 7 and 8].
The following dictionnary can be helpful:

- $Q = \mathbb{F}_q(C) \rightsquigarrow k = \mathbb{F}_q(T)$
- $\Gamma(C', \mathcal{O}_{C'}) \rightsquigarrow A = \mathbb{F}_q[T]$
- $z \rightsquigarrow \mathfrak{p}_v$
- $\mathbb{F}_q[[z]] \rightsquigarrow A_v$
- $\mathcal{O}_S[[z]] \rightsquigarrow W$
- $\mathcal{O}_S[[z]]\left[\frac{1}{z}\right] \rightsquigarrow W[V]$
- Abelian sheaf $\mathcal{F} \rightsquigarrow$ Drinfeld module ϕ
- Dieudonné module $\left(\widehat{\mathcal{F}}, F\right) \rightsquigarrow$ Dieudonné $W[F,V]$-module $T_v\phi$

3.3 Main theorem

Before giving the main theorem, let us lay the groundwork with the following lemmas and remarks.

Lemma 3.1. *Let $M(x) = x^r + a_1 x^{r-1} + \cdots + a_{r-1}x + \mu \mathfrak{p}_v^m$ be a Weil polynomial as described in the previous chapter.*
The height h (see definition 1.17) of the isogeny class defined by $M(x)$ is the sub-degree of the polynomial $M(x) \mod \mathfrak{p}_v$. That is
$M(x) \equiv x^r + a_1 x^{r-1} + \cdots + a_{r-h}x^h \mod \mathfrak{p}_v$.

Proof: Let us first of all recall that the height is an isogeny invariant. That means two isogenous Drinfeld modules share the same height.
Let ψ be a Drinfeld module in our isogeny class. We recall that the Dieudonné module $T_v\psi$ of ψ is a $W[F,V]$-module and the Frobenius endomorphism π acts on it via $\pi = F^m$ as we mentioned before.
$\pi = F^m$ acts W-linearly on the Dieudonné module $T_v\psi$ with the same characteristic polynomial (in A[x]) as it does as A_ω-linear endomorphism of the Tate module $T_\omega\psi$ for any $\omega \neq v$ (see [5, proof of theorem A1.1.1] or replacing Tate modules by Dieudonné modules in the proof of theorem 4 in [17, page 167]).
But the characteristic polynomial of the action of π on the Tate module $T_\omega\psi$ is the minimal polynomial $M(x)$ of π over k (since $End\phi \otimes k = k(\pi)$ see remark 3.2).
Therefore $M(x)$ is also the characteristic polynomial of the action of the Frobenius endomorphism $\pi = F^m$ on the Dieudonné module $T_v\psi$.
One gets from there that $M(x) \mod \mathfrak{p}_v$ is the characteristic polynomial of the action of π on $T_v\psi/\mathfrak{p}_v T_v\psi = D(\psi[\mathfrak{p}_v])$ (see remark 3.4).
As mentioned in remark 3.4, we also know that $D(\psi[\mathfrak{p}_v])$ decomposes (via the corresponding group scheme) into its étale and local parts i.e.
$D(\psi[\mathfrak{p}_v]) = D(\psi[\mathfrak{p}_v])_{loc} \oplus D(\psi[\mathfrak{p}_v])_{\text{ét}}$.
Therefore the characteristic polynomial also splits into

$$M(x) \equiv M_{loc}(x) \cdot M_{\text{ét}}(x) \mod \mathfrak{p}_v$$

where $M_{loc}(x) \mod \mathfrak{p}_v$ (resp. $M_{\text{ét}}(x) \mod \mathfrak{p}_v$) is the characteristic polynomial of the action of π on the local part $D(\psi[\mathfrak{p}_v])_{loc}$ (resp. on the étale part $D(\psi[\mathfrak{p}_v])_{\text{ét}}$). That means,
$\deg(M_{loc}(x) \mod \mathfrak{p}_v) = rank_W D(\psi[\mathfrak{p}_v])_{loc}$ and
$\deg(M_{\text{ét}}(x) \mod \mathfrak{p}_v) = rank_W D(\psi[\mathfrak{p}_v])_{\text{ét}}$
But we have by the definition of the height of ψ (see definition 1.17)

$$\begin{aligned} \psi_{\mathfrak{p}_v} &= \tau^{r\deg\mathfrak{p}_v} + \alpha_1\tau^{r\deg\mathfrak{p}_v - 1} + \cdots + \alpha_{(r-h)\deg\mathfrak{p}_v}\tau^{h\deg\mathfrak{p}_v} \\ &= \left(\tau^{(r-h)\deg\mathfrak{p}_v} + \alpha_1\tau^{(r-h)\deg\mathfrak{p}_v - 1} + \cdots + \alpha_{(r-h)\deg\mathfrak{p}_v}\tau^0\right)\tau^{h\deg\mathfrak{p}_v} \end{aligned}$$

with $\alpha_{(r-h)\deg\mathfrak{p}_v} \neq 0$ That is,
$\psi_{\mathfrak{p}_v}(x)=\left(x^{q^{(r-h)\deg\mathfrak{p}_v}} + \alpha_1 x^{q^{(r-h)\deg\mathfrak{p}_v - 1}} + \cdots + \alpha_{(r-h)\deg\mathfrak{p}_v}\right) x^{q^{h\deg\mathfrak{p}_v}} = g(x)\cdot x^{q^{h\deg\mathfrak{p}_v}}$
where $g(x)$ is a separable polynomial (since $\alpha_{(r-h)\deg\mathfrak{p}_v} \neq 0$) and
$\psi[\mathfrak{p}_v]_{\text{ét}} = Spec\left(\overline{L}[x]/\langle g(x)\rangle\right)$ and $\psi[\mathfrak{p}_v]_{loc} = Spec\left(\overline{L}[x]/\langle x^{q^{h\deg\mathfrak{p}_v}}\rangle\right)$
where $\overline{L}$ is an algebraic closure of L.
As we have mentioned in remark 3.4, π acts on $D\left(\psi[\mathfrak{p}_v]\right)_{loc}$ (resp. $D\left(\psi[\mathfrak{p}_v]\right)_{\text{ét}}$) as a nilpotent element (resp. as an isomorphism). That means the characteristic polynomial $M_{loc}(x) \mod \mathfrak{p}_v$ is a power of x and the characteristic polynomial $M_{\text{ét}}(x) \mod \mathfrak{p}_v$ has only non-zero roots (non-zero eigenvalues). In addition, $\deg\left(M_{\text{ét}}(x) \mod \mathfrak{p}_v\right) = rank_W D\left(\psi[\mathfrak{p}_v]_{\text{ét}}\right) = r-h$ (see remark 3.3).
Therefore

$$M(x) \equiv M_{loc}(x)\cdot M_{\text{ét}}(x) \equiv x^h\left(x^{r-h} + a_1 x^{r-h-1} + \cdots + a_{r-h}\right) \mod \mathfrak{p}_v$$

and the result follows.

$\Diamond$

Corollary 3.2. *Let $M(x)$ be as in the previous lemma.*
$M_{loc}(x)$ is the irreducible factor of $M(x)$ in $k_v[x]$ that describes the unique zero of π in $k(\pi)$

Proof:

- First of all $M_{loc}(x)$ is an irreducible factor of $M(x)$ in $k_v[x]$. Indeed, if $M_{loc}(x) = f_i(x)\cdot f_j(x) \in k_v[x]$ is a product of two irreducible factors of $M(x)$ in $k_v[x]$, then since $M_{loc}(x) \equiv x^h \mod \mathfrak{p}_v$, $f_i(x)$ and $f_j(x)$ would have a common zero modulo $\mathfrak{p}_v$. That is not possible since $M(x)$ is a Weil polynomial.

- If $f_{i_0}(x)$ is the factor of $M(x)$ in $k_v[x]$ describing the zero $\mathfrak{p}_{i_0}$ of π in $k(\pi)$, then the constant coefficient a_{0,i_0} of $f_{i_0}(x)$ must be divisible by $\mathfrak{p}_v$. Indeed,
$v_{i_0}(\pi) > 0$ i.e. $\overline{v}\circ\tau_{i_0}(\pi) > 0$. In other words $\overline{v}(\pi_{i_0}) > 0$,
where π_{i_0} denotes a root of $f_{i_0}(x)$.
That means, $\overline{v}_{|k_v(\pi_{i_0})}(\pi_{i_0}) > 0$ i.e. $v_{i_0}(\pi_{i_0}) > 0$.
As a result $v_{i_0}\left(N_{k_v(\pi_{i_0})/k_v}(\pi_{i_0})\right) > 0$ and thus
$v\left(N_{k_v(\pi_{i_0})/k_v}(\pi_{i_0})\right) > 0$ since $N_{k_v(\pi_{i_0})/k_v}(\pi_{i_0}) \in k_v$.
But the constant coefficient of $f_{i_0}(x)$, $a_{0,i_0} = (-1)^{\deg f_{i_0}(x)} N_{k_v(\pi_{i_0})/k_v}(\pi_{i_0})$.
That means we also have $v(a_{0,i_0}) > 0$ and the claim follows.

- Since $M(x)$ is a Weil polynomial, there must be only one such factor $f_{i_0}(x)$ of $M(x)$ in $k_v[x]$. Since $M_{loc}(x) \equiv x^h \mod \mathfrak{p}_v$, the constant coefficient of $M_{loc}(x)$ in $A_v[x]$ is divisible by $\mathfrak{p}_v$.

Hence $M_{loc}(x) = f_{i_0}(x)$ is the irreducible factor of $M(x)$ in $k_v[x]$ describing the zero $\mathfrak{p}_{i_0}$ of π in $k(\pi)$.

◊

Before moving forward, let us formulate the problem.

Formulation of the problem:

Yu in [26] basically showed that for an isogeny class of rank 2 Drinfeld modules, the orders occurring as endomorphism ring of a Drinfeld module are either (in case the endomorphism algebra is not a field) the maximal orders in the quaternion algebra over k ramified at exactly the places v and ∞, or those orders $\mathcal{O}$ of $k(\pi)$ containing π that are maximal at all the places lying over v i.e. such that $\mathcal{O} \otimes A_v$ is a maximal A_v-order of the k_v-algebra $k_v(\pi)$.
Now the question is: What about Drinfeld modules of higher rank ($r \geq 3$)? Of course for an order $\mathcal{O}$ of (the endomorphism algebra) $k(\pi)$ to be the endomorphism ring of a Drinfeld module, it is necessary that the Frobenius $\pi \in \mathcal{O}$. But must we have $\mathcal{O}$ maximal at all the places of $k(\pi)$ lying over the place v? In other words, must we have $\mathcal{O} \otimes A_v$ maximal A_v-order of the k_v-algebra $k_v(\pi)$? The answer is No! and we provide below an example of a rank 3 Drinfeld module whose endomorphism ring is not at all places of $k(\pi)$ lying over the place v maximal.
Before the example, let us recall the definition and a fact concerning the notion of conductor of an order.

Definition 3.3 (Recall). $A = \mathbb{F}_q[T],\ k = \mathbb{F}_q(T)$
Let F/k be a function field and $\mathcal{O}_{max}$ be the ring of integers of F. Let $\mathcal{O}$ be an A-order of F. The conductor $\mathfrak{c}$ of $\mathcal{O}$ is the maximal ideal of $\mathcal{O}$ which is also an ideal of $\mathcal{O}_{max}$. It is defined by $\mathfrak{c} = \{x \in F \mid x\mathcal{O}_{max} \subseteq \mathcal{O}\}$.

Remark 3.5. *As a very well known fact, $disc\,(\mathcal{O}) = N_{F/k}\,(\mathfrak{c})\, disc\,(\mathcal{O}_{max})$. Where $disc(?)$ denotes the discriminant of a basis of the corresponding free A-lattice and $N_{F/k}(?)$ denotes the norm of the ideal in argument. We recall that if $\mathfrak{P}$ is a prime of F above the prime $\mathfrak{p}$ of k then $N_{F/k}\,(\mathfrak{P}) = \mathfrak{p}^{\mathfrak{f}}$ where $\mathfrak{f}$ denotes the residual degree of $\mathfrak{P} \mid \mathfrak{p}$. In addition $N_{F/k}(?)$ is multiplicative i.e. $N_{F/k}\,(\mathfrak{P}_1\mathfrak{P}_2) = N_{F/k}\,(\mathfrak{P}_1)\, N_{F/k}\,(\mathfrak{P}_2)$.*

Example 3.1.
$A = \mathbb{F}_5[T],\ k = \mathbb{F}_5(T),\ L = \mathbb{F}_{125} = \mathbb{F}_5(\alpha)$ with $\alpha^3 + 3\alpha + 3 = 0$.
$\mathfrak{p}_v = Ker\gamma = \langle T\rangle$. $M(x) = x^3 + (T+1)x^2 + (T^2 + 3T + 4)x + 4T^3$.
One shows using the algorithm 2.1 that $M(x)$ is a Weil polynomial.

$disc\,(M(x)) = T^2(T+4)^2(T^2+4T+2)$. Following the paper [21] one computes the following:
The discriminant of the cubic function field $k(\pi)$ is
$\Delta = disc\,(k(\pi)) = (T+4)^2(T^2+4T+2)$. We set $I = \sqrt{\frac{disc(M(x))}{\Delta}} = T$.
The maximal order of the function field $k(\pi)/k$ is the order generated by $\langle \omega_0, \omega_1, \omega_2 \rangle$, where $\omega_0 = 1$, $\omega_1 = \tilde{\pi} = \pi + 2T + 2$, $\omega_2 = \frac{\alpha_2+\beta_2\tilde{\pi}+\tilde{\pi}^2}{I} = \frac{\alpha_2+\beta_2\tilde{\pi}+\tilde{\pi}^2}{T}$
With

$$\begin{cases} 3\beta_2^2 + c_1 \equiv 0 \mod I \\ \beta_2^3 + c_1\beta_2 + c_2 \equiv 0 \mod I^2 \\ \alpha_2 \equiv -2\beta_2^2 \equiv \frac{2c_1}{3} \mod I \end{cases}$$

Where c_1 and c_2 denote the coefficients of the so-called standard form of the cubic polynomial $M(x)$. We will come back later on to this.
After solving the system, one gets $\beta_2 = 4$ and $\alpha_2 = 3$.
That is, $\omega_2 = \frac{3+4(\pi+2T+2)+(\pi+2T+2)^2}{T}$
We now claim that the conductor $\mathfrak{c}$ of $\mathcal{O} = A[\pi]$ is $\mathfrak{c} = T\cdot\mathcal{O} + (\pi - 3T + 3)\cdot\mathcal{O}$.
Indeed,

$$M(x) \equiv x(x-3T+3)^2 \mod T$$

We also have $(\pi - 3T + 3)(\lambda_0\omega_0 + \lambda_1\omega_1 + \lambda_2\omega_2) \in A[\pi]$ for $\lambda_i \in A$. Because $(\pi - 3T + 3)\omega_2 = (T+1)\pi + 4T^2 + 4T + 3 \in A[\pi]$. That means $\pi - 3T + 3 \in \mathfrak{c}$.
Therefore $T\cdot\mathcal{O} + (\pi - 3T + 3)\cdot\mathcal{O} \subseteq \mathfrak{c} \subsetneq \mathcal{O}$.
Let us consider the canonical morphisms

$$A[\pi] \simeq A[x]/M(x)\cdot A[x] \xrightarrow{\varphi_1} \frac{(A/T\cdot A)[x]}{M(x)\cdot(A/T\cdot A)[x])} \xrightarrow{\varphi_2} \frac{(A/T\cdot A)[x]}{(x-3T+3)\cdot(A/T\cdot A)[x])} \simeq A/T\cdot A$$

$T\cdot\mathcal{O} + (\pi - 3T + 3)\cdot\mathcal{O}$ is a maximal ideal of $\mathcal{O}$ as kernel of the morphism $\varphi_2\circ\varphi_1$ since $A[\pi]/Ker(\varphi_2\circ\varphi_1) \simeq Im(\varphi_2\circ\varphi_1) \simeq A/T\cdot A$ is a field. Therefore $\mathfrak{c} = T\cdot\mathcal{O} + (\pi - 3T + 3)\cdot\mathcal{O}$.
$M(x) \equiv x(x+3)^2 \mod T$. Since $M(x)$ is a Weil polynomial, the irreducible decomposition of $M(x)$ over the completion field k_v is of the form
$M(x) = M_1(x)\cdot M_2(x) \in k_v[x]$. That means $\mathfrak{p}_v = T$ splits into two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in $k(\pi)$.
As a matter of fact, any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ containing T is either
$T\cdot\mathcal{O} + (\pi - 3T + 3)\cdot\mathcal{O}$ or $T\cdot\mathcal{O} + \pi\cdot\mathcal{O}$. Indeed,
First of all $T\cdot\mathcal{O} + (\pi - 3T + 3)\cdot\mathcal{O}$ and $T\cdot\mathcal{O} + \pi\cdot\mathcal{O}$ are maximal ideals of $\mathcal{O} = A[\pi]$ as kernel of the canonical morphisms

$$A[\pi] \simeq A[x]/M(x)\cdot A[x] \xrightarrow{\varphi_1} \frac{(A/T\cdot A)[x]}{M(x)\cdot(A/T\cdot A)[x])} \xrightarrow{\varphi_2} \frac{(A/T\cdot A)[x]}{(x-3T+3)\cdot(A/T\cdot A)[x])} \simeq A/T\cdot A$$

and

$$A[\pi] \simeq A[x]/M(x) \cdot A[x] \xrightarrow{\varphi_1'} \frac{(A/T \cdot A)[x]}{M(x) \cdot (A/T \cdot A)[x])} \xrightarrow{\varphi_2'} \frac{(A/T \cdot A)[x]}{x \cdot (A/T \cdot A)[x])} \simeq A/T \cdot A$$

respectively.
Since $M(x) \equiv x(x - 3T + 3)^2 \mod T$ *and* $M(\pi) = 0$*, we have* $\pi(\pi - 3T + 3)^2 \in T \cdot A[\pi] \subseteq \mathfrak{p}$*. But* $\mathfrak{p}$ *is a prime ideal of* $\mathcal{O}$*. That means* $\pi \in \mathfrak{p}$ *or* $\pi - 3T + 3 \in \mathfrak{p}$*. In other words*
$T \cdot \mathcal{O} + (\pi - 3T + 3) \cdot \mathcal{O} \subseteq \mathfrak{p}$ *or* $T \cdot \mathcal{O} + \pi \cdot \mathcal{O} \subseteq \mathfrak{p}$
From the maximality of these ideals we conclude that
$\mathfrak{p} = T \cdot \mathcal{O} + (\pi - 3T + 3) \cdot \mathcal{O}$ *or* $\mathfrak{p} = T \cdot \mathcal{O} + \pi \cdot \mathcal{O}$.
We assume then WLOG that $\mathfrak{p}_2 \cap \mathcal{O} = T \cdot \mathcal{O} + (\pi - 3T + 3) \cdot \mathcal{O} = \mathfrak{c}$.
That is, $\mathfrak{p}_2 \mid \mathfrak{c}$ *and* $\mathfrak{p}_1 \nmid \mathfrak{c}$.
The norm of the conductor is
$N_{k(\pi)/k}(\mathfrak{c}) = T^2$ *since* $disc\,(M(x)) = T^2 \cdot disc\,(k(\pi))$.
Therefore we have only two possibilities for orders occurring as endomorphism of a Drinfeld module: $A[\pi]$ *and the maximal order* $\mathcal{O}_{max}$*. This is due to the fact that the norm of the conductor of any order* $\mathcal{O}$ *containing properly* $A[\pi]$ *(i.e.* $A[\pi] \subsetneq \mathcal{O} \subseteq \mathcal{O}_{max}$*) is a square of a proper divisor of* T^2 *and thus must be a unit. In other words* $disc(\mathcal{O}) = disc\,(\mathcal{O}_{max})$*. i.e.* $\mathcal{O} = \mathcal{O}_{max}$*.*
After some computations (using a code we implemented in the computer algebra system SAGE) we found the following:

- *For* $\phi_T = -\alpha^2\tau^3 + 2\alpha^2\tau^2 + \alpha^2\tau$ *we have:*

  $$\omega_2 = \frac{3 + 4(\tau^3 + 2\phi_T + 2) + (\tau^3 + 2\phi_T + 2)^2}{\phi_T} \in L\{\tau\} \text{ and } \phi_T \cdot \omega_2 = \omega_2 \cdot \phi_T.$$

  In other words $\omega_2 \in End\phi$*. Therefore* $End\phi = \mathcal{O}_{max}$*.*

- *For* $\psi_T = \tau^3 + \tau^2 + \tau$ *we have:*

  $$\omega_2 = \frac{3 + 4(\tau^3 + 2\psi_T + 2) + (\tau^3 + 2\psi_T + 2)^2}{\psi_T} \notin L\{\tau\} \text{ and a fortiori } \omega_2 \notin End\psi.$$

  Since we have only two possibilities for $End\psi$*, we can conclude that* $End\psi = A[\pi]$*.*
  $A[\pi]$ *is therefore the endomorphism ring of a Drinfeld module but* $A[\pi]$ *is not maximal at at least one of the places of* $k(\pi)$ *lying over the place* v *because its conductor* $\mathfrak{c}$ *is not relatively prime to* $\mathfrak{p}_v = T$*.*

One can notice in the example above that $M_{loc}(x) = M_1(x) \equiv x \mod \mathfrak{p}_v$. That means $\deg M_{loc}(x) = 1$. Thus any order containing π is maximal at the corresponding place v_1 (which represent the zero of π in $k(\pi)$).
Concerning the étale part,
$M_{\text{ét}}(x) = M_2(x) \equiv (x+3)^2 \mod \mathfrak{p}_v$. i.e. $\deg M_{\text{ét}}(x) = 2$.
We have then here "enough" $\mathfrak{p}_v$-torsion points.
This example already encodes some tips for the generalization.

Definition 3.4. *[10, remark 4.7.12.1][recall]*
Let ϕ and ψ be two isogenous Drinfeld modules over L. Let $u : \phi \longrightarrow \psi$, $u \in L\{\tau\}$ be an isogeny from ϕ to ψ.
ψ is called the quotient of the Drinfeld module ϕ by the kernel G of u and denoted $\psi := \phi/G$.

Lemma 3.2. *Let ϕ be a Drinfeld module over the finite A-field L whose endomorphism algebra is a field i.e. $End\phi \otimes k = k(\pi)$, where π is the Frobenius endomorphism of ϕ. Let $\mathcal{O}$ be an A-order of $k(\pi)$ containing π. We choose a place ω of k different from v.*
If $End\phi \otimes A_\omega \ncong \mathcal{O} \otimes A_\omega$ as A_ω-module then there exists a Drinfeld module quotient $\psi = \phi/G_{\mathcal{L}}$ such that
$End\psi \otimes A_\omega \cong \mathcal{O} \otimes A_\omega$ and $End\psi \otimes A_\nu \cong End\phi \otimes A_\nu$ for all places $\nu \neq \omega$.

Proof: With the hypotheses of the lemma,
let us assume that $End\phi \otimes A_\omega \ncong \mathcal{O} \otimes A_\omega$. We are looking for an isogeny u that changes (via its kernel) the Drinfeld module ϕ into a Drinfeld module ψ so that the endomorphism ring of the resulting Drinfeld module coincides at ω with $\mathcal{O}$.
$\mathcal{O}$ is an A-order of $k(\pi)$ containing π. That means $\mathcal{O} \otimes A_\omega$ is an A_ω-order of the k_ω-algebra $k_\omega(\pi) = End\phi \otimes k_\omega$. We also know from the corollary 3.1 of the Tate theorem that there is a canonical isomorphism of k_ω-algebras $End\phi \otimes k_\omega \overset{\sim}{\longrightarrow} End_{k_\omega[\pi]} V_\omega\phi$, where $V_\omega\phi = T_\omega\phi \otimes k_\omega$.
Since in addition $\pi \in \mathcal{O}$, $V_\omega\phi$ therefore contains an A_ω-lattice $\mathcal{L}$ containing $T_\omega\phi$ and stable under the action of π such that the corresponding order $End_{A_\omega[\pi]}\mathcal{L} \cong \mathcal{O} \otimes A_\omega$ as A_ω-modules. We consider then such an A_ω-lattice $\mathcal{L}$. We have then $T_\omega\phi \subseteq \mathcal{L} \subseteq V_\omega\phi$.
Let $(t_1; \cdots, t_r)$ be an A_ω-basis of $T_\omega\phi$ and $(z_1, \cdots, z_r)$ be an A_ω-basis of $\mathcal{L}$, where $r = rank\phi$. M_0 denotes the matrix in $\mathscr{M}_{r\times r}(A_\omega)$ such that

$$\begin{pmatrix} t_1 \\ \vdots \\ t_r \end{pmatrix} = M_0 \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix}$$

Let $s = \omega\,(detM_0)$ be the valuation (wrt ω) of the determinant $detM_0$. $detM_0 = \alpha_0 \mathfrak{p}_\omega^s$, where $\mathfrak{p}_\omega$ is the uniformizing element of the place ω and α_0 is a unit in A_ω. The reader can notice that $s > 0$ because $End\phi \otimes A_\omega \ncong \mathcal{O} \otimes A_\omega$. We consider the following map

$$\begin{array}{ccc} Co(M_0)^t : T_\omega\phi & \longrightarrow & \mathcal{L} \\ \begin{pmatrix} t_1 \\ \vdots \\ t_r \end{pmatrix} & \longmapsto & \alpha_0 \mathfrak{p}_\omega^s \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} \end{array}$$

The kernel of this map is $kerCo(M_0)^t = M_0 \cdot \phi[\mathfrak{p}_\omega^s]$.

We recall that $Co(M_0)^t$ (as one can guess) denotes the transpose of the comatrix of the matrix M_0.

Indeed,

if $\lambda_1 t_1 + \cdots + \lambda_r t_r \in M_0 \cdot \phi[\mathfrak{p}_\omega^s]$ then

$Co(M_0)^t \cdot (\lambda_1 t_1 + \cdots + \lambda_r t_r) \in Co(M_0)^t \cdot M_0 \cdot \phi[\mathfrak{p}_\omega^s] = \mathfrak{p}_\omega^s \cdot \phi[\mathfrak{p}_\omega^s] = \{0\}$.

That is, $Co(M_0)^t \cdot (\lambda_1 t_1 + \cdots + \lambda_r t_r) = 0$ and thus

$\lambda_1 t_1 + \cdots + \lambda_r t_r \in KerCo(M_0)^t$.

Conversely if $\lambda_1 t_1 + \cdots + \lambda_r t_r \in KerCo(M_0)^t$ then $Co(M_0)^t \cdot (\lambda_1 t_1 + \cdots + \lambda_r t_r) = 0$ i.e. $\alpha_0 \mathfrak{p}_\omega^s\,(\lambda_1 z_1 + \cdots + \lambda_r z_r) = 0$ and therefore $\lambda_1 z_1 + \cdots + \lambda_r z_r \in \phi[\mathfrak{p}_\omega^s]$.

That means $\lambda_1 t_1 + \cdots + \lambda_r t_r = M_0 \cdot (\lambda_1 z_1 + \cdots + \lambda_r z_r) \in M_0 \cdot \phi[\mathfrak{p}_\omega^s]$.

Hence $kerCo(M_0)^t = M_0 \cdot \phi[\mathfrak{p}_\omega^s]$.

Applying the first isomorphism theorem to the morphism of A_ω-modules, one gets $T_\omega\phi / M_0 \cdot \phi[\mathfrak{p}_\omega^s] \cong Im\,(Co(M_0)^t) = \langle \mathfrak{p}_\omega^s z_1, \cdots, \mathfrak{p}_\omega^s z_r \rangle$.

Let $\mathcal{L}_s = \langle \mathfrak{p}_\omega^s z_1, \cdots, \mathfrak{p}_\omega^s z_r \rangle$ be the A_ω-lattice generated by $(\mathfrak{p}_\omega^s z_1, \cdots, \mathfrak{p}_\omega^s z_r)$.

$T_\omega\phi / M_0 \cdot \phi[\mathfrak{p}_\omega^s] \cong \mathcal{L}_s = \mathfrak{p}_\omega^s \cdot \mathcal{L}$.

We set $G_\mathcal{L} = M_0 \cdot \phi[\mathfrak{p}_\omega^s]$ and we consider the Drinfeld module quotient $\psi = \phi / G_\mathcal{L}$ defined over L.

The existence of the Drinfeld module ψ is guaranteed by the fact that the separable additive polynomial

$$u = x \prod_{\alpha \in G_\mathcal{L}} \left(1 - \frac{x}{\alpha}\right)$$

whose kernel $G_\mathcal{L}$ (which is stable under the action of the Frobenius endomorphism π mainly because $\pi \in \mathcal{O}$), lie in $L\{\tau\}$ (see [10, proposition 1.1.5 and corollary 1.2.2]), in addition to the fact that the local part of the group scheme $H = Spec\,\big(\overline{L}[x]/\langle u(x) \rangle\big)$ is trivial because $u \in L\{\tau\}$ is separable (see [10, proposition 4.7.11, for t=0]).

We have then $T_\omega\psi \cong T_\omega\phi / M_0 \cdot \phi[\mathfrak{p}_\omega^s] \cong \mathcal{L}_s = \mathfrak{p}_\omega^s \cdot \mathcal{L}$ as A_ω-modules.

Since $G_\mathcal{L} = M_0 \cdot \phi[\mathfrak{p}_\omega^s]$ and $\mathcal{L}$ are stable under the action of π, so are $T_\omega\psi$ and

$\mathcal{L}_s$. In other words $T_\omega\psi \cong \mathcal{L}_s$ as $A_\omega[\pi]$-modules.
That means $End_{A_\omega[\pi]}T_\omega\psi \cong End_{A_\omega[\pi]}\mathcal{L}_s$.
One also easily checks that (since $\mathcal{L}_s = \mathfrak{p}_\omega^s \cdot \mathcal{L}$) $\mathcal{L}$ and $\mathcal{L}_s$ generate the same order i.e. $End_{A_\omega}\mathcal{L}_s = End_{A_\omega}\mathcal{L}$.
Therefore $End_{A_\omega[\pi]}T_\omega\psi \cong End_{A_\omega[\pi]}\mathcal{L}$. Applying the Tate theorem 3.1, one gets then $End\psi \otimes A_\omega \cong End_{A_\omega[\pi]}T_\omega\psi \cong End_{A_\omega[\pi]}\mathcal{L} \cong \mathcal{O} \otimes A_\omega$.
At all the other places $\nu \neq \omega, v$ of k, we have the following:
$0 \longrightarrow G_\mathcal{L} = M_0 \cdot \phi[\mathfrak{p}_\omega^s] \hookrightarrow \phi \xrightarrow{u} \psi \longrightarrow 0$ is an exact sequence.
$G_\mathcal{L}$ has no non-trivial $\mathfrak{p}_\nu$-torsion points. Applying the Tate theorem at the place ν to this short exact sequence, one gets the exact sequence
$0 \longrightarrow T_\nu\phi \longrightarrow T_\nu\psi \longrightarrow 0$. That means $T_\nu\phi \cong T_\nu\psi$ as A_ν-modules.
In other words $End\psi \otimes A_\nu \cong End_{A_\nu[\pi]}T_\nu\psi \cong End_{A_\nu[\pi]}T_\nu\phi \cong End\phi \otimes A_\nu$.

◊

Lemma 3.3. *Let ϕ be a Drinfeld module over the finite A-field L whose endomorphism algebra $End\phi \otimes k = k(\pi)$ is a field, where π denotes the Frobenius endomorphism of ϕ. Let $\mathcal{O}$ be an A-order of $k(\pi)$ containing π and such that $\mathcal{O}$ is maximal at the unique zero v_0 of π in $k(\pi)$ lying over the place v of k.*
If $\mathcal{O} \otimes A_v \ncong End\phi \otimes A_v$ then there exists a quotient Drinfeld module $\psi = \phi/G_\mathcal{L}$ such that
$End\psi \otimes A_v \cong \mathcal{O} \otimes A_v$ and $End\psi \otimes A_\omega \cong End\phi \otimes A_\omega$ at all the other places $\omega \neq v$ of k.

Proof: With the hypothesis of the lemma,
we assume that $End\phi \otimes A_v \ncong \mathcal{O} \otimes A_v$ as A_v-modules. That means there must exist at least one other place $v_1 \neq v_0$ of $k(\pi)$ lying over the place v of k (i.e. ϕ is not supersingular) such that the completion $\mathcal{O}_{v_1}$ of $\mathcal{O}$ at the place v_1 is different from the completion $(End\phi)_{v_1}$ of $End\phi$ at that same place v_1.
Let $v_0,\ v_1, \cdots, v_s$ be the places of $k(\pi)$ lying over the place v of k. We choose v_0 here to be the unique zero of π in $k(\pi)$ lying over the place v.
We are looking for a quotient Drinfeld module $\psi = \phi/G_\mathcal{L}$ such that
$End\psi \otimes A_v \cong \mathcal{O} \otimes A_v$ and $End\psi \otimes A_\omega \cong End\phi \otimes A_\omega$ at all the other places $\omega \neq v$.
The idea here is to act on the étale part of the Dieudonné module $T_v\phi$ of ϕ so that the resulting endomorphism ring meets our needs.
Let then $M(x)$ be the minimal polynomial (Weil polynomial) of π over k.
We know that the places $v_0,\ v_1, \cdots, v_s$ are described by the irreducible factors of $M(x)$ in $k_v[x]$. Let then $M(x) = M_0(x) \cdot M_1(x) \cdots M_s(x) \in k_v[x]$ be the irreducible decomposition of $M(x)$ over the completion field k_v.
We also know that the irreducible factor $M_0(x) =: M_{loc}(x)$ describing the zero v_0 of π in $k(\pi)$ is the characteristic polynomial of the action of π on the

local part of the Dieudonné module $(T_v\phi)_{loc}$ (see corollary 3.2).
In addition, $M_0(x) \equiv x^h \mod \mathfrak{p}_v$, where h is the height of ϕ (see lemma 3.1).
$M_{\text{ét}}(x) = M_1(x) \cdots M_s(x)$ is the characteristic polynomial of the action of π on the étale part of the Dieudonné module $(T_v\phi)_{\text{ét}}$. In this case, we therefore clearly see that $rank_W\,(T_v\phi)_{\text{ét}} = \deg M_{\text{ét}}(x) \geq 2$. Because if we had $\deg M_{\text{ét}}(x) = 0$, ϕ would be supersingular and if we had $\deg M_{\text{ét}}(x) = 1$, $End\phi \otimes A_v$ and $\mathcal{O} \otimes A_v$ would be both maximal orders of the k_v-algebra $k_v(\pi)$ and thus we would have
$End\phi \otimes A_v \cong \mathcal{O} \otimes A_v$, which in either case contradicts our assumption.
We recall the notation K_v which is the unique degree m unramified extension of k_v and W its ring of integers.
We know that $\mathcal{O} \otimes A_v = \prod\limits_{v_i|v} \mathcal{O}_{v_i}$ is an A_v-order of the k_v-algebra
$k_v(\pi) = End\phi \otimes k_v \cong End_{K_v[F,V]}V_v\phi$ (see remark 3.4).
i.e. $\mathcal{O} \otimes A_v \subseteq k_v(\pi) \cong End_{K_v[F,V]}V_v\phi$.
Also, $\mathcal{O}$ is maximal at v_0 i.e. the completion $\mathcal{O}_{v_0}$ is the maximal order of the field $k_v(\pi_0) = k_v[x]/M_0(x) \cdot k_v[x]$.
Thus there exists a W-lattice $\mathcal{L}_0$ of $(V_v\phi)_{\text{ét}} = (T_v\phi)_{\text{ét}} \otimes K_v$ containing $(T_v\phi)_{\text{ét}}$ stable under the actions of F and V,
(i.e. $T_v\phi = (T_v\phi)_{loc} \oplus (T_v\phi)_{\text{ét}} \subseteq (T_v\phi)_{loc} \oplus \mathcal{L}_0 \subseteq V_v\phi = (V_v\phi)_{loc} \oplus (V_v\phi)_{\text{ét}}$)
such that the corresponding order $End_W\left((T_v\phi)_{loc} \oplus \mathcal{L}_0\right) \cong \mathcal{O} \otimes A_v$.
We set $l = r - h = \deg M_{\text{ét}}(x) \geq 2$. Let $(t_1, \cdots, t_l)$ be a W-basis of $(T_v\phi)_{\text{ét}}$ and $(z_1, \cdots, z_l)$ be a W-basis of $\mathcal{L}_0$. N_0 denotes the matrix in $\mathscr{M}_{l\times l}(W)$ such that

$$\begin{pmatrix} t_1 \\ \vdots \\ t_l \end{pmatrix} = N_0 \begin{pmatrix} z_1 \\ \vdots \\ z_l \end{pmatrix}$$

Let $s_0 = v\,(detN_0)$. Since $End\phi \otimes A_v \cong End_{W[F,V]}T_v\phi \ncong \mathcal{O} \otimes A_v$, $s_0 \geq 1$.
Since K_v is an unramified extension of k_v and the corresponding ring of integers W is a discrete valuation ring, we keep (by abuse of language) the same notation v for the place of K_v extending the place v of k_v. $\mathfrak{p}_v$ denotes the corresponding prime.
$\det N_0 = \beta_0 \mathfrak{p}_v^{s_0}$, where β_0 is a unit in W. The same way we did before, let us consider the morphism

$$\begin{array}{rcl} Co(N_0)^t : (T_v\phi)_{\text{ét}} & \longrightarrow & \mathcal{L}_0 \\ \begin{pmatrix} t_1 \\ \vdots \\ t_l \end{pmatrix} & \longmapsto & Co(N_0)^t \begin{pmatrix} t_1 \\ \vdots \\ t_l \end{pmatrix} = \beta_0 \mathfrak{p}_v^{s_0} \begin{pmatrix} z_1 \\ \vdots \\ z_l \end{pmatrix} \end{array}$$

where $Co(N_0)^t$ denotes the transpose of the co-matrix of N_0. We recall that

$Co(N_0)^t \cdot N_0 = \det N_0 \cdot IdentityMatrix.$
The kernel of $Co(N_0)^t$ is given by $Ker\,(Co(N_0)^t) = N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$.
$D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$ is the $W[F,V]$-module associated to the group-scheme $\phi[\mathfrak{p}_v^{s_0}]_{\text{ét}}$ (see remark 3.3). Indeed,
Let $\lambda_1 t_1 + \cdots + \lambda_l t_l \in N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$. We have then,
$Co(N_0)^t{\cdot}(\lambda_1 t_1 + \cdots + \lambda_l t_l) \in Co(N_0)^t{\cdot}N_0{\cdot}D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}} = \mathfrak{p}_v^{s_0}{\cdot}D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}{=}\{0\}$.
We recall that $D\,(\phi[\mathfrak{p}_v^n])$ can be identified to $T_v\phi/\mathfrak{p}_v^n \cdot T_v\phi$ for any $n \in \mathbb{N}$.
Conversely, let $\lambda_1 t_1{+}\cdots{+}\lambda_l t_l \in Ker\,(Co(N_0)^t)$ i.e. $Co(N_0)^t{\cdot}(\lambda_1 t_1 + \cdots + \lambda_l t_l){=}0$
That means $\beta_0 \mathfrak{p}_v^{s_0}(\lambda_1 z_1 + \cdots + \lambda_l z_l) = 0$ and then
$\lambda_1 z_1 + \cdots + \lambda_l z_l \in D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$.
But $\lambda_1 t_1 + \cdots + \lambda_l t_l = N_0 \cdot (\lambda_1 z_1 + \cdots + \lambda_l z_l) \in N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$.
Therefore $Ker\,(Co(N_0)^t) = N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$.
Applying the first isomorphism theorem to our morphism, one gets that
$(T_v\phi)_{\text{ét}}\,/N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}} \cong Im\,(Co(N_0)^t) = \langle \mathfrak{p}_v^{s_0} z_1, \cdots, \mathfrak{p}_v^{s_0} z_l \rangle$.
Let $\mathcal{L}_{s_0}$ be the W-lattice generated by $(\mathfrak{p}_v^{s_0} z_1, \cdots, \mathfrak{p}_v^{s_0} z_l)$.
i.e. $(T_v\phi)_{\text{ét}}\,/N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}} \cong \mathcal{L}_{s_0}$.
$N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$ is stable under the actions of F and V because N_0 commutes with the actions of F and V (via the stability of $(T_v\phi)_{\text{ét}}$ and $\mathcal{L}_0$ under those actions) and $D\,(\phi[\mathfrak{p}_v^{s_0}])$ is by definition stable under those actions (see theorem 3.2).
Let G_{s_0} be the finite commutative L-group scheme associated to the $W[F,V]$-module $N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$ (theorem 3.2). We consider the additive separable polynomial

$$u = x \prod_{\substack{\alpha \in G_{s_0} \\ \alpha \neq 0}} \left(1 - \frac{x}{\alpha}\right)$$

whose kernel is G_{s_0}. By definition, G_{s_0} is stable under the action of $\pi = F^m$. For the same reason as the case $\omega \neq v$ in lemma 3.2, $u \in L\{\tau\}$ and u is an isogeny from the Drinfeld module ϕ to a Drinfeld module ψ. That is, $\phi_T \cdot u = u \cdot \psi_T$. In fact $\psi := \phi/G_{s_0}$.
The Dieudonné module of ψ is given as follows:
$T_v\psi = T_v\,(\phi/G_{s_0}) \cong T_v\phi/D(G_{s_0}) = ((T_v\phi)_{loc} \oplus (T_v\phi)_{\text{ét}})\,/N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}}$.
That is,
$T_v\psi \cong (T_v\phi)_{loc} \oplus (T_v\phi)_{\text{ét}}\,/N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}])_{\text{ét}} \cong (T_v\phi)_{loc} \oplus \mathcal{L}_{s_0}$
One easily checks that since $\mathcal{L}_{s_0} = \mathfrak{p}_v^{s_0} \cdot \mathcal{L}_0$, $End_W \mathcal{L}_{s_0} = End_W \mathcal{L}_0$.
Therefore $End_W\,((T_v\phi)_{loc} \oplus \mathcal{L}_{s_0}) \cong End_W\,((T_v\phi)_{loc} \oplus \mathcal{L}_0) \cong \mathcal{O} \otimes A_v$ and from the stability under the actions of F and V, one gets
$\mathcal{O} \otimes A_v \cong End_{W[F,V]}\,((T_v\phi)_{loc} \oplus \mathcal{L}_0) \cong End_{W[F,V]}\,((T_v\phi)_{loc} \oplus \mathcal{L}_{s_0}) \cong End_{W[F,V]} T_v\psi$
Hence $\mathcal{O} \otimes A_v \cong End\psi \otimes A_v$ (Thanks to the Tate's theorem 3.3).

At all the other places $\omega \neq v$ we have the exact sequence

$$0 \longrightarrow G_{s_0} \hookrightarrow \phi \xrightarrow{u} \psi = \phi/G_{s_0} \longrightarrow 0$$

Applying the Tate's theorem at the place ω, we get

$$0 \longrightarrow T_\omega\phi \longrightarrow T_\omega\psi \longrightarrow 0$$

In fact by definition of the Dieudonné functor in theorem 3.2 and from the Lagrange theorem for finite group scheme, we have the following:
If $r_0 = rank\,(N_0 \cdot D\,(\phi[\mathfrak{p}_v^{s_0}]))$ then $\mathfrak{p}_v^{r_0} \cdot G_{s_0} = \{0\}$ i.e. $G_{s_0} \subseteq \phi[\mathfrak{p}_v^{r_0}]$. That means the Tate module $T_\omega G_{s_0} = \{0\}$ for any place $\omega \neq v$.
Hence we get from the above exact sequence that $T_\omega\phi \cong T_\omega\psi$.
In other words
$End\phi\otimes A_\omega \cong End_{A_\omega[\pi]}T_\omega\phi \cong End_{A_\omega[\pi]}T_\omega\psi \cong End\psi\otimes A_\omega$.

Theorem 3.4. *$A = \mathbb{F}_q[T]$, $k = \mathbb{F}_q(T)$ and $\mathfrak{p}_v$ is the (generator of the) kernel of the characteristic morphism $\gamma : A \longrightarrow L$ defining the finite A-field L.*
$M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu\mathfrak{p}_v^m \in A[x]$ is a Weil polynomial, where $m = [L : A/\mathfrak{p}_v \cdot A]$. Let $\mathcal{O}$ be an A-order of the function field
$k(\pi) = k[x]/M(x)\cdot k[x]$. Let v_0 be the unique zero of π in $k(\pi)$ lying over the place v of k.
$\mathcal{O}$ is the endomorphism ring of a Drinfeld module in the isogeny class defined by the Weil polynomial $M(x)$ if and only if $\mathcal{O}$ contains π and $\mathcal{O}$ is maximal at the place v_0.

Proof: With the hypotheses of the theorem, we have the following:
$\boxed{\Rightarrow}$ If $\mathcal{O} = End\phi$ then it is clear that $\mathcal{O}$ contains the Frobenius endomorphism π. Yu proved in [26] that $End\phi$ is maximal at the zero v_0 of π in $k(\pi)$.

$\boxed{\Leftarrow}$ Conversely, let us assume that $\mathcal{O}$ contains π and $\mathcal{O}$ is maximal at the place v_0.
Let ϕ be any Drinfeld module over L in the isogeny class defined by $M(x)$.
We know that $\mathcal{O}$ and $End\phi$ differ at only finitely many places, since both are orders of the same function field $k(\pi)$. That means there exist finitely many places $\omega_1, \cdots, \omega_s$ such that
$\mathcal{O}\otimes A_\omega \cong End\phi\otimes A_\omega$ for all places ω except (may be) at $\omega \in \{v,\ \omega_1,\ \omega_2, \cdots, \omega_s\}$.
For $\omega = \omega_1$, one can get from lemma 3.2 a Drinfeld module ϕ_1 defined over L such that
$End\phi_1 \otimes A_{\omega_1} \cong \mathcal{O} \otimes A_{\omega_1}$ and
$End\phi_1 \otimes A_\nu \cong End\phi \otimes A_\nu$ at all other places $\nu \neq \omega_1, v$.
That means $End\phi_1 \otimes A_\omega \cong \mathcal{O} \otimes A_\omega$ for all places ω of k except (may be) at

$\omega \in \{v,\ \omega_2,\ \omega_3, \cdots, \omega_s\}$.
Repeating the process at all the places ω_i, one gets from lemma 3.2 a Drinfeld module φ defined over L such that
$End\varphi \otimes A_\omega \cong \mathcal{O} \otimes A_\omega$ for all places ω of k with $\omega \neq v$.
Concerning the place v, we know in addition that $\mathcal{O}$ is maximal at the unique zero v_0 of π in $k(\pi)$ lying over the place v.
We can therefore apply lemma 3.3 and get the following:

- If φ (equivalently our isogeny class) is supersingular, then we already have $End\varphi \otimes A_v \cong \mathcal{O} \otimes A_v$ as maximal order of the k_v-algebra (which is actually in this case a field) $k_v(\pi)$.

- If φ (equivalently our isogeny class) is not supersingular and
  $End\varphi \otimes A_v \ncong \mathcal{O} \otimes A_v$, then there exists (see lemma 3.3) a Drinfeld module $\psi = \varphi/G_{\mathcal{L}}$ such that
  $End\psi \otimes A_v \cong \mathcal{O} \otimes A_v$ and
  $End\psi \otimes A_\omega \cong End\varphi \otimes A_\omega \cong \mathcal{O} \otimes A_\omega$ at all the other places $\omega \neq v$.
  In any case, we get a Drinfeld module ψ such that
  $End\psi \otimes A_\omega \cong \mathcal{O} \otimes A_\omega$ at all the places ω of k.
  Hence $\mathcal{O} = End\psi$.

◊

CHAPTER 4

L-isomorphism classes of Drinfeld modules defined over a finite field L

We keep the same notations,
$\mathbb{F}_q$ is a finite field with q elements.
$A = \mathbb{F}_q[T]$ is the ring of polynomials with coefficients in $\mathbb{F}_q$.
L is a finite A-field defined by an $\mathbb{F}_q$-algebra homomorphism $\gamma : A \longrightarrow L$.
$L\{\tau\}$ is the twisted ring of Ore polynomials.

Introduction

While going through the Drinfeld modules theory, one can notice the wonderful resemblance with elliptic curves. This resemblance has been a great source of inspiration for mathematician involved in that theory. It is for instance known from the elliptic curves theory that, two elliptic curves defined over a field L are isomorphic over $\overline{L}$ if and only if they have the same J-invariant. Potemine has proved this result in [19] for the case of Drinfeld module, after having defined the notion of J-invariants of a rank r Drinfeld A-module. It is also known from theory of elliptic curve that Hasse invariants and j-invariants determine the L-isomorphism class of an elliptic curve. Likewise in the theory of Drinfeld modules, we define in the sequel the notion of fine isomorphy invariants for any rank r Drinfeld A-module. Afterwards, we prove that the fine isomorphy invariants together with J-invariants determine the L-isomorphism class of a rank r Drinfeld A-module.

4.1 Isomorphism invariants

Definition 4.1 (Fine Isomorphy Invariant).
Let $\phi : A \longrightarrow L\{\tau\}$ be a rank r Drinfeld A-module defined by

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

We set

$$d = gcd(q^k - 1,\ k \in I) = q^\delta - 1$$

where $I = \{i = 1, \cdots, r;\ g_i \neq 0\}$ and $\delta = gcd(k :\ k \in I)$.
We write $d = \sum_{k\in I} \lambda_k(q^k - 1)$; $\lambda_k \in \mathbb{Z}$ and we set $\lambda = (\lambda_k)_{k\in I}$.
Let $B = \left\{\alpha = (\alpha_k)_{k\in I},\ \ d = \sum_{k\in I} \alpha_k(q^k - 1)\right\}$.
The fine isomorphy invariant of ϕ is defined as $FI(\phi) = (FI_\lambda(\phi))_{\lambda\in B}$, where

$$FI_\lambda(\phi) = \prod_{k\in I} g_k^{\lambda_k}\ modL^{*d}$$

Example 4.1. *Let $\phi : A \longrightarrow L\{\tau\}$ be a rank 2 Drinfeld module defined by $\phi_T = \gamma(T) + g_1\tau + g_2\tau^2$. We assume $g_1 \neq 0$ and $g_2 \neq 0$. We know from Bezout's lemma that if $a,\ b \in \mathbb{Z}$ and $d = gcd(a, b)$, then there exists α_0 and β_0 integers such that $d = \alpha_0 a + \beta_0 b$. All the other Bezout's coefficients of d are given by $\begin{cases} \alpha_k = \alpha_0 + k\frac{b}{d} \\ \beta_k = \beta_0 - k\frac{a}{d} \end{cases} \quad k \in \mathbb{Z}$*
Let's come back to our Drinfeld module $\phi_T = \gamma(T) + g_1\tau + g_2\tau^2$.
$d = gcd(q - 1, q^2 - 1) = q - 1$.
$d = q - 1 = -q(q - 1) + 1(q^2 - 1)$. The complete list of Bezout's coefficients of d is given by: $\begin{cases} \alpha_k = -q + k(q + 1) = (k - 1)q + k \\ \beta_k = 1 - k \end{cases} \quad k \in \mathbb{Z}$.
Therefore the fine isomorphy invariant of ϕ is given by

$$FI(\phi) = \left(g_1^{(k-1)q+k}.g_2^{1-k}\ \left(modL^{*(q-1)}\right)\right)_{k\in\mathbb{Z}}$$

Definition 4.2. *[19, J-Invariants]*
Let $(k_1, \cdots, k_l)$ be a tuple with $1 \leq k_1 < \cdots < k_l \leq r - 1$ and $\delta_1, \cdots, \delta_l$ be integers such that

a) $\delta_1(q^{k_1} - 1) + \cdots + \delta_l(q^{k_l} - 1) = \delta_r(q^r - 1)$.

b) $0 \leq \delta_i \leq \frac{q^r-1}{q^{gcd(i,r)}-1}$. *for* $i = 1, \cdots, l$.

c) $gcd(\delta_1, \cdots, \delta_l, \delta_r) = 1$

The so-called basic J-invariants of the Drinfeld module ϕ *are defined as*

$$J^{\delta_1 \cdots \delta_l}_{k_1 \cdots k_l}(\phi) = \frac{g_{k_1}^{\delta_1} \cdots g_{k_l}^{\delta_l}}{g_r^{\delta_r}}$$

4.2 Main theorems

Theorem 4.1. *We keep the same notation above and we consider* ϕ *and* $\psi : A \longrightarrow L\{\tau\}$ *as two rank r Drinfeld A-modules defined by*

$$\phi_T = \gamma(T) + g_1\tau + \cdots + g_r\tau^r \text{ and } \psi_T = \gamma(T) + g'_1\tau + \cdots + g'_r\tau^r$$

. *The followings are equivalent*

(i) $\phi \overset{L}{\cong} \psi$

(ii) $\phi \overset{L^{sep}}{\cong} \psi$ *and* $\exists \lambda \in B, \quad FI_\lambda(\phi) = FI_\lambda(\psi)$

(iii) $\phi \overset{L^{sep}}{\cong} \psi$ *and* $FI(\phi) = FI(\psi)$

Proof: Our plan is to prove following the loop $(iii) \Rightarrow (ii) \Rightarrow (i) \Rightarrow (iii)$. Let's assume (iii). It obviously implies (ii) since $B \neq \emptyset$.

Let's now assume for the second part of the proof that $\phi \overset{L^{sep}}{\cong} \psi$ and $\exists \lambda = (\lambda_k)_{k \in I} \in B$ such that $FI_\lambda(\phi) = FI_\lambda(\psi)$.

We want to show that $\phi \overset{L}{\cong} \psi$.

$\phi \overset{L^{sep}}{\cong} \psi$ implies that there exists $x \in L^{sep}$ such that $\psi_T = x^{-1}\phi_T x$.
That is

$$\text{for all } \ k \in I, \ g'_k = g_k x^{q^k-1} \tag{4.1}$$

$FI_\lambda(\phi) = FI_\lambda(\psi)$ implies $\prod\limits_{k\in I} g'^{\lambda_k}_k = \prod\limits_{k\in I} g^{\lambda_k}_k \ modL^{*d}$. That is

$$\text{there is } y \in L^* \text{ such that } \prod_{k\in I} g'^{\lambda_k}_k = \prod_{k\in I} g^{\lambda_k}_k .y^d. \tag{4.2}$$

From equation (4.1) we get $g'^{\lambda_k}_k = g^{\lambda_k}_k x^{\lambda_k(q^k-1)}$ for all $k \in I$
Thus

$$\prod_{k\in I} g'^{\lambda_k}_k = \prod_{k\in I} g^{\lambda_k}_k .x^{\sum\limits_{k\in I}\lambda_k(q^k-1)} = \prod_{k\in I} g^{\lambda_k}_k .x^d \tag{4.3}$$

The equations (4.2) and (4.3) imply that $x^d = y^d$.
But $d = gcd(q^k - 1,\ k \in I)$. That is for all $k \in I$, there exists $\alpha_k \in \mathbb{Z}$ such that $q^k - 1 = \alpha_k d$.
Hence $x^{q^k-1} = x^{\alpha_k d} = \left(x^d\right)^{\alpha_k} = \left(y^d\right)^{\alpha_k} = y^{\alpha_k d} = y^{q^k-1}$.
Thus $\forall\ k \in I\ \ g'_k = g_k x^{q^k-1} = g_k y^{q^k-1}$.
Therefore $\psi_T = y^{-1}\phi_T y$ and $y \in L^*$.
Hence $\phi \overset{L}{\cong} \psi$
For the last part of the proof we consider (i). That is $\phi \overset{L}{\cong} \psi$. It obviously implies also that $\phi \overset{L^{sep}}{\cong} \psi$.
Let's now check that $FI(\phi) = FI(\psi)$.
$\phi \overset{L}{\cong} \psi$ implies that there exists $x \in L$ such that $\psi_T = x^{-1}\phi_T x$.
That is, for all $k \in I$, $g'_k = g_k x^{q^k-1}$. From The Bezout's lemma $B \neq \emptyset$. Let's then pick any $\lambda = (\lambda_k)_{k\in I} \in B$. We have $g'^{\lambda_k}_k = g^{\lambda_k}_k x^{\lambda_k(q^k-1)}$.
Thus

$$\prod_{k\in I} g'^{\lambda_k}_k = \prod_{k\in I} g^{\lambda_k}_k \prod_{k\in I} x^{\lambda_k(q^k-1)} = \prod_{k\in I} g^{\lambda_k}_k . x^{\sum\limits_{k\in I}\lambda_k(q^k-1)} = \prod_{k\in I} g^{\lambda_k}_k . x^d$$

Therefore $\prod\limits_{k\in I} g'^{\lambda_k}_k = \prod\limits_{k\in I} g^{\lambda_k}_k . x^d,\ x \in L^*$.
Which implies $\prod\limits_{k\in I} g'^{\lambda_k}_k = \prod\limits_{k\in I} g^{\lambda_k}_k\ modL^{*d}$
Hence $FI_\lambda(\phi) = FI_\lambda(\psi)$.
Since λ has been picked randomly, we can conclude that
$FI_\lambda(\phi) = FI_\lambda(\psi)\ \ \forall\lambda \in B$.
Therefore $FI(\phi) = FI(\psi)$. $\Diamond$

Remark 4.1. *In the sequel, we might at some point abuse the language by considering as fine isomorphy invariants of ϕ, $FI_{\lambda_0}(\phi) \equiv FI(\phi)$ for some $\lambda_0 \in B$. As we can notice from the theorem above, this will not have any impact on the generality.*

Remark 4.2. *Potemine proved in [19, Theorem 2.2] that*

$$\phi \overset{L^{sep}}{\cong} \psi \Leftrightarrow J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\phi) = J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\psi)\ \textit{ for any } (k_1,\cdots,k_l) \textit{ and } (\delta_1,\cdots,\delta_l)$$

as defined above.
Taking it into account, one can reformulate the theorem 4.1 as follows.

Theorem 4.2.

$$\phi \overset{L}{\cong} \psi \Leftrightarrow J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\phi) = J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\psi)\ \textit{ and } FI(\phi) = FI(\psi)$$

In other words, L-isomorphism classes of Drinfeld modules defined over the finite A-field L are determined by their fine isomorphy invariants and J-invariants.

Example 4.2. *For the case of rank 2 Drinfeld A-modules, the only basic J-invariant is* $J_1^{q+1} = \frac{g_1^{q+1}}{g_2}$*. Here* $d = \begin{cases} \gcd(q-1, q^2-1) = q-1 & if\ g_1 \neq 0 \\ q^2 - 1 & if\ g_1 = 0 \end{cases}$

Therefore $\lambda_1 = \begin{cases} -q & if\ g_1 \neq 0 \\ 0 & if\ g_1 = 0 \end{cases}$ *and* $\lambda_2 = 1$ *in any case.*

Thus $FI(\phi) = \begin{cases} g_1^{-q} g_2 \mod L^{*q-1} & if\ g_1 \neq 0 \\ g_2 \mod L^{*q^2-1} & if\ g_1 = 0 \end{cases}$

The invariants J_1^{q+1} *and* $FI(\phi)$ *match clearly with the invariants describing the isomorphism classes of a rank 2 Dinfeld module as shown by Gekeler in [8].*

Example 4.3. *Let's consider a rank 3 Drinfeld A-module defined over the field* $L = \mathbb{F}_{25} = \mathbb{F}_5(\alpha)$ *with* $\alpha^2 + 4\alpha + 2 = 0$*. We take* $A = \mathbb{F}_5[T]$*. L is an A-field defined by the ring homomorphism* $\gamma : A \longrightarrow L,\ T \mapsto \alpha$*.*
Let $\phi_T = \alpha + g_1\tau + g_2\tau^2 + g_3\tau^3$*.*
Following the definition 4.2, one can easily compute the basic J-invariants of ϕ *which are:*
$J_{1,2}^{31,0}(\phi),\ J_{1,2}^{1,5}(\phi),\ J_{1,2}^{7,4}(\phi),\ J_{1,2}^{8,9}(\phi),\ J_{1,2}^{9,14}(\phi),\ J_{1,2}^{10,19}(\phi),\ J_{1,2}^{11,24}(\phi),\ J_{1,2}^{12,29}(\phi)$
$J_{1,2}^{13,3}(\phi),\ J_{1,2}^{15,13}(\phi),\ J_{1,2}^{17,23}(\phi),\ J_{1,2}^{19,2}(\phi),\ J_{1,2}^{20,7}(\phi),\ J_{1,2}^{22,17}(\phi),\ J_{1,2}^{23,22}(\phi),\ J_{1,2}^{25,1}(\phi)$
$J_{1,2}^{27,11}(\phi),\ J_{1,2}^{29,21}(\phi),\ J_{1,2}^{31,31}(\phi),$

The fine isomorphy invariant of ϕ *is given by*

$$FI(\phi) = \begin{cases} g_1\ modL^{*4} & if\ g_1 \neq 0 \\ \frac{g_3}{g_2^5}\ modL^{*4} & if\ g_1 = 0\ and\ g_2 \neq 0 \\ g_3\ modL^{*124} & if\ g_1 = g_2 = 0 \end{cases}$$

Therefore the isomorphism class of ϕ *is parametrized by those 20 invariants*

Remark 4.3. *For Drinfeld modules of a given rank defined over a finite field, Potemine proved in [19] that the number of isomorphism classes is given by:*

$$\#Cl(D^r/L) = q^{n_r} - 1 + \sum_{(i_1,\cdots,i_s)\in I_0} \left(q^{gcd(i_1,\cdots,i_s,n_r)} - 1\right)(q^n - 1)^s + (q-1)\left[q^{(r-1)n} - q^{r-\varphi(n_r,r)n}\right]$$

Where $n = [L : \mathbb{F}_q]$*,* $n_r = gcd(n, r)$*.* I_0 *is the power set of* $\{1, \cdots, r\}$ *and* $I_1 \subset I_0$ *is made up of subsets* $(i_1, \cdots, i_s)$ *such that* $gcd(i_1, n_r) > 1, \cdots, gcd(i_s, n_r) > 1$*.* $\varphi(n_r, r)$ *is the number of integers* $< r$ *and coprime with* n_r*.*

Remark 4.4. *Each isomorphism class has a finite number of elements. Indeed* $\#Cl(\phi) \leq \#L^{*d}$.

We provide in the sequel an algorithm generating the isomorphism classes of rank r Drinfeld modules in a given isogeny class.

Algorithm 4.1. *[Isomorphism classes of a Drinfeld modules]*
Inputs*:* $M(x) = x^r + a_1(T)x^{r-1} + \cdots + a_{r-1}(T)x + \mu Q(T)$.
Ouputs*: Isomorphism classes of Drinfeld modules in the isogeny class defined by* $M(x)$

1- *Set* $\phi_T = g_r\tau^r + \cdots + g_1\tau + \gamma(T)$ *and solve the equation (system of equations) given by* $\tau^{sr} + a_1(\phi_T)\tau^{s(r-1)} + \cdots + a_{r-1}(\phi_T)\tau^s + \mu Q(\phi_T) = 0$. *Where* $s = [L : \mathbb{F}_q]$. *Let* Γ *be the set of all solutions of that equation.*

2- *Pick a Drinfeld module* $\phi \in \Gamma$. *We assume* $\phi_T = g_r\tau^r + \cdots + g_1\tau + \gamma(T)$.

3- *Compute the fine isomorphy invariant and the* J*-invariants of* ϕ. *i.e.* $FI(\phi)$ *and* $J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\phi)$.

4- *for* ψ *in* Γ*: Compute* $FI(\psi)$ *and* $J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\psi)$.
If $FI(\psi) = FI(\phi)$ *and* $J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\psi) = J^{\delta_1\cdots\delta_l}_{k_1\cdots k_l}(\phi)$*:*
Then store ψ *in the isomorphism class of* ϕ.

5- *Pick another* ϕ *in* Γ *which is not in the previously computed isomorphism classes and move to step 3.*

6- *If the set* Γ *is exhausted then output the isomorphism classes and exit.*

Remark 4.5. *This algorithm also works for any isogeny class defined by a Weil polynomial of the form*

$$M(x) = x^{r_1} + a_1x^{r_1-1} + \cdots + a_{r_1-1}x + \mu Q^{1/r_2} \text{ with } r = r_1r_2 \text{ and } r_2 \mid m.$$

CHAPTER 5

Application: Explicit description for the cases of rank 3 and rank 4 Drinfeld modules

We aim in this chapter (as indicated by the title) to describe explicitly (for the cases of rank 3 and rank 4 Drinfeld modules) the isogeny classes, to list the endomorphism rings corresponding to a given isogeny class and provide an example of computation for L-isomorphism classes in a given isogeny class of Drinfeld modules defined over the finite field L.

5.1 Explicit description for rank 3 Drinfeld modules

5.1.1 Isogeny classes of rank 3 Drinfeld modules

We keep the same data as before. That is $A = \mathbb{F}_q[T],\ k = \mathbb{F}_q(T)$ with a distinguished place at infinity ∞. $Q = \mathfrak{p}_v^m$ is a power of a prime element $\mathfrak{p}_v$ of A.
As we have seen before, the isogeny classes are given by the following rank 3 Weil polynomials:

- $M(x) = x^3 + a_1x^2 + a_2x + \mu Q \in A[x]$ with $\mu \in \mathbb{F}_q$. Where $\deg a_1 \leq \frac{\deg Q}{3}$ and $\deg a_2 \leq \frac{2\deg Q}{3}$ such that the resultant modulo $\mathfrak{p}_v$ of any two irreducible factors $M(x) \mod \mathfrak{p}_v^n$ is non-zero and $\overline{M_0(x)} \equiv x^3 + \frac{a_1}{T^s}x^2 + \frac{a_2}{T^{2s}}x + \mu\frac{Q}{T^{3s}} \mod \frac{1}{T^h}$ is irreducible.
  Where $h = v_\infty\left(disc\left(M(x)\right)\right) + sr(r-1) + 1$ and $n = v\left(disc\left(M(x)\right)\right) + 1$ (see algorithm 2.1).

- $M(x) = x - \mu Q^{\frac{1}{3}}$ with $3|m$ and $\mu \in \mathbb{F}_q^*$

We provide in the sequel some results that help to quickly identify rank 3 Weil polynomials and therefore improve for this special case algorithm 2.1.

Definition 5.1 (Standard form)**.**
Let $k(\tilde{\pi})/k$ be a cubic function field. The minimal polynomial $M_0(x) \in A[x]$ of $\tilde{\pi}$ is said to be in the standard form if $M_0(x) = x^3 + ax + b$ with a and $b \in A$ satisfying the following:

$$\textit{There is no } c \in A \textit{ such that } c^2|a \textit{ and } c^3|b.$$

Remark 5.1. *Let $M(x) = x^3+a_1x^2+a_2x+\mu Q$ be a potential Weil polynomial whose corresponding cubic field is $k(\pi)/k$.*
If $char(k) \neq 3$, setting $x = y - \frac{a_1}{3}$, one can transform

$$M(x) = x^3 + a_1x^2 + a_2x + \mu Q$$

into a polynomial of the form

$$y^3 + b_1y + b_2 \in A[y] \textit{ where } b_1 = \frac{-a_1^2}{3} + a_2,\ b_2 = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + \mu Q.$$

Using the algorithm 4.1 in [15]. One can therefore convert the polynomial $N(y) = y^3 + b_1y + b_2 \in A[y]$ into a standard polynomial $x^3 + c_1x + c_2$. By "converting" we mean getting from the irreducible polynomial $y^3+b_1y+b_2$ an irreducible polynomial in the standard form $M_0(x) = x^3+c_1x+c_2$ whose any root $\tilde{\pi}$ is such that $k(\tilde{\pi}) \backsimeq k(\pi)$ (i.e. $k(\tilde{\pi})$ and $k(\pi)$ define the same field).
In fact doing it, is really a simple exercise. One takes the square-free factorizations of b_1 and b_2. That is $b_1 = \mu_1 \prod_{i=1}^{n_1} b_{1i}^i$ and $b_2 = \mu_2 \prod_{j=1}^{n_2} b_{2j}^j$ where $\mu_1,\ \mu_2 \in \mathbb{F}_q$ and b_{1i} $i = 1, \cdots, n_1$ (resp. b_{2j} $j = 1, \cdots, n_2$) are pairwise coprime square-free elements of A. We set $g_1 = \prod_{i=1}^{n_1} b_{1i}^{\lfloor \frac{i}{2} \rfloor}$ and $g_2 = \prod_{j=1}^{n_2} b_{2j}^{\lfloor \frac{j}{3} \rfloor}$.
Taking $c_1 = \frac{b_1}{\gcd(g_1,g_2)^2}$ and $c_2 = \frac{b_2}{\gcd(g_1,g_2)^3}$, we have that $M_0(x) = x^3+c_1x+c_2$ is a polynomial in the standard form in $A[x]$. In addition we have the following:
π is a root of $M(x)$ if and only if $\pi + \frac{a_1}{3}$ is a root of $N(y) = y^3 + b_1y + b_2$ if and only if $\tilde{\pi} = \frac{\pi+\frac{a_1}{3}}{\gcd(g_1,g_2)}$ is a root of $M_0(x) = x^3 + c_1x + c_2$.
Therefore $disc\,(M(x)) = disc\,(N(y))$ and $ind(\pi) = ind\left(\pi + \frac{a_1}{3}\right)$.
But $ind(\tilde{\pi}) = \frac{ind(\pi)}{\gcd(g_1,g_2)^3}$ because $disc\,(M_0(x)) = \frac{disc(M(x))}{\gcd(g_1,g_2)^6}$.
Also, $k(\pi) = k\left(\pi + \frac{a_1}{3}\right) = k(\tilde{\pi})$.

As a consequence of proposition 2.2 in the special case of the degree 3 polynomial $M_0(x)$ in the standard form, we have the following:

Proposition 5.1.
Let $M_0(x) = x^3 + c_1x + c_2$ be the standard form of the minimal polynomial $M(x)$ of π.
There is a unique place of $k(\pi)$ above the place at infinity ∞ of k only in the following cases.

($s1$) $3\deg c_1 < 2\deg c_2,\ \deg c_2 \equiv 0 \mod 3$ *and $LC(c_2)$ is not a cube in $\mathbb{F}_q$. $LC(?)$ denotes here the leading coefficient of the argument.*

($s2$) $3\deg c_1 = 2\deg c_2,\ 4LC(c_1)^3 + 27LC(c_2)^2 \neq 0$ *and* $x^3 + LC(c_1)x + LC(c_2)$ *has no root in $\mathbb{F}_q$.*

($s3$) $3\deg c_1 < 2\deg c_2$ *and* $\deg c_2 \not\equiv 0 \mod 3$

In order to show it, let us first of all get rid of all the cases where $3\deg c_1 > 2\deg c_2$ through the following lemma.

Lemma 5.1. *Let $\tilde{\pi}$ be a root of the irreducible polynomial $M_0(x) = x^3 + c_1x + c_2 \in A[x]$ in the standard form. We consider the cubic function field $k(\tilde{\pi})/k$.*
If there is a unique place of $k(\tilde{\pi})$ above the place at infinity ∞ of k then $3\deg c_1 \leq 2\deg c_2$.

Proof: Let us assume that $3\deg c_1 > 2\deg c_2$.
$k(\tilde{\pi}) = \mathbb{F}_q(T)(\tilde{\pi}) = \mathbb{F}_q(\tilde{\pi})(T)$. T is a root of the irreducible polynomial $N_0(y) = c_2(y) + c_1(y)\tilde{\pi} + \tilde{\pi}^3$. We can therefore consider the field extension $\mathbb{F}_q(\tilde{\pi})(T)/\mathbb{F}_q(\tilde{\pi})$ whose degree is $[\mathbb{F}_q(\tilde{\pi})(T) : \mathbb{F}_q(\tilde{\pi})] = max\{\deg c_1, \deg c_2\}$.
$c_2(T) + c_1(T)\tilde{\pi} + \tilde{\pi}^3 = 0$. Thus for any prime $\mathfrak{p}$ above ∞

$$3v_{\mathfrak{p}}(\tilde{\pi}) \geq min\{-e_{\mathfrak{p}}\deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}),\ -e_{\mathfrak{p}}\deg c_2\}$$

where $e_{\mathfrak{p}}$ denotes the ramification index of the extension $\mathfrak{p} \mid \infty$.
If $-e_{\mathfrak{p}}\deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}) > -e_{\mathfrak{p}}\deg c_2$ then we have $3v_{\mathfrak{p}}(\tilde{\pi}) = -e_{\mathfrak{p}}\deg c_2$ i.e. $v_{\mathfrak{p}}(\tilde{\pi}) = -\frac{e_{\mathfrak{p}}\deg c_2}{3}$ That is,
$-e_{\mathfrak{p}}\deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}) = -e_{\mathfrak{p}}\left(\deg c_1 + \frac{\deg c_2}{3}\right) > -e_{\mathfrak{p}}\deg c_2$.
In other words $\deg c_1 + \frac{\deg c_2}{3} < \deg c_2$.
This contradicts the fact that $3\deg c_1 > 2\deg c_2$. That means we have $-e_{\mathfrak{p}}\deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}) < -e_{\mathfrak{p}}\deg c_2$ i.e. $3v_{\mathfrak{p}}(\tilde{\pi}) = -e_{\mathfrak{p}}\deg c_1 + v_{\mathfrak{p}}(\tilde{\pi})$ and then $v_{\mathfrak{p}}(\tilde{\pi}) = -\frac{e_{\mathfrak{p}}\deg c_1}{2}$ or,
$-e_{\mathfrak{p}}\deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}) = -e_{\mathfrak{p}}\deg c_2$ i.e. $v_{\mathfrak{p}}(\tilde{\pi}) = e_{\mathfrak{p}}(\deg c_1 - \deg c_2)$. But

(i) If $v_{\mathfrak{p}}(\tilde{\pi}) = -\frac{e_{\mathfrak{p}} \deg c_1}{2}$ for all primes $\mathfrak{p} \mid \infty$ then we have
$$\sum_{\mathfrak{p}\mid\infty} v_{\mathfrak{p}}(\tilde{\pi}) f_{\mathfrak{p}} = -\sum_{\mathfrak{p}\mid\infty} e_{\mathfrak{p}} f_{\mathfrak{p}} \frac{\deg c_1}{2} = -\frac{\deg c_1}{2} \sum_{\mathfrak{p}\mid\infty} e_{\mathfrak{p}} f_{\mathfrak{p}} = -\frac{3\deg c_1}{2}$$

(ii) If $v_{\mathfrak{p}}(\tilde{\pi}) = e_{\mathfrak{p}}\left(\deg c_1 - \deg c_2\right)$ for all primes $\mathfrak{p} \mid \infty$ then
$$\sum_{\mathfrak{p}\mid\infty} v_{\mathfrak{p}}(\tilde{\pi}) f_{\mathfrak{p}} = \left(\deg c_1 - \deg c_2\right) \sum_{\mathfrak{p}\mid\infty} e_{\mathfrak{p}} f_{\mathfrak{p}} = 3\left(\deg c_1 - \deg c_2\right)$$

We also know that $v_{\mathfrak{q}}(\tilde{\pi}) \geq 0$ for all finite primes $\mathfrak{q}$ since $\tilde{\pi}^3 + c_1\tilde{\pi} + c_2 = 0$ with c_1 and $c_2 \in A = \mathbb{F}_q[T]$. That means the poles of $\tilde{\pi}$ lie over the place ∞. In other words the degree of the pole divisor of $\tilde{\pi}$ is,
$\deg\left((\tilde{\pi})_\infty\right) = -\sum_{\mathfrak{p}\mid\infty} v_{\mathfrak{p}}(\tilde{\pi}) f_{\mathfrak{p}} = [\mathbb{F}_q(\tilde{\pi})(T) : \mathbb{F}_q(\tilde{\pi})] = max\{\deg c_1, \deg c_2\}$ (see [20, prop 5.1]). $f_{\mathfrak{p}}$ denotes here the residual (or relative) degree of $\mathfrak{p} \mid \infty$.
Thus $\sum_{\mathfrak{p}\mid\infty} v_{\mathfrak{p}}(\tilde{\pi}) f_{\mathfrak{p}} = -max\{\deg c_1, \deg c_2\}$.

Unfortunately (i) cannot occur because $-\frac{3\deg c_1}{2} \neq -max\{\deg c_1, \deg c_2\}$ since $3\deg c_1 > 2\deg c_2$ and $\frac{3\deg c_1}{2} \neq \deg c_1$
Also (ii) cannot occur since $3(\deg c_1 - \deg c_2) \neq -max\{\deg c_1, \deg c_2\}$ because,
If $max\{\deg c_1, \deg c_2\} = \deg c_2$ then $3(\deg c_1 - \deg c_2) \neq -\deg c_2$ since $3\deg c_1 > 2\deg c_2$.
If $max\{\deg c_1, \deg c_2\} = \deg c_1$ then $3(\deg c_1 - \deg c_2) \neq -\deg c_1$ since $3(\deg c_1 - \deg c_2) \geq 0$ (because by hypothesis $\deg c_1 \geq \deg c_2$) and $-\deg c_1 < 0$ (because $3\deg c_1 > 2\deg c_2$).
Hence if $3\deg c_1 > 2\deg c_2$ then there must be at least two primes above the place at infinity ∞. Some for which $v_{\mathfrak{p}}(\tilde{\pi}) = -\frac{e_{\mathfrak{p}} \deg c_1}{2}$ and other for which $v_{\mathfrak{p}}(\tilde{\pi}) = e_{\mathfrak{p}}\left(\deg c_1 - \deg c_2\right)$. ◊

Proof: [Proof of the proposition 5.1]
According to the previous lemma, we can have a unique place above the place at infinity ∞ only when $3\deg c_1 \leq 2\deg c_2$.
The statements $(s1)$ and $(s2)$ are direct consequences of the the proposition 2.2 where $h = 1$.
Let us now focus on the last statement $(s3)$
The proof follows the same idea like the one of the former lemma.
We know that $\tilde{\pi}^3 + c_1\tilde{\pi} + c_2 = 0$ i.e. $3v_{\mathfrak{p}}(\tilde{\pi}) \geq min\{-e_{\mathfrak{p}} \deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}),\ -e_{\mathfrak{p}} \deg c_2\}$.
If $-e_{\mathfrak{p}} \deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}) < -e_{\mathfrak{p}} \deg c_2$ then $3v_{\mathfrak{p}}(\tilde{\pi}) = -e_{\mathfrak{p}} \deg c_1 + v_{\mathfrak{p}}(\tilde{\pi})$
i.e. $v_{\mathfrak{p}}(\tilde{\pi}) = -\frac{e_{\mathfrak{p}} \deg c_1}{2}$
Thus $-e_{\mathfrak{p}} \deg c_1 + v_{\mathfrak{p}}(\tilde{\pi}) = -e_{\mathfrak{p}}\left(\deg c_1 + \frac{\deg c_1}{2}\right) < -e_{\mathfrak{p}} \deg c_2$.

i.e. $-\frac{3e_{\mathfrak{p}}\deg c_1}{2} < -e_{\mathfrak{p}}\deg c_2$ which contradicts the fact that $3\deg c_1 < 2\deg c_2$. Therefore for some prime $\mathfrak{p}$ above the place ∞ we must have $v_{\mathfrak{p}}(\tilde{\pi}) = -\frac{e_{\mathfrak{p}}\deg c_2}{3}$. Hence if $\deg c_2 \not\equiv 0 \mod 3$ i.e. $3 \nmid \deg c_2$ then we must have $3 \mid e_{\mathfrak{p}}$ since $v_{\mathfrak{p}}(\tilde{\pi})$ is an integer. But $1 \leq e_{\mathfrak{p}} \leq 3$. Hence $e_{\mathfrak{p}} = 3$. Therefore such a prime is the unique one above ∞ since $3 = \sum_{\mathfrak{q}|\infty} e_{\mathfrak{q}} f_{\mathfrak{q}}$. ◊

For more details about the signature of the place at infinity in a cubic function field in general, one can have a look at [2, theorem 2.1.4].
What about the condition 2 of definition 2.1 concerning the zero of π above the place v? In the following, we work that condition out and provide a lighter way to check if it is satisfied by $M(x)$ or not.

Proposition 5.2. *Let $M(x) = x^3 + a_1x^2 + a_2x + \mu\mathfrak{p}_v^m \in A[x]$ be as mentioned before.*

1. *If $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \nmid a_1$ then there is a unique zero of π in $k(\pi)$ above the place v if and only if $v(a_2) \geq \frac{m}{2}$.*
2. *If $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \mid a_1$ then there is a unique zero of π in $k(\pi)$ above the place v if and only if there is a unique place of $k(\pi)$ above v (i.e. if and only if $M(x)$ is irreducible over the completion field k_v).*
3. *If $\mathfrak{p}_v \nmid a_2$ then there is a unique zero of π in $k(\pi)$ above v.*

Before proving this proposition, let us recall the following lemma, known as Hensel lemma or Hensel lifting.

Lemma 5.2. *Let $M(x) \in A[x]$ and $\mathfrak{p}$ be a prime in A. Let $m, n \in \mathbb{N}$ with $m \leq n$*

- *If $M(x_0) \equiv 0 \mod \mathfrak{p}^n$ and $M'(x_0) \not\equiv 0 \mod \mathfrak{p}$ then there exists a unique lifting of x_0 modulo $\mathfrak{p}^{n+m}$. i.e. there exists a unique $x_1 \in A$ such that $M(x_1) \equiv 0 \mod \mathfrak{p}^{n+m}$ and $x_1 \equiv x_0 \mod \mathfrak{p}^n$.*
- *If $M(x_0) \equiv 0 \mod \mathfrak{p}^n$ and $M'(x_0) \equiv 0 \mod \mathfrak{p}$ then we have two possibilities:*
  - *If $M(x_0) \not\equiv 0 \mod \mathfrak{p}^{n+1}$ then there is no lifting of x_0 modulo $\mathfrak{p}^{n+1}$.*
  - *If $M(x_0) \equiv 0 \mod \mathfrak{p}^{n+1}$ then every lifting of x_0 modulo $\mathfrak{p}^{n+1}$ is a zero of $M(x)$ modulo $\mathfrak{p}^{n+1}$.*

Proof:[Proof of proposition 5.2]

1. We assume here that $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \nmid a_1$.

   $\boxed{\Rightarrow}$ We assume that there is a unique zero of π in $k(\pi)$ above v.

   $M(x) \equiv x^2(x+a_1) \mod \mathfrak{p}_v$ and $\mathfrak{p}_v \nmid a_1$. That means 0 (as double root) and $-a_1$ are the roots of $M(x)$ module $\mathfrak{p}_v$.
   Using the Hensel lemma 5.2, one can lift these roots modulo $\mathfrak{p}_v^l$ (for $l \geq 1$) as long as $M(0) \equiv 0 \mod \mathfrak{p}_v^l$.
   We know that $disc\,(M(x)) = (a_1^2 - 4a_2)a_2^2 + \mathfrak{p}_v^m(-4a_1^3 - 27\mathfrak{p}_v^m + 18a_1a_2)$
   Let us assume that $v(a_2) < \frac{m}{2}$.
   That means $v(a_2^2) < m$. Since $\mathfrak{p}_v \nmid a_1$ and $\mathfrak{p}_v \mid a_2$, $v(a_1^2 - 4a_2) = 0$ and $v(-4a_1^3 - 27\mathfrak{p}_v^m + 18a_1a_2) = 0$. In other word

   $$v\,(disc\,(M(x))) = v(a_2^2) < m.$$

   For any $n \in \mathbb{N}$ with $n \leq m$, $M(0) \equiv 0 \mod \mathfrak{p}_v^n$. One can therefore lift the root $x_0 = 0$ modulo $\mathfrak{p}_v$ to roots modulo $\mathfrak{p}_v^n$ for $n = v(a_2^2) + 1$ and the (simple) root $x_1 = -a_1$ modulo $\mathfrak{p}_v$ to a root modulo $\mathfrak{p}_v^n$. One gets then

   $$M(x) \equiv M_1(x) \cdot M_2(x) \cdot M_3(x) \mod \mathfrak{p}_v^{v(disc(M(x)))+1}$$

   With $M_1(x) \equiv M_2(x) \equiv x \mod \mathfrak{p}_v$ and $M_3(x) \equiv x + a_1 \mod \mathfrak{p}_v$.
   Thus $Res\,(M_1(x), M_2(x)) \equiv 0 \mod \mathfrak{p}_v$ which contradicts the fact that there is a unique zero of π in $k(\pi)$ above v (see proposition 2.4 and corollary 2.1).
   Therefore $v(a_2) \geq \frac{m}{2}$.

   $\boxed{\Leftarrow}$ Let us assume conversely that $v(a_2) \geq \frac{m}{2}$. We want to show that there is a unique zero of π in $k(\pi)$ above v.
   We recall that $disc\,(M(x)) = (a_1^2 - 4a_2)a_2^2 + \mathfrak{p}_v^m(-4a_1^3 - 27\mathfrak{p}_v^m + 18a_1a_2)$.
   $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \nmid a_1$ implies that $v(a_1^2 - 4a_2) = v(-4a_1^3 - 27\mathfrak{p}_v^m + 18a_1a_2) = 0$. In addition, $v(a_2^2) = 2v(a_2) \geq m$. Thus $v\,(disc\,(M(x))) \geq m$.
   But $M(x) \equiv x^2(x + a_1) \mod \mathfrak{p}_v$ with $\mathfrak{p}_v \nmid a_1$.
   The root $x_0 = 0$ of $M(x) \mod \mathfrak{p}_v$ can be lifted to a root of $M(x) \mod \mathfrak{p}_v^n$ for $n \leq m$. But since for $n \geq m + 1$ $M(0) \not\equiv 0 \mod \mathfrak{p}_v^n$, there is no lifting of x_0 to a root of $M(x) \mod \mathfrak{p}_v^n$ (see Hensel lemma 5.2). In other words, we cannot have $M(x) \equiv M_1(x) \cdot M_2(x) \cdot M_3(x) \mod \mathfrak{p}_v^{v(disc(M(x)))+1}$ with $M_1(x) \equiv M_2(x) \equiv x \mod \mathfrak{p}_v$ and $M_3(x) \equiv x + a_1 \mod \mathfrak{p}_v$.
   Therefore we are only left with the possibility
   $M(x) \equiv M_1(x) \cdot M_2(x) \mod \mathfrak{p}_v^{v(disc(M(x)))+1}$ with
   $M_1(x) \equiv x^2 \mod \mathfrak{p}_v$ and $M_2(x) \equiv x + a_1 \mod \mathfrak{p}_v$ (see [24, Corollary 2.4]). We therefore clearly have $Res\,(M_1(x), M_2(x)) \not\equiv 0 \mod \mathfrak{p}_v$ since $\mathfrak{p}_v \nmid a_1$.
   Hence there is a unique zero of π in $k(\pi)$ above the place v.

2. we assume here that $\mathfrak{p}_v \mid a_1$ and $\mathfrak{p}_v \mid a_2$.
   $M(\pi) = 0$ implies that $\pi^3 = -a_1\pi^2 - a_2\pi - \mu\mathfrak{p}_v^m = \mathfrak{p}_v\left(-b_1\pi^2 - b_2\pi - \mu\mathfrak{p}_v^{m-1}\right)$ where $a_i = b_i \cdot \mathfrak{p}_v$. In other words $\mathfrak{p}_v$ divides π. That means any place of $k(\pi)$ above v is a zero of π.
   Therefore there is a unique zero of π in $k(\pi)$ above v if and only if there is a unique place of $k(\pi)$ above v.

3. This case has already been shown in proposition 2.6.

$\diamondsuit$

We summarize our previous results in the following theorem.

Theorem 5.1. *Let $M(x) = x^3 + a_1x^2 + a_2x + \mu\mathfrak{p}_v^m \in A[x]$ be a potential Weil polynomial. i.e. $\deg a_i \leq \frac{im \deg \mathfrak{p}_v}{3}$ and $M(x)$ irreducible over k. We also consider $M_0(x) = x^3 + c_1x + c_2$ the standard form of $M(x)$.*

1. *There is a unique place of $k(\pi)$ lying over the place at ∞ of k if and only if one of the following holds.*

   $(s1)$ $3\deg c_1 < 2\deg c_2,\ \deg c_2 \equiv 0 \mod 3$ *and $LC(c_2)$ is not a cube in $\mathbb{F}_q$.*

   $(s2)$ $3\deg c_1 = 2\deg c_2,\ 4LC(c_1)^3 + 27LC(c_2)^2 \neq 0$ *and* $x^3 + LC(c_1)x + LC(c_2)$ *has no root in $\mathbb{F}_q$.*

   $(s3)$ $3\deg c_1 < 2\deg c_2$ *and* $\deg c_2 \not\equiv 0 \mod 3$
   $LC(?)$ denotes here the leading coefficient of the argument.

2. *There is a unique zero of π in $k(\pi)$ lying over the place v of k if and only if one of the following holds.*

   $(s4)$ $\mathfrak{p}_v \mid a_2,\ \ \mathfrak{p}_v \nmid a_1$ *and* $v(a_2) \geq \frac{m}{2}$

   $(s5)$ $\mathfrak{p}_v \mid a_2,\ \ \mathfrak{p}_v \mid a_1$ *and $M(x) \mod \mathfrak{p}_v^n$ is irreducible.*
   Where $n = v\left(disc\left(M(x)\right)\right) + 1$.

   $(s6)$ $\mathfrak{p}_v \nmid a_2$.

Using the previous results, one can therefore improve the algorithm 2.1 for $r = 3$ as follows:

Algorithm 5.1. ***Input**: $M(x) = x^3 + a_1x^2 + a_2x + \mu Q \in A[x]$ irreducible polynomial defining the cubic field $k(\pi)/k$.*
***Ouput**: **True** if $M(x)$ is a Weil polynomial and **False** otherwise.*

1. *Compute $b_1 = \frac{-a_1^2}{3} + a_2;\ \ b_2 = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + \mu Q$.*

2. *Compute the square-free decomposition of* b_1 *and* b_2*:*
   $b_1 = \mu_1 \prod_{i=1}^{n_1} b_{1i}^{i}, \quad b_2 = \mu_2 \prod_{j=1}^{n_2} b_{1j}^{j}$
   Set $g_1 = \prod_{i=1}^{n_1} b_{1i}^{\lfloor \frac{i}{2} \rfloor}$ *and* $g_2 = \prod_{j=1}^{n_2} b_{1j}^{\lfloor \frac{j}{3} \rfloor}$

3. *Compute* $c_1 = \frac{b_1}{gcd(g_1,g_2)^2}$ *and* $c_2 = \frac{b_2}{gcd(g_1,g_2)^3}$

4. *If* c_1 *and* c_2 *fulfill one of the statements* $(s1)$, $(s2)$ *or* $(s3)$ *of proposition 5.1 then move to the next step. Otherwise output* ***False*** *and exit*

5. *Compute* $n = v\left(disc(M(x))\right) + 1$ *and*
   $\overline{M(x)} \equiv x^3 + a_1x^2 + a_2x + \mu Q \mod \mathfrak{p}_v^n$*.*
   If $\mathfrak{p}_v \mid a_2$ *and* $\mathfrak{p}_v \nmid a_1$ *and* $v(a_2) \geq \frac{m}{2}$ *then output* ***True*** *and exit.*
   Else if $\mathfrak{p}_v \mid a_2$ *and* $\mathfrak{p}_v \mid a_1$ *and* $\overline{M(x)}$ *is irreducible then the output* ***True*** *and exit.*
   Else if $\mathfrak{p}_v \nmid a_2$ *then output* ***True*** *and exit.*
   Else output ***False*** *and exit.*

Remark 5.2. *These new conditions are easier to check than the general ones in the initial algorithm.*

5.1.2 Endomorphism rings in a given isogeny class of rank 3 Drinfeld modules

We give in this part a better description of the orders occurring as endomorphism of a Drinfeld module in the special case of an isogeny class of rank 3 Drinfeld modules. The reader can wonder what we mean by "better" here. As it has been our philosophy throughout this thesis, we always want to provide conditions that can be checked using only the basic data we have at our disposal. That is, the coefficients of the Weil polynomial $M(x)$, the ring A and its field of fractions k, the finite A-field L and its A-characteristic $\mathfrak{p}_v$. In order to check in general whether an order $\mathcal{O}$ is the endomorphism ring of a Drinfeld module in the chosen isogeny class, the theorem 3.4 requires to know the conductor of $\mathcal{O}$ and the zero v_0 of the Frobenius π. But these data lie in the upper field $k(\pi)$. In this special case of rank 3, we are able to provide conditions that do not require to know additional data apart from the ones at our disposal.
As a direct consequence of theorem 3.4, we have the following:

Proposition 5.3. *We keep the same notation we have in the above mentioned theorem.*
Let $M(x) = x^3 + a_1x^2 + a_2x + \mu\mathfrak{p}_v^m$ be a rank 3 Weil polynomial.

1) *If $\mathfrak{p}_v \nmid a_2$ then an A-order $\mathcal{O}$ of $k(\pi)$ is the endomorphism ring of a Drinfeld module in the isogeny class defined by $M(x)$ if and only if it contains the Frobenius $\pi \in \mathcal{O}$.*

2) *Otherwise (i.e. if $\mathfrak{p}_v \mid a_2$), an order $\mathcal{O}$ of $k(\pi)$ occurs as endomorphism ring of a Drinfeld module in the isogeny class defined by $M(x)$ if and only if the Frobenius endomorphism $\pi \in \mathcal{O}$ and $\mathcal{O}$ is maximal at all the places of $k(\pi)$ lying over v (i.e. $\mathcal{O} \otimes A_v$ is a maximal order of the k_v-algebra $k_v(\pi)$).*

Proof:

1) If $\mathfrak{p}_v \nmid a_2$ then $M(x) \equiv x(x^2 + a_1x + a_2) \mod \mathfrak{p}_v$. That means (see corollary 3.2) the irreducible factor $M_{loc}(x)$ of $M(x)$ in $k_v[x]$ describing the unique zero v_0 of π in $k(\pi)$ is a degree 1 polynomial. Therefore any A-order of $k(\pi)$ containing π is already maximal at v_0. The statement follows then from theorem 3.4.

2) If $\mathfrak{p}_v \mid a_2$ then we have two sub-cases.

   - If $\mathfrak{p}_v \nmid a_1$ then $M(x) \equiv x^2(x + a_1) \mod \mathfrak{p}_v$.
     That means there are two places of $k(\pi)$ lying over the place v. The zero v_0 of π which is described by the irreducible factor $M_{loc}(x)$ of $M(x)$ in $k_v[x]$ fulfilling $M_{loc}(x) \equiv x^2 \mod \mathfrak{p}_v$ (see corollary 3.2), and another place v_1 described by the irreducible factor $M_1(x)$ of $M(x)$ in $k_v[x]$ fulfilling $M_1(x) \equiv x + a_1 \mod \mathfrak{p}_v$. As a consequence, $\deg M_1(x) = 1$. That means the completion of any A-order $\mathcal{O}$ of $k(\pi)$ containing π at the place v_1 must be maximal.
     It follows that, $\mathcal{O}$ is maximal at the zero v_0 of π if and only if $\mathcal{O}$ is maximal at all the places (v_0 and v_1) of $k(\pi)$ lying over v and the statement follows.

   - If $\mathfrak{p}_v \mid a_1$ then $M(x) \equiv x^3 \mod \mathfrak{p}_v$. That means the isogeny class defined by $M(x)$ is supersingular. In other words there is a unique place (the zero v_0 of π) of $k(\pi)$ lying over v and the statement follows from theorem 3.4.

$\Diamond$

Remark 5.3 (Recall).
To check that $\mathcal{O} \otimes A_v$ is a maximal A_v-order in the k_v-algebra $k_v(\pi)$ one can just check that the norm of the conductor $\mathfrak{c}$ of $\mathcal{O}$ is not divisible by $\mathfrak{p}_v$. We recall that the norm of the conductor can be gotten from the relationship between the discriminant of the order $\mathcal{O}$ and the discriminant of the field $k(\pi)$.

$$disc\,(\mathcal{O}) = N_{k(\pi)/k}\,(\mathfrak{c}) \cdot disc\,(k(\pi))$$

In the upcoming part, we want to explicitly compute the maximal order of the cubic function field $k(\pi)$ and all the sub-orders occurring as endomorphism ring of a rank-3 Drinfeld module.

Proposition 5.4. *[15, Corollary 5.2]*
Let $M_0(x) = x^3 + c_1x + c_2$ be the standard form of the polynomial $M(x) = x^3 + a_1x^2 + a_2x + \mu Q$. Where c_1 and c_2 are like computed in the algorithm 5.1. Let $disc\,(M_0(x)) = \lambda \prod_{i=1}^{l} D_i^i$ be the square-free factorization of $disc\,(M_0(x))$. The discriminant of the function field $k(\pi)$ is given by

$$disc\,(k(\pi)) = \lambda D \gcd(D_2D_4, c_2)^2 \text{ where } D = \prod_{i \text{ odd}} D_i, \quad \lambda \in \mathbb{F}_q^*.$$

We will not give the proof in details since it has already been done in [15]. We just remind that the proof strongly relies on the fact that
$M_0(x) = x^3 + c_1x + c_2$ is given in the standard form. That is, for any prime element $\mathfrak{p} \in A$, $v_\mathfrak{p}(c_1) < 2$ or $v_\mathfrak{p}(c_2) < 3$. This condition forces the valuation of the discriminant $v_\mathfrak{p}(disc\,(M_0(x))) = v_\mathfrak{p}(-4c_1^3 - 27c_2^2)$ to be bounded and leads to the following lemma.

Lemma 5.3. *[16, theorem 2]*
Let $k(\pi)/k$ be a cubic function field defined by the irreducible polynomial $M_0(x) = x^3 + c_1x + c_2$ given in the standard form. Let $D_0 = disc\,(M_0(x))$ and $\Delta_0 = disc\,(k(\pi))$. For any prime $\mathfrak{p}$ of k we have the the following:

(1) $v_\mathfrak{p}(\Delta_0) = 2$ if and only if $v_\mathfrak{p}(c_1) \geq v_\mathfrak{p}(c_2) \geq 1$.

(2) $v_\mathfrak{p}(\Delta_0) = 1$ if and only if $v_\mathfrak{p}(D_0)$ is odd.

(3) $v_\mathfrak{p}(\Delta_0) = 0$ otherwise.

Remark 5.4. *The index of $\tilde{\pi}$ can therefore be computed using the fact that $disc\,(M_0(x)) = ind(\tilde{\pi})^2 disc\,(k(\pi))$ i.e.*

$$I := ind(\tilde{\pi}) = \sqrt{\frac{disc\,(M_0(x))}{disc\,(k(\pi))}}$$

We recall that $\tilde{\pi}$ and π define the same function field $k(\pi) = k(\tilde{\pi})$.

Proposition 5.5. *[15, theorem 6.4] and [21, lemma 3.1]*
Let $M_0(x) = x^3 + c_1x + c_2$ be the standard form of the Weil polynomial $M(x) = x^3 + a_1x^2 + a_2x + \mu Q$. π denotes a root of $M(x)$ and $\tilde{\pi} = \dfrac{\pi + \frac{a_1}{3}}{\gcd(g_1, g_2)}$ is a root of $M_0(x)$. Let $\omega_1 = \alpha_1 + \tilde{\pi}$ and $\omega_2 = \dfrac{\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2}{I}$, where α_1, α_2 and β_2 are elements of A.
$(1, \omega_1, \omega_2)$ is an integral basis of the cubic function field $k(\pi) = k(\tilde{\pi})$ if and only if $\begin{cases} 3\beta_2^2 + c_1 \equiv 0 \mod I \\ \beta_2^3 + c_1\beta_2 + c_2 \equiv 0 \mod I^2 \\ \alpha_2 \equiv -2\beta_2^2 \equiv 2c_1/3 \mod I \end{cases}$

Proof: The proof mainly relies on the following two facts:

- $disc(1, \tilde{\pi}, \tilde{\pi}^2) = I^2 disc\,(k(\pi)/k)$
- For $\omega_2 = \frac{\alpha_2+\beta_2\tilde{\pi}+\tilde{\pi}^2}{I}$ to be integral it is necessary that

  $$\omega_2^2 = \frac{\left(\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2\right)^2}{I^2} \text{ and } (\alpha_1 + \tilde{\pi})\omega_2 \text{ both lie in } A[1, \tilde{\pi}, \omega_2]$$

  In other words there exist $\lambda_0, \mu_0,\ \lambda_1, \mu_1$ and $\lambda_2, \mu_2 \in A$ such that $\omega_2^2 = \lambda_0 + \lambda_1\tilde{\pi} + \lambda_2\omega_2$ and $\tilde{\pi}\omega_2 = \mu_0 + \mu_1\tilde{\pi} + \mu_2\omega_2$.

◊

Corollary 5.1. *α_1 in the previous proposition can be assumed to be 0 because if $\left(1, \alpha_1 + \tilde{\pi}, \dfrac{\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2}{I}\right)$ is an integral basis, then so is $\left(1, \tilde{\pi}, \dfrac{\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2}{I}\right)$.*

This is simply due to the fact that both triples have the same discriminant.

Remark 5.5. *One can therefore, given an isogeny class of Drinfeld modules described by the Weil polynomial $M(x) = x^3 + a_1x^2 + a_2x + \mu Q$, compute the corresponding maximal order $\mathcal{O}_{max}$ which is the A-module generated by $(1,\ \omega_1,\ \omega_2)$ as mentioned before.*

Let $\mathcal{O}_{max} = \langle 1,\ \omega_1, \omega_2\rangle = \left\{(X, Y, Z)\begin{pmatrix}1\\ \omega_1\\ \omega_2\end{pmatrix} \,\middle|\, X,\ Y,\ Z \in A\right\}$.

We want now to give a complete list of sub-orders of $\mathcal{O}_{max}$ occurring as endomorphism rings of Drinfeld modules. We know from proposition 5.3 that this

is equivalent to looking for sub-orders containing π and whose conductor's norm (in case $\mathfrak{p}_v \mid a_2$) is relatively prime to $\mathfrak{p}_v$.
Let then $\mathcal{O} = \langle \tilde{\omega_0},\ \tilde{\omega_1},\ \tilde{\omega_2} \rangle$ be a sub-order of $\mathcal{O}_{max}$.
$1 \in \mathcal{O}$. That means one can write without loss of generality

$$\mathcal{O} = \langle 1,\ \tilde{\omega_1},\ \tilde{\omega_2} \rangle = \left\{ (\tilde{X}, \tilde{Y}, \tilde{Z}) \begin{pmatrix} 1 \\ \tilde{\omega_1} \\ \tilde{\omega_2} \end{pmatrix} \middle| \tilde{X},\ \tilde{Y},\ \tilde{Z} \in A \right\}$$

But $\tilde{\omega_1}$ and $\tilde{\omega_2} \in \mathcal{O}_{max}$. That means

$$\tilde{\omega_1} = \tilde{\alpha_1} + \tilde{\beta_1}\omega_1 + \tilde{\gamma_1}\omega_2 \text{ and } \tilde{\omega_2} = \tilde{\alpha_2} + \tilde{\beta_2}\omega_1 + \tilde{\gamma_2}\omega_2$$

for some $\tilde{\alpha_i},\ \tilde{\beta_i},\ \tilde{\gamma_i} \in A \quad i = 1, 2$. In other words,
$\begin{pmatrix} 1 \\ \tilde{\omega_1} \\ \tilde{\omega_2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \tilde{\alpha_1} & \tilde{\beta_1} & \tilde{\gamma_1} \\ \tilde{\alpha_2} & \tilde{\beta_2} & \tilde{\gamma_2} \end{pmatrix} \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \end{pmatrix}$. Let $M = \begin{pmatrix} 1 & 0 & 0 \\ \tilde{\alpha_1} & \tilde{\beta_1} & \tilde{\gamma_1} \\ \tilde{\alpha_2} & \tilde{\beta_2} & \tilde{\gamma_2} \end{pmatrix} \in \mathscr{M}_3(A)$
Where $\mathscr{M}_3(A)$ denotes the ring of 3×3 -matrices with entries in A.
M can be transformed into the so-called Hermite normal form. That means there the exists a matrix $U \in GL_3(A)$ and an upper triangular matrix H such that $U \cdot M = H$.
Some simple row operations show that the Hermite normal form of M looks like

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & b \\ 0 & 0 & a \end{pmatrix} \text{ with } \deg_T(b) < \deg_T(a) \tag{5.1}$$

We therefore redefine $\tilde{\omega_1}$ and $\tilde{\omega_2}$ as $\tilde{\omega_1} = c\omega_1 + b\omega_2$ and $\tilde{\omega_2} = a\omega_2$.
The sub-lattice $\mathcal{O}$ can then be written as

$$\mathcal{O} = \langle 1,\ \tilde{\omega_1},\ \tilde{\omega_2} \rangle = \left\{ (X,\ Y,\ Z) \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & b \\ 0 & 0 & a \end{pmatrix} \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \end{pmatrix} \middle| X,\ Y,\ Z \in A \right\}$$

Remark 5.6. *One clearly notices that the sub-lattice $\mathcal{O}$ above is an order if and only if $\tilde{\omega_1}^2$, $\tilde{\omega_2}^2$ and $\tilde{\omega_1}\tilde{\omega_2}$ belong to $\mathcal{O}$*

$$\text{But} \begin{cases} \tilde{\omega_1}^2 = (c\omega_1 + b\omega_2)^2 = c^2\omega_1^2 + 2bc\omega_1\omega_2 + b^2\omega_2^2 \\ \tilde{\omega_2}^2 = (a\omega_2)^2 = a^2\omega_2^2 \\ \tilde{\omega_1}\tilde{\omega_1} = (c\omega_1 + b\omega_2)(a\omega_2) = ac\omega_1\omega_2 + ab\omega_2^2 \end{cases}$$

$$\text{Thus} \begin{pmatrix} \tilde{\omega_1}^2 \\ \tilde{\omega_2}^2 \\ \tilde{\omega_1}\tilde{\omega_2} \end{pmatrix} = \underbrace{\begin{pmatrix} c^2 & b^2 & 2bc \\ 0 & a^2 & 0 \\ 0 & ab & ac \end{pmatrix}}_{M_1} \begin{pmatrix} \omega_1^2 \\ \omega_2^2 \\ \omega_1\omega_2 \end{pmatrix}$$

As we have seen in proposition 5.5 and its corollary,

$\omega_1 = \tilde{\pi}$ and $\omega_2 = \dfrac{\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2}{I}$ where $\tilde{\pi}^3 + c_1\tilde{\pi} + c_2 = 0$
One can therefore compute $\omega_1^2,\ \omega_2^2$ and $\omega_1\omega_2$ in terms of ω_1 and ω_2. One gets
$\begin{pmatrix} \omega_1^2 \\ \omega_2^2 \\ \omega_1\omega_2 \end{pmatrix} = \underbrace{\begin{pmatrix} X_{11} & X_{12} & X_{13} \\ X_{21} & X_{22} & X_{23} \\ X_{31} & X_{32} & X_{33} \end{pmatrix}}_{M_2} \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \end{pmatrix}$ where

$X_{11} = -\alpha_2,\ X_{12} = -\beta_2,\ X_{13} = I$
$X_{21} = \dfrac{\alpha_2\beta_2^2 - c_1\alpha_2 + 3\alpha_2^2 - 2c_2\beta_2}{I^2},\ X_{22} = \dfrac{-\beta_2^3 - c_1\beta_2 - c_2}{I^2},\ X_{23} = \dfrac{\beta_2^2 - c_1 + 2\alpha_2}{I}$
$X_{31} = \dfrac{\alpha_2\beta_2 - c_2}{I},\ X_{32} = \dfrac{-\beta_2^2 - c_1 + \alpha_2}{I}$ and $X_{33} = \beta_2$.
Therefore

$$\begin{pmatrix} \tilde{\omega_1}^2 \\ \tilde{\omega_2}^2 \\ \tilde{\omega_1}\tilde{\omega_2} \end{pmatrix} = M_1M_2 \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \end{pmatrix} = M_1M_2H^{-1} \begin{pmatrix} 1 \\ \tilde{\omega_1} \\ \tilde{\omega_2} \end{pmatrix}$$

Remark 5.7. *$\mathcal{O}$ is an order if and only if $M_1M_2H^{-1} \in \mathscr{M}_3(A)$*

Let us now investigate the orders occurring as endomorphism ring of a rank 3 Drinfeld module.
We know that in addition to the above mentioned condition, $\mathcal{O} = \langle 1,\ \tilde{\omega_1},\ \tilde{\omega_2}\rangle$ must contain the Frobenius π. In other words, there should exist $a_0,\ b_0,\ c_0 \in A$ such that
$\pi = a_0 + b_0\tilde{\omega_1} + c_0\tilde{\omega_2}$. But

$$\omega_1 = \tilde{\pi} \text{ and } \tilde{\pi} = \frac{\pi + \frac{a_1}{3}}{\gcd(g_1, g_2)}$$

Also $\tilde{\omega_1} = c\omega_1 + b\omega_2$ and $\tilde{\omega_2} = a\omega_2$. Therefore

$$-\frac{a_1}{3} + \gcd(g_1, g_2)\cdot\omega_1 = a_0 + b_0c\cdot\omega_1 + (b_0b + c_0a)\cdot\omega_2$$

Thus

$$b_0c = \gcd(g_1, g_2) \text{ and } b_0b = -c_0a \tag{5.2}$$

That is,

$$\begin{cases} c \text{ divides } \gcd(g_1, g_2) \text{ and} \\ a \text{ divides } b\dfrac{\gcd(g_1, g_2)}{c} \end{cases}$$

We summarize our discussion in the following theorem:

Theorem 5.2. *$A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$*
Let $M(x) = x^3 + a_1x^2 + a_2x + \mu Q \in A[x]$ be a Weil polynomial. In order

to put $M(x)$ in a simple form $x^3 + b_1 x + b_2$, let $b_1 = \dfrac{-a_1^2}{3} + a_2$ and $b_2 = \dfrac{2a_1^3}{27} - \dfrac{a_1 a_2}{3} + \mu Q$ whose square-free factorizations are given by

$$b_1 = \mu_1 \prod_{i=1}^{n_1} b_{1i}^{i} \quad b_2 = \mu_2 \prod_{j=1}^{n_2} b_{2j}^{j} \quad \mu_1, \mu_2 \in \mathbb{F}_q^*$$

In order to get the standard form $M_0(x) = x^3 + c_1 x + c_2$ of $M(x)$ (as defined in 5.1), we consider g_1 and g_2 the elements of A defined by

$$g_1 = \prod_{i=1}^{n_1} b_{1i}^{\lfloor \frac{i}{2} \rfloor} \text{ and } g_2 = \prod_{j=1}^{n_2} b_{2j}^{\lfloor \frac{j}{3} \rfloor}$$

We remove out from b_1 and b_2 resp. the highest square common divisor and the highest cubic common divisor by setting

$$c_1 = \frac{b_1}{\gcd(g_1, g_2)^2} \text{ and } c_2 = \frac{b_2}{\gcd(g_1, g_2)^3}$$

Let $\tilde{\pi} = \frac{\pi + \frac{a_1}{3}}{\gcd(g_1, g_2)}$ be a root of the standard polynomial $x^3 + c_1 x + c_2$.
Let $I = ind(\tilde{\pi}) = \frac{ind(\pi)}{gcd(g_1, g_2)^3}$, α_2 and $\beta_2 \in A$ such that

$$\begin{cases} 3\beta_2^2 + c_1 \equiv 0 \mod I \\ \beta_2^3 + c_1 \beta_2 + c_2 \equiv 0 \mod I^2 \\ \alpha_2 \equiv -2\beta_2^2 \equiv 2c_1/3 \mod I \end{cases}$$

We consider the matrix $M_2 \in \mathscr{M}_3(k)$ defined by

$$M_2 = \begin{pmatrix} X_{11} & X_{12} & X_{13} \\ X_{21} & X_{22} & X_{23} \\ X_{31} & X_{32} & X_{33} \end{pmatrix} \text{ where}$$

$X_{11} = -\alpha_2,\ X_{12} = -\beta_2,\ X_{13} = I$
$X_{21} = \dfrac{\alpha_2\beta_2^2 - c_1\alpha_2 + 3\alpha_2^2 - 2c_2\beta_2}{I^2},\ X_{22} = \dfrac{-\beta_2^3 - c_1\beta_2 - c_2}{I^2},\ X_{23} = \dfrac{\beta_2^2 - c_1 + 2\alpha_2}{I}$
$X_{31} = \dfrac{\alpha_2\beta_2 - c_2}{I},\ X_{32} = \dfrac{-\beta_2^2 - c_1 + \alpha_2}{I}$ *and* $X_{33} = \beta_2$.

The Endomorphism rings of Drinfeld modules in the isogeny class defined by the Weil polynomial $M(x)$ are:

$$\mathcal{O} = A + A \cdot \left(c\tilde{\pi} + b \left(\frac{\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2}{I} \right) \right) + A \cdot a \left(\frac{\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2}{I} \right)$$

such that $M_1M_2H^{-1} \in \mathscr{M}_3\,(A)$ *and in addition* $gcd(\mathfrak{p}_v, ac) = 1$ *if* $\mathfrak{p}_v \mid a_2$. *Where*

$$M_1 = \begin{pmatrix} c^2 & b^2 & 2bc \\ 0 & a^2 & 0 \\ 0 & ab & ac \end{pmatrix} \text{ and } H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & b \\ 0 & 0 & a \end{pmatrix}$$

$$\begin{cases} c \textit{ runs through the divisors of } \gcd(g_1, g_2) \\ a \textit{ runs through the divisors of } I \\ b \in A \textit{ such that } \deg_T b < \deg_T a \textit{ and } a \mid b\dfrac{\gcd(g_1, g_2)}{c} \end{cases}$$

Proof: The proof follows straightforwardly from our discussion before. The condition $gcd(\mathfrak{p}_v, ac) = 1$ comes from the fact that in case $\mathfrak{p}_v \mid a_2$, the norm of the conductor of $\mathcal{O}$ must be prime to $\mathfrak{p}_v$ (see Proposition 5.3). ◊

Corollary 5.2. *Let* $M(x) = x^3+a_1x^2+a_2x+\mu Q \in A[x]$ *be a Weil polynomial.* π *is a root of* $M(x)$ *and* $\tilde{\pi} = \pi + \dfrac{a_1}{3}$. *Let*
$b_1 = \dfrac{-a_1^2}{3} + a_2$ *and* $b_2 = \dfrac{2a_1^3}{27} - \dfrac{a_1a_2}{3} + \mu Q$.
If there is no prime $\mathfrak{p} \in A$ *such that* $\mathfrak{p}^2 \mid b_1$ *and* $\mathfrak{p}^3 \mid b_2$ *(in particular if* b_1 *and* b_2 *are coprime or* b_1 *is square-free or* b_2 *is cubic-free) then the endomorphism rings of Drinfeld modules in the isogeny class defined by the Weil polynomial* $M(x)$ *are*

$$\mathcal{O}_a = A + A \cdot \tilde{\pi} + A \cdot a \left(\frac{\alpha_2 + \beta_2\tilde{\pi} + \tilde{\pi}^2}{I} \right)$$

such that $M_aM_2H_a^{-1} \in \mathscr{M}_3(A)$ *and in addition* $gcd(\mathfrak{p}_v, a) = 1$ *if* $\mathfrak{p}_v \mid a_2$. *Where*

$$M_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a^2 & 0 \\ 0 & 0 & a \end{pmatrix} \text{ and } H_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix}$$

Here a *runs through the divisors of the index* $I = ind(\tilde{\pi})$.

Proof: One can just reconsider the equation (5.2) right after remark 5.7. Here $\gcd(g_1, g_2) = 1$. Thus $b_0c = 1$ i.e. b_0 and c are units. In addition $b_0b = -c_0a$ and b_0 is a unit. That means $a \mid b$. But $\deg_T b < \deg_T a$ (see equation (5.1)). Therefore $b = 0$. Hence the matrix H in equation (5.1) and the matrix M_1 become

$$H_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix} \text{ and } M_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a^2 & 0 \\ 0 & 0 & a \end{pmatrix}$$

and the result follows. ◊

5.1.3 Isomorphism classes in a given isogeny class of rank 3 Drinfeld modules

Here we mainly explain how the computation can be done and we provide a concrete example.
We consider the isogeny class defined by the polynomial

$$M(x) = x^3 + a_1(T)x^2 + a_2(T)x + \mu Q(T)$$

We want to list all the isomorphism classes of Drinfeld modules in this isogeny class. We know that the Frobenius endomorphism $\pi = \tau^s$ (with $s = [L : \mathbb{F}_q]$) is a root of $M(x)$. That means

$$\tau^{3s} + a_1(T)\tau^{2s} + a_2(T)\tau^s + \mu Q(T) = 0.$$

By definition of the action of the Drinfeld module ϕ we have

$$\tau^{3s} + a_1(\phi_T)\tau^{2s} + a_2(\phi_T)\tau^s + \mu Q(\phi_T) = 0 \qquad (\star)$$

We consider $(\star)$ as an equation with unknown ϕ_T. This equation can be solved by setting $\phi_T = \gamma(T) + \alpha_1\tau + \alpha_2\tau^2 + \alpha_3\tau^3$. We recall that $\gamma(T)$ is already known since γ is the ring homomorphism defining the A-field L. One can therefore plug ϕ_T in the equation $(\star)$ and get a non-linear system of equation (with unknowns $\alpha_{i's}$). Even though the system is non-linear, a way to solve it can be by "brute force". That is, looking for all tuples $(\alpha_1, \alpha_2, \alpha_3) \in L^3$ solutions of the system. Since L is finite, we have finitely many such tuples. Each of those solutions yields a Drinfeld module ϕ defined by $\phi_T = \gamma(T)+\alpha_1\tau+\alpha_2\tau^2+\alpha_3\tau^3$. We therefore gather those Drinfeld modules with respect to their isomorphism classes by computing and comparing their J-invariants and fine isomorphy invariants.
Let us have a look at a concrete example.
Let $A = \mathbb{F}_5[T],\ k = \mathbb{F}_5(T),\ L = \mathbb{F}_5(\alpha)$ with $\alpha^2 + 4\alpha + 2 = 0$. L is an A-field defined by $\gamma : A \longrightarrow L,\ f(T) \longmapsto f(0)$. The A-characteristic of L is T because $\mathfrak{p}_v = Ker\gamma = T \cdot A$ is the ideal generated by T.
$m = [L : A/\mathfrak{p}_v] = [L : A/T \cdot A] = [\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 2$. We consider the polynomial

$$M(x) = x^3 + 3x^2 + (1 + T)x + T^2$$

<u>Claim</u>: $M(x)$ is a Weil polynomial.
first of all $M(x)$ is irreducible in $A[x]$ and therefore (Gauss lemma) is also irreducible in $k[x]$. One easily shows using the algorithm 2.1 that

- $\overline{M_0(x)} = x^3+\frac{3}{T}x^2+\frac{1+T}{T^2}x+\frac{T^2}{T^3} \mod \frac{1}{T^3} \equiv x^3+\frac{3}{T}x^2+\frac{1+T}{T^2}x+\frac{1}{T} \mod \frac{1}{T^3}$ $(h = 3)$ is irreducible.

- $\overline{M(x)} = x^3+3x^2+(1+T)x+T^2 \mod T^2 \equiv x(x^2+3x+1+T) \mod T^2$ $(n=2)$ and we clearly have $Res(x, x^2+3x+1+T) \mod T \not\equiv 0$.

Hence $M(x)$ defines an isogeny class of Drinfeld modules.
We aim to list (as explained before) all the isomorphism classes of Drinfeld modules in the isogeny class defined by $M(x) = x^3+3x^2+(1+T)x+T^2$.
$\pi = \tau^s$ with $s = [L : \mathbb{F}_5] = 2$. i.e. $\pi = \tau^2$. In addition $M(\pi) = 0$ i.e.

$$\tau^6 + 3\tau^4 + (1+\phi_T)\tau^2 + \phi_T^2 = 0$$

That means $\phi_T^2 + \phi_T\tau^2 + \tau^6 + 3\tau^4 + \tau^2 = 0$. We clearly see from the Weil polynomial that $T \in ker\gamma$. i.e. $\gamma(T) = 0$.
We can therefore set $\phi_T = \alpha_1\tau + \alpha_2\tau^2 + \alpha_3\tau^3 \in L\{\tau\}$.
i.e. $(\alpha_1\tau + \alpha_2\tau^2 + \alpha_3\tau^3)^2 + (\alpha_1\tau + \alpha_2\tau^2 + \alpha_3\tau^3)\tau^2 + \tau^6 + 3\tau^4 + \tau^2 = 0$.
Solving this equation yields the following Drinfeld modules:

$\phi(T)$	
$(\alpha+3)\tau + 2\tau^2 + (4\alpha+4)\tau^3$	$(\alpha+3)\tau + 2\tau^2 + 3\tau^3$
$(\alpha+3)\tau + (2\alpha+1)\tau^2 + (\alpha+3)\tau^3$	$(\alpha+3)\tau + 4\alpha\tau^2 + 2\tau^3$
$(\alpha+3)\tau + 4\alpha\tau^2 + (\alpha+1)\tau^3$	$(\alpha+3)\tau + (3\alpha+3)\tau^2 + (\alpha+3)\tau^3$
$(\alpha+3)\tau + (\alpha+4)\tau^2 + 2\tau^3$	$(\alpha+3)\tau + (\alpha+4)\tau^2 + (\alpha+1)\tau^3$
$2\tau + 2\tau^2 + (4\alpha+2)\tau^3$	$2\tau + 2\tau^2 + (\alpha+1)\tau^3$
$2\tau + (2\alpha+1)\tau^2 + 2\tau^3$	$2\tau + 4\alpha\tau^2 + (\alpha+3)\tau^3$
$2\tau + 4\alpha\tau^2 + (4\alpha+4)\tau^3$	$2\tau + (3\alpha+3)\tau^2 + 2\tau^3$
$2\tau + (\alpha+4)\tau^2 + (\alpha+3)\tau^3$	$2\tau + (\alpha+4)\tau^2 + (4\alpha+4)\tau^3$
$(4\alpha+4)\tau + 2\tau^2 + (\alpha+3)\tau^3$	$(4\alpha+4)\tau + 2\tau^2 + 3\tau^3$
$(4\alpha+4)\tau + (2\alpha+1)\tau^2 + (4\alpha+4)\tau^3$	$(4\alpha+4)\tau + 4\alpha\tau^2 + 2\tau^3$
$(4\alpha+4)\tau + 4\alpha\tau^2 + (4\alpha+2)\tau^3$	$(4\alpha+4)\tau + (3\alpha+3)\tau^2 + (4\alpha+4)\tau^3$
$(4\alpha+4)\tau + (\alpha+4)\tau^2 + 2\tau^3$	$(4\alpha+4)\tau + (\alpha+4)\tau^2 + (4\alpha+2)\tau^3$
$(4\alpha+2)\tau + 2\tau^2 + 2\tau^3$	$(4\alpha+2)\tau + 2\tau^2 + (\alpha+1)\tau^3$
$(4\alpha+2)\tau + (2\alpha+1)\tau^2 + (4\alpha+2)\tau^3$	$(4\alpha+2)\tau + 4\alpha\tau^2 + (4\alpha+4)\tau^3$
$(4\alpha+2)\tau + 4\alpha\tau^2 + 3\tau^3$	$(4\alpha+2)\tau + (3\alpha+3)\tau^2 + (4\alpha+2)\tau^3$
$(4\alpha+2)\tau + (\alpha+4)\tau^2 + (4\alpha+4)\tau^3$	$(4\alpha+2)\tau + (\alpha+4)\tau^2 + 3\tau^3$
$3\tau + 2\tau^2 + (\alpha+3)\tau^3$	$3\tau + 2\tau^2 + (4\alpha+4)\tau^3$
$3\tau + (2\alpha+1)\tau^2 + 3\tau^3$	$3\tau + 4\alpha\tau^2 + (4\alpha+2)\tau^3$
$3\tau + 4\alpha\tau^2 + (\alpha+1)\tau^3$	$3\tau + (3\alpha+3)\tau^2 + 3\tau^3$
$3\tau + (\alpha+4)\tau^2 + (4\alpha+2)\tau^3$	$3\tau + (\alpha+4)\tau^2 + (\alpha+1)\tau^3$
$(\alpha+1)\tau + 2\tau^2 + 2\tau^3$	$(\alpha+1)\tau + 2\tau^2 + (4\alpha+2)\tau^3$
$(\alpha+1)\tau + (2\alpha+1)\tau^2 + (\alpha+1)\tau^3$	$(\alpha+1)\tau + 4\alpha\tau^2 + (\alpha+3)\tau^3$
$(\alpha+1)\tau + 4\alpha\tau^2 + 3\tau^3$	$(\alpha+1)\tau + (3\alpha+3)\tau^2 + (\alpha+1)\tau^3$
$(\alpha+1)\tau + (\alpha+4)\tau^2 + (\alpha+3)\tau^3$	$(\alpha+1)\tau + (\alpha+4)\tau^2 + 3\tau^3$

We have implemented a SAGE code adapted to algorithm 4.1 in order to gather these Drinfeld modules with respect to their isomorphism classes and we got the following:

$\phi_1(T)$	$\phi_2(T)$
$(\alpha+3)\tau+2\tau^2+(4\alpha+4)\tau^3$	$(\alpha+3)\tau+2\tau^2+3\tau^3$
$2\tau+2\tau^2+(4\alpha+2)\tau^3$	$2\tau+2\tau^2+(\alpha+1)\tau^3$
$(4\alpha+4)\tau+2\tau^2+3\tau^3$	$(4\alpha+4)\tau+2\tau^2+(\alpha+3)\tau^3$
$(4\alpha+2)\tau+2\tau^2+(\alpha+1)\tau^3$	$(4\alpha+2)\tau+2\tau^2+2\tau^3$
$3\tau+2\tau^2+(\alpha+3)\tau^3$	$3\tau+2\tau^2+(4\alpha+4)\tau^3$
$(\alpha+1)\tau+2\tau^2+2\tau^3$	$(\alpha+1)\tau+2\tau^2+(4\alpha+2)\tau^3$

$\phi_3(T)$	$\phi_4(T)$
$(\alpha+3)\tau+(2\alpha+1)\tau^2+(\alpha+3)\tau^3$	$(\alpha+3)\tau+4\alpha\tau^2+2\tau^3$
$2\tau+(2\alpha+1)\tau^2+2\tau^3$	$2\tau+4\alpha\tau^2+(4\alpha+4)\tau^3$
$(4\alpha+4)\tau+(2\alpha+1)\tau^2+(4\alpha+4)\tau^3$	$(4\alpha+4)\tau+4\alpha\tau^2+(4\alpha+2)\tau^3$
$(4\alpha+2)\tau+(2\alpha+1)\tau^2+(4\alpha+2)\tau^3$	$(4\alpha+2)\tau+4\alpha\tau^2+3\tau^3$
$3\tau+(2\alpha+1)\tau^2+3\tau^3$	$3\tau+4\alpha\tau^2+(\alpha+1)\tau^3$
$(\alpha+1)\tau+(2\alpha+1)\tau^2+(\alpha+1)\tau^3$	$(\alpha+1)\tau+4\alpha\tau^2+(\alpha+3)\tau^3$

$\phi_5(T)$	$\phi_6(T)$
$(\alpha+3)\tau+4\alpha\tau^2+(\alpha+1)\tau^3$	$(\alpha+3)\tau+(3\alpha+3)\tau^2+(\alpha+3)\tau^3$
$2\tau+4\alpha\tau^2+(\alpha+3)\tau^3$	$2\tau+(3\alpha+3)\tau^2+2\tau^3$
$(4\alpha+4)\tau+4\alpha\tau^2+2\tau^3$	$(4\alpha+4)\tau+(3\alpha+3)\tau^2+(4\alpha+4)\tau^3$
$(4\alpha+2)\tau+4\alpha\tau^2+(4\alpha+4)\tau^3$	$(4\alpha+2)\tau+(3\alpha+3)\tau^2+(4\alpha+2)\tau^3$
$3\tau+4\alpha\tau^2+(4\alpha+2)\tau^3$	$3\tau(3\alpha+3)\tau^2+3\tau^3$
$(\alpha+1)\tau+4\alpha\tau^2+3\tau^3$	$(\alpha+1)\tau+(3\alpha+3)\tau^2+(\alpha+1)\tau^3$

$\phi_7(T)$	$\phi_8(T)$
$(\alpha+3)\tau+(\alpha+4)\tau^2+2\tau^3$	$(\alpha+3)\tau+(\alpha+4)\tau^2+(\alpha+1)\tau^3$
$2\tau+(\alpha+4)\tau^2+(4\alpha+4)\tau^3$	$2\tau+(\alpha+4)\tau^2+(\alpha+3)\tau^3$
$(4\alpha+4)\tau+(\alpha+4)\tau^2+(4\alpha+2)\tau^3$	$(4\alpha+4)\tau+(\alpha+4)\tau^2+2\tau^3$
$(4\alpha+2)\tau+(\alpha+4)\tau^2+3\tau^3$	$(4\alpha+2)\tau+(\alpha+4)\tau^2+(4\alpha+4)\tau^3$
$3\tau+(\alpha+4)\tau^2+(\alpha+1)\tau^3$	$3\tau+(\alpha+4)\tau^2+(4\alpha+2)\tau^3$
$(\alpha+1)\tau+(\alpha+4)\tau^2+(\alpha+3)\tau^3$	$(\alpha+1)\tau+(\alpha+4)\tau^2+3\tau^3$

Remark 5.8. *We know you are probably asking yourself right now the question concerning the list of orders that are endomorphism rings of Drinfeld modules in this isogeny class. The answer is straightforward. All those Drinfeld modules have the same endomorphism ring, that is $A[\pi]$. This is due to the fact that disc$(M(x)) = 3T^4 + 3T^2 + T$ is square-free. That means $A[\pi]$*

is the maximal order of $k(\pi)$.
One would say in a fancier language that all the isogenies are horizontal.

5.2 Explicit description for the case of rank 4 Drinfeld modules

5.2.1 Rank 4 Weil numbers

We still keep the notations $A = \mathbb{F}_q[T],\ k = \mathbb{F}_q(T)$ and $Q = \mathfrak{p}_v^m$.
The possible rank 4 Weil polynomials are

- $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q,\ \mu \in \mathbb{F}_q,\ \deg a_i \leq \frac{i \deg Q}{4}$ and $M(x)$ is approved by the test in algorithm 2.1.
- $M(x) = x^2 + a_1x + \mu Q^{1/2},\ \mu \in \mathbb{F}_q,\ \deg a_1 \leq \frac{\deg Q}{4},\ 2 \mid m$ and $M(x)$ is approved by the algorithm 2.1
- $M(x) = x - \mu Q^{1/4},\ \mu \in \mathbb{F}_q$ and $4 \mid m$.

For the same reason we mentioned before, we focus first on Weil polynomials of the first form. i.e. $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$.
The following result provide for this special case some simpler ways to check whether the condition 2 of definition 2.1 is fulfilled.

Lemma 5.4. *Let* $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu\mathfrak{p}_v^m$ *be a potential Weil polynomial with all the required restrictions on the coefficients* $a_{i's}$.
If $\mathfrak{p}_v \nmid a_1^2 - 4a_2$ *and* $\mathfrak{p}_v \mid a_3$ *then*
there is a unique zero of π *in* $k(\pi)$ *lying over the place* v *of* k *if and only if* $v\,(disc\,(M(x))) \geq m$.

Proof: With hypotheses of the lemma, we have the following:

$\boxed{\Rightarrow}$ We assume that there is a unique zero of π in $k(\pi)$ lying over the place v of k.
Since $\mathfrak{p}_v \mid a_3$ we have $M(x) \equiv x^2(x^2 + a_1x + a_2) \mod \mathfrak{p}_v$.
If $v\,(disc\,(M(x))) < m$ then we can conclude from the Hensel lemma 5.2 that the double root $x_0 = 0$ modulo $\mathfrak{p}_v$ can be lifted modulo $\mathfrak{p}_v^n$, where $n = v\,(disc\,(M(x))) + 1 \leq m$, because $M(0) \equiv 0 \mod \mathfrak{p}_v^n$.
That means $M(x) \equiv M_1(x) \cdot M_2(x) \cdot M_3(x) \mod \mathfrak{p}_v^n$, where
$M_1(x) \equiv M_2(x) \equiv x \mod \mathfrak{p}_v$ and $M_3(x) \equiv x^2 + a_1x + a_2 \mod \mathfrak{p}_v$.
i.e. $Res\,(M_1(x), M_2(x)) \equiv 0 \mod \mathfrak{p}_v$ which contradicts the fact that there is a unique zero of π in $k(\pi)$ lying over the place v of k.

Hence $v\left(disc\left(M(x)\right)\right) \geq m$.

$\boxed{\Leftarrow}$ Let us assume conversely that $v\left(disc\left(M(x)\right)\right) \geq m$.
We know that $M(x) \equiv x^2(x^2 + a_1x + a_2) \mod \mathfrak{p}_v$.
Since $n = v\left(disc\left(M(x)\right)\right) + 1 \geq m + 1 > m$, $M(0) \not\equiv 0 \mod \mathfrak{p}_v^n$.
That means (Hensel lemma 5.2) the multiple root $x_0 = 0$ modulo $\mathfrak{p}_v$ cannot be lifted modulo $\mathfrak{p}_v^n$. Also $\mathfrak{p}_v \nmid a_1^2 - 4a_2$ i.e. $\mathfrak{p}_v \nmid a_1$ or $\mathfrak{p}_v \nmid a_2$.
That means $M(x) \equiv M_1(x) \cdot M_2(x) \mod \mathfrak{p}_v^n$
where $M_1(x)$ is irreducible over k_v and
$M_1(x) \equiv \begin{cases} x^2 \mod \mathfrak{p}_v \text{ if } \mathfrak{p}_v \nmid a_2 \\ x^3 \mod \mathfrak{p}_v \text{ otherwise} \end{cases}$ and $M_2(x) \equiv \begin{cases} x^2 + a_1x + a_2 \mod \mathfrak{p}_v \text{ if } \mathfrak{p}_v \nmid a_2 \\ x + a_1 \mod \mathfrak{p}_v \text{ otherwise} \end{cases}$
Since $a_1^2 - 4a_2 \not\equiv 0 \mod \mathfrak{p}_v$, $M_2(x)$ has (in case there exist) only simple roots modulo $\mathfrak{p}_v$.
Hence in any case, any two irreducible factors of $M(x) \mod \mathfrak{p}_v^n$ have no commom root modulo $\mathfrak{p}_v$. In other words there is a unique zero of π in $k(\pi)$ lying over the place v of k (see corollary 2.1).

$\Diamond$

Proposition 5.6. *Let $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu\mathfrak{p}_v^m$ be a potential Weil polynomial with all the required restrictions on the coefficients $a_{i's}$.*

1. *If $\mathfrak{p}_v \nmid a_3$ then there is a unique zero of π in $k(\pi)$ lying over the place v of k.*

2. *If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \nmid a_1$ then there is a unique zero of π in $k(\pi)$ lying over the place v of k if and only if $v\left(-27a_3^4 + 18a_1a_2a_3^3 - 4a_1^3a_3^3 + a_1^2a_2^2a_3^2 - 4a_2^3a_3^2\right) \geq m$.*

3. *If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_2$ and $\mathfrak{p}_v \mid a_1$ then there is a unique zero of π in $k(\pi)$ lying over the place v of k if and only if $v(a_3) \geq \frac{m}{2}$.*

4. *If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \mid a_1$ then there is a unique zero of π in $k(\pi)$ lying over the place v of k if and only if $M(x) \mod \mathfrak{p}_v^{v(disc(M(x)))+1}$ is irreducible.*

5. *If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_2$ and $\mathfrak{p}_v \nmid a_1$ then we have the following:*

   - *If in addition $\mathfrak{p}_v \nmid a_1^2 - 4a_2$ then there is a unique zero of π in $k(\pi)$ lying over the place v of k if and only if $v(a_3) \geq \frac{m}{2}$.*

- *If in addition* $\mathfrak{p}_v \mid a_1^2 - 4a_2$ *then there is a unique zero of* π *in* $k(\pi)$ *lying over the place* v *of* k *if and only if* $M(x) \mod \mathfrak{p}_v^{v(disc(M(x)))+1}$ *has no root.*

Proof:

1. This case has already been shown in proposition 2.6.

2. If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \nmid a_1$ then we have the following: $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_1^2 - 4a_2$. In addition the discriminant of the quartic polynomial $M(x)$ is given by:
$$\begin{aligned} disc\,(M(x)) = \; & 256\mu^3\mathfrak{p}_v^{3m} - 192\mu^2 a_1 a_3 \mathfrak{p}_v^{2m} - 128\mu^2 a_2^2 \mathfrak{p}_v^{2m} + 144\mu a_2 a_3^2 \mathfrak{p}_v^{m} - \\ & 27a_3^4 + 144\mu^2 a_1^2 a_2 \mathfrak{p}_v^{2m} - 6\mu a_1^2 a_3^2 \mathfrak{p}_v^{m} - 80\mu a_1 a_2^2 a_3 \mathfrak{p}_v^{m} + \\ & 18a_1 a_2 a_3^3 + 16\mu a_2^4 \mathfrak{p}_v^{m} - 4a_2^3 a_3^2 - 27\mu^2 a_1^4 \mathfrak{p}_v^{2m} + 18\mu a_1^3 a_2 a_3 \mathfrak{p}_v^{m} - \\ & 4a_1^3 a_3^3 - 4\mu a_1^2 a_2^3 \mathfrak{p}_v^{m} + a_1^2 a_2^2 a_3^2. \\ = \; & (256\mu^3\mathfrak{p}_v^{2m} - 192\mu^2 a_1 a_3 \mathfrak{p}_v^{m} - 128\mu^2 a_2^2 \mathfrak{p}_v^{m} + 144\mu a_2 a_3^2 + \\ & 144\mu^2 a_1^2 a_2 \mathfrak{p}_v^{m} - 6\mu a_1^2 a_3^2 - 80\mu a_1 a_2^2 a_3 - 27\mu^2 a_1^4 \mathfrak{p}_v^{m} + \\ & 18\mu a_1^3 a_2 a_3 - 4\mu a_2^3\,(a_1^2 - 4a_2))\,\mathfrak{p}_v^{m} - 27a_3^4 + 18a_1 a_2 a_3^3 - \\ & 4a_1^3 a_3^3 + a_1^2 a_2^2 a_3^2 - 4a_2^3 a_3^2 \end{aligned}$$
   That means
   $v\,(disc\,(M(x))) \geq m$ if and only if
   $v\,(-27a_3^4 + 18a_1a_2a_3^3 - 4a_1^3a_3^3 + a_1^2a_2^2a_3^2 - 4a_2^3a_3^2) \geq \; m.$
   The result follows then from lemma 5.4.

3. If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_2$ and $\mathfrak{p}_v \mid a_1$ then we have again
   $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_1^2 - 4a_2$.
   In addition
   $v\,(-27a_3^4 + 18a_1a_2a_3^3 - 4a_1^3a_3^3 + a_1^2a_2^2a_3^2 - 4a_2^3a_3^2)$
   $= v\,((-27a_3^2 + 18a_1a_2a_3 - 4a_1^3a_3 + a_2^2\,(a_1^2 - 4a_2))\,a_3^2)$.
   That means
   $v\,(disc\,(M(x))) \geq m$ if and only if
   $v\,(-27a_3^4 + 18a_1a_2a_3^3 - 4a_1^3a_3^3 + a_1^2a_2^2a_3^2 - 4a_2^3a_3^2) \geq \; m$ if and only if $v\,((-27a_3^2 + 18a_1a_2a_3 - 4a_1^3a_3 + a_2^2\,(a_1^2 - 4a_2))\,a_3^2) \geq m$
   if and only if $v(a_3^2) = 2v(a_3) \geq m$ and the result follows from lemma 5.4.

4. If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \mid a_2$ and $\mathfrak{p}_v \mid a_1$ then $M(x) \equiv x^4 \mod \mathfrak{p}_v$.
   It follows then from corollary 2.1 that there is a unique zero of π in $k(\pi)$ if and only if $M(x)$ is irreducible over k_v; which is equivalent to saying that $M(x) \mod \mathfrak{p}_v^n$ is irreducible, where $n = v\,(disc\,(M(x))) + 1$.

5. If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_2$ and $\mathfrak{p}_v \nmid a_1$
and in addition $\mathfrak{p}_v \nmid a_1^2 - 4a_2$ then the result follows the same way as it did for the case 3.
If we have instead $\mathfrak{p}_v \mid a_1^2 - 4a_2$ then since $a_1^2 - 4a_2 \equiv 0 \mod \mathfrak{p}_v$
$M(x) \equiv x^2(x^2+a_1x+a_2) \equiv x^2(x+\alpha_0)^2 \mod \mathfrak{p}_v$. with $\alpha_0 \not\equiv 0 \mod \mathfrak{p}_v$.
It follows from corollary 2.1 that there is a unique zero of π in $k(\pi)$ if and only if $M(x) \equiv M_1(x) \cdot M_2(x) \mod \mathfrak{p}_v^n$ with $M_1(x)$ and $M_2(x)$ irreducible over k_v and
$M_1(x) \equiv x^2 \mod \mathfrak{p}_v$ and $M_2(x) \equiv (x+\alpha_0)^2 \mod \mathfrak{p}_v$;
where $n = v\,(disc\,(M(x))) + 1$.
Since in this case $M(x)$ cannot be irreducible over k_v (otherwise it would be a power of an irreducible polynomial modulo $\mathfrak{p}_v$), this is then equivalent to saying that $M(x)$ has no root in k_v and the result follows.

◊

5.2.2 Endomorphism rings in an isogeny class defined by the Weil polynomial $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$.

As we did for the rank 3 case, the following result provides a more specific description of orders occurring as endomorphism ring of a rank 4 Drinfeld module in our isogeny class.

Proposition 5.7. *$M(x) = x^4+a_1x^3+a_2x^2+a_3x+\mu\mathfrak{p}_v^m$ is the Weil polynomial describing our isogeny class.*

1. *If $\mathfrak{p}_v \nmid a_3$ then an order $\mathcal{O}$ of $k(\pi)$ is the endomorphism ring of a Drinfeld module in the isogeny class defined by $M(x)$ if and only if the Frobenius $\pi \in \mathcal{O}$.*

2. *If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_2$ then we have the following:*
Let $M(x) \equiv (x^2+b_1x+b_2)(x^2+c_1x+c_2) \mod \mathfrak{p}_v^n$ (where $n = v\,(disc\,(M(x)))+1$) be a decomposition of $M(x)$ over the completion field k_v, where $x^2+b_1x+b_2$ is the irreducible factor of $M(x) \mod \mathfrak{p}_v^n$ such that
$x^2+b_1x+b_2 \equiv x^2 \mod \mathfrak{p}_v$. We denote $\Delta_0 = b_1^2 - 4b_2 = \lambda_0^2\delta_0$ with δ_0 square free in $A/\mathfrak{p}_v^nA$.
An order $\mathcal{O} = \langle 1, \tilde{\omega}_1, \tilde{\omega}_2, \tilde{\omega}_3\rangle$ of $k(\pi)$ is the endomorphism ring of a Drinfeld module in the isogeny class defined by $M(x)$ if and only if the Frobenius $\pi \in \mathcal{O}$ and there exists $\alpha_0,\ \alpha_1,\ \alpha_2,\ \alpha_3 \in A/\mathfrak{p}_v^nA$ with $(\alpha_0 + \alpha_1\tilde{\omega}_1 + \alpha_2\tilde{\omega}_2 + \alpha_3\tilde{\omega}_3)^2 = \delta_0$.

3. *If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \mid a_2$ then*
An order $\mathcal{O}$ of $k(\pi)$ occurs as endomorphism ring of a Drinfeld module in the isogeny class described by $M(x)$ if and only if the Frobenius $\pi \in \mathcal{O}$ and $\mathcal{O}$ is maximal at all the places of $k(\pi)$ lying over the place v (i.e. the norm of the conductor of $\mathcal{O}$ is relatively prime to $\mathfrak{p}_v$).

Proof:

1. If $\mathfrak{p} \nmid a_3$ then $M(x) \equiv x(x^3 + a_1x^2 + a_2x + a_3) \mod \mathfrak{p}_v$.
That means $\deg M_{loc}(x) = 1$. We recall that $M_{loc}(x)$ is the irreducible factor of $M(x)$ over the completion field k_v describing the unique zero of π in $k(\pi)$ lying over the place v of k (see corollary 3.2 for more details).
Therefore any order $\mathcal{O}$ containing π is already maximal at that zero of π described by $M_{loc}(x)$.
Hence an order $\mathcal{O}$ of $k(\pi)$ in this case, is the endomorphism ring of a Drinfeld module if and only if it contains π.

2. If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_2$ then we have the following:
$$M(x) \equiv x^2(x^2 + a_1x + a_2) \mod \mathfrak{p}_v$$
We know that an order $\mathcal{O}$ of $k(\pi)$ is the endomorphism ring of a Drinfeld module if and only if $\pi \in \mathcal{O}$ and $\mathcal{O}$ is maximal at the zero v_0 of π in $k(\pi)$ lying over the place v of k (see theorem 3.4).
But v_0 is described by the degree 2 irreducible polynomial
$M_{loc}(x) = x^2 + b_1x + b_2 \in A_v[x]$ such that $M_{loc}(x) \equiv x^2 \mod \mathfrak{p}_v$. The completion $\mathcal{O}_{v_0}$ of $\mathcal{O}$ at v_0 must therefore be the maximal order of the quadratic extension of k_v defined by $M_{loc}(x) = x^2 + b_1x + b_2$.
We know that the maximal order of that quadratic extension is given by $A_v + A_v \cdot \sqrt{\delta_0}$, where δ_0 is the square-free element of A_v such that $\Delta_0 = b_1^2 - 4b_2 = \lambda_0^2\delta_0$.
$\mathcal{O}_{v_0} = A_v + A_v \cdot \sqrt{\delta_0}$ if and only if $\sqrt{\delta_0} \in \mathcal{O}_{v_0}$. Especially, $\sqrt{\delta_0} \in \mathcal{O} \otimes A_v$.
Therefore $\mathcal{O}$ is the endomorphism ring of a Drinfeld module in the isogeny class defined by $M(x)$ if and only if $\pi \in \mathcal{O}$ and the polynomial $x^2 - \delta_0$ has a root in $\mathcal{O} \otimes A_v$.
i.e. if and only if $\pi \in \mathcal{O}$ and $(\alpha_0 + \alpha_1\tilde{\omega}_1 + \alpha_2\tilde{\omega}_2 + \alpha_3\tilde{\omega}_3)^2 = \delta_0$ for some $\alpha_i \in A_v,\ i = 0, 1, 2, 3$.
This is equivalent (Hensel lemma) to checking that
$\pi \in \mathcal{O}$ and $(\alpha_0 + \alpha_1\tilde{\omega}_1 + \alpha_2\tilde{\omega}_2 + \alpha_3\tilde{\omega}_3)^2 = \delta_0$
for some $\alpha_i \in A_v/\mathfrak{p}_v^nA_v = A/\mathfrak{p}_v^nA$. Where $n = v\left(disc\left(M(x)\right)\right) + 1 \geq v(\delta_0) + 1$.

3. If $\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \mid a_2$ then we have two cases.
   <u>**First case**</u>: If $\mathfrak{p}_v \mid a_1$ then we have the following:

   $$M(x) \equiv x^4 \mod \mathfrak{p}_v$$

   Thus the Weil polynomial $M(x)$ must be irreducible over the completion field k_v. In other words there is a unique place (the zero of π) of $k(\pi)$ extending the place v of k. Therefore the statement follows from theorem 3.4.
   <u>**Second case**</u>: If $\mathfrak{p}_v \nmid a_1$ then we have the following:

   $$M(x) \equiv x^3(x + a_1) \mod \mathfrak{p}_v$$

   That means the irreducible factor $M_{loc}(x)$ of $M(x)$ over the completion field k_v describing the zero of π in $k(\pi)$ satisfies $M_{loc}(x) \equiv x^3 \mod \mathfrak{p}_v$ (see corollary 3.2).
   That means the irreducible decomposition of $M(x)$ over the completion field k_v has the form $M(x) = M_{loc}(x)M_1(x)$ with
   $M_1(x) \equiv x + a_1 \mod \mathfrak{p}_v$. this implies that $\deg M_1(x) = 1$.
   Let us denote v_1 the place of $k(\pi)$ lying over v and described by $M_1(x)$. Since $\deg M_1(x) = 1$, the completion of the A-order $\mathcal{O}$ at the place v_1 is maximal.
   Therefore $\mathcal{O}$ is maximal at the zero v_0 of π (described by $M_{loc}(x)$) if and only if $\mathcal{O}$ is maximal at all the places (v_0 and v_1) of $k(\pi)$ lying over v. That is, $\mathcal{O} \otimes A_v$ is a maximal order of the k_v-algebra $k_v(\pi)$.
   Hence $\mathcal{O}$ occurs as the endomorphism ring of a Drinfeld module in the isogeny class defined by the Weil polynomial $M(x)$ if and only if the Frobenius $\pi \in \mathcal{O}$ and $\mathcal{O}$ is maximal at all the places of $k(\pi)$ lying over v (equivalently the norm of the conductor of $\mathcal{O}$ is relatively prime to $\mathfrak{p}_v$).

$\Diamond$

In the sequel, we compute the maximal order of the field $k(\pi)$ and compute the list of all the sub-orders of that maximal order occurring as endomorphism ring of a Drinfeld module in the isogeny class defined by the rank 4 Weil polynomial $M(x)$.
The general description of an explicit (like in quadratic and cubic fields) integral basis of (quartic) function fields is still so far a problem. Nevertheless, there are algorithms (Zassenhaus algorithm, Puisseux expansion, Montes algorithm, Frobenius based method) implemented in most of the computer algebra system to compute an integral basis of a function field. One can therefore assume the integral basis to be known and move forward directly

to the computation of orders occurring as endomorphism rings of Drinfeld modules.
We discuss in the follwing part the explicit description of integral basis for the very special case of biquadratic function field. We rely on the work of Wu and Scheidler in [25]

Integral basis of a cyclic biquadratic function field

Definition 5.2. *A biquadratic function field extension of k is a degree 4 function field extension of k that contains an intermediate quadratic subfield. It is said to be cyclic if it is Galois and the Galois group is $\mathbb{Z}_4$.*

Definition 5.3. *[Standard form]*
a polynomial $M_0(x) = x^4+c_1x^2+c_2x+c_3 \in A[x]$ is said to be in the standard form if there is no $c \in A$ such that $c^2 \mid c_1,\ c^3 \mid c_2$ and $c^4 \mid c_3$.

Remark 5.9. *Let $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$ be our Weil polynomial and $k(\pi)/k$ be the corresponding function field. If $char(k) \neq 2$, one can transform (by setting $x = y - \frac{a_1}{4}$) $M(x)$ into a polynomial of the form $y^4 + b_1y^2 + b_2y + b_3$. This polynomial is therefore converted into its standard form as follows:*
Let $b_1 = \mu_1 \prod_{i=1}^{n_1} b_{1i}^i,\ b_2 = \mu_2 \prod_{i=1}^{n_2} b_{2i}^i$ and $b_3 = \mu_3 \prod_{i=1}^{n_3} b_{3i}^i$ be the square-free factorizations of $b_1,\ b_2$ and b_3. We set $g_1 = \prod_{i=1}^{n_1} b_{1i}^{\lfloor \frac{i}{2} \rfloor},\ g_2 = \prod_{i=1}^{n_2} b_{2i}^{\lfloor \frac{i}{3} \rfloor}\ g_3 = \prod_{i=1}^{n_3} b_{3i}^{\lfloor \frac{i}{4} \rfloor}$. Consider $c_1 = \frac{b_1}{gcd(g_1,g_2,g_3)^2},\ c_2 = \frac{b_2}{gcd(g_1,g_2,g_3)^3},\ c_3 = \frac{b_3}{gcd(g_1,g_2,g_3)^4}$. The polynomial $M_0(x) = x^4+c_1x^2+c_2x+c_3 \in A[x]$ is in the standard form. In addition, π is a root of $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$ if and only if $\pi + \frac{a_1}{4}$ is a root of $y^4 + b_1y^2 + b_2y + b_3$ if and only if $\tilde{\pi} = \frac{\pi+\frac{a_1}{4}}{gcd(g_1,g_2,g_3)}$ is a root of $M_0(x)$. Also $k(\tilde{\pi}) = k(\pi + \frac{a_1}{4}) = k(\pi)$.

Proposition 5.8. *[25, theorem 5.1] Let $M(x) = x^4+a_1x^3+a_2x^2+a_3x+\mu Q$ be our Weil polynomial. We assume that the standard form of $M(x)$ is a biquadratic polynomial*

$$M_0(x) = x^4 + c_1x^2 + c_3.$$

The corresponding biquadratic function field $k(\pi) = k[x]/M(x) \cdot k[x]$ is cyclic if and only if $(c_1^2 - 4c_3)c_3$ is a square in $A = \mathbb{F}_q[T]$.

Proposition 5.9. *[25, theorem 7.6] We consider our cyclic biquadratic function field $k(\pi)$ as in the previous proposition.*
The discriminant of the function field $k(\pi)$ is given by:

$$disc\,(k(\pi)) = \frac{16G_0^3F_0^2}{D_0^2}$$

where $c_1^2 - 4c_3 = G_0S_0^2$, $\;c_3 = H_0T_0^2$ with G_0 and H_0 square-free.
$D_0 = gcd(G_0, S_0, T_0)$ and $F_0 = gcd(S_0, T_0)$.

Theorem 5.3. *[25, theorem 8.1] We consider the Weil polynomial $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$ which corresponding function field is $k(\pi) = k[x]/M(x) \cdot k[x]$. We assume that the standard form of $M(x)$ is given by a biquadratic polynomial $M_0(x) = x^4 + c_1x^2 + c_3$ which defines a cyclic biquadratic function field $k(\tilde{\pi}) = k[x]/M_0(x) \cdot k[x]$. An integral basis of $k(\tilde{\pi}) = k(\pi)$ is*

$$\left(1,\ \tilde{\pi},\ \frac{\tilde{\pi}^2 + c_1/2}{S_0},\ \frac{\tilde{\pi}^3 + C_0\tilde{\pi}}{E_0D_0}\right)$$

where,
$D_0 = gcd(G_0, S_0, T_0)$, $E_0 = lcm(S_0, T_0)$, $F_0 = gcd(S_0, T_0)$
$\lambda_1S_0 + \mu_1T_0 = F_0$, $\lambda_2E_0 + \mu_2D_0^2 = gcd(E_0, D_0^2) = D_0$
$C_0 = \mu_2c_1D_0\frac{\mu_1T_0/2+\lambda_1S_0}{F_0}$.

Let us now move to the computation of endomorphism rings of rank 4 Drinfeld modules in the isogeny classes defined by Weil polynomials of the form $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$.

Endomorphism rings

$M_0(x) = x^4 + c_1x^2 + c_2x + c_3$ is the standard form of the polynomial $M(x)$. π denotes the Frobenius endomorphism (which is a root of $M(x)$) and $\tilde{\pi}$ denotes the corresponding root of $M_0(x)$.
We know that a necessary condition for an A-order in the function field $k(\pi)$ to occur as endomorphism ring of a Drinfeld module in the isogeny class defined by the Weil polynomial $M(x)$ is that it must contain π. We proceed exactly the same way we did in the case of rank 3. We assume without loss of generality that the maximal order $\mathcal{O}_{max}$ of $k(\pi)$ is generated by the integral basis
$\mathcal{O}_{max} = \langle 1, \tilde{\pi}, \tilde{\pi}^2, \dfrac{\tilde{\pi}^3 + U\tilde{\pi}^2 + V\tilde{\pi} + W}{I}\rangle = \langle 1, \omega_1, \omega_2, \omega_3\rangle$.
Where the index $I = \sqrt{\frac{disc(M_0(x))}{disc(k(\pi))}}$.

Let $\mathcal{O} = \langle \tilde{\omega_0}, \tilde{\omega_1}, \tilde{\omega_2}, \tilde{\omega_3} \rangle$ be a sub-lattice of $\mathcal{O}_{max}$. A necessary condition for $\mathcal{O}$ to be an order is that $1 \in \mathcal{O}$. We can therefore without loss of generality assume that $\tilde{\omega_0} = 1$.

$$\mathcal{O} = \langle 1, \tilde{\omega_1}, \tilde{\omega_2}, \tilde{\omega_3} \rangle = \Big\{ \begin{pmatrix} \tilde{X} & \tilde{Y} & \tilde{Z} & \tilde{T} \end{pmatrix} \begin{pmatrix} 1 \\ \tilde{\omega_1} \\ \tilde{\omega_2} \\ \tilde{\omega_3} \end{pmatrix}, \quad \tilde{X},\ \tilde{Y},\ \tilde{Z},\ \tilde{T} \in A \Big\}$$

$\tilde{\omega_1},\ \tilde{\omega_2}$ and $\tilde{\omega_3} \in \mathcal{O}_{max}$. That means,

$$\begin{cases} \tilde{\omega_1} = a_1 + b_1\omega_1 + c_1\omega_2 + d_1\omega_3 \\ \tilde{\omega_2} = a_2 + b_2\omega_1 + c_2\omega_2 + d_2\omega_3 \\ \tilde{\omega_3} = a_3 + b_3\omega_1 + c_3\omega_2 + d_3\omega_3 \end{cases} \quad \text{for some } a_i, b_i, c_i, d_i \in A \quad i = 1,2,3.$$

That is,

$$\begin{pmatrix} 1 \\ \tilde{\omega_1} \\ \tilde{\omega_2} \\ \tilde{\omega_3} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix}}_{M} \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix}$$

There exists an invertible matrix $N \in GL_4(A)$ such that $N \cdot M = H$ where H is an upper triangular matrix of the form

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & b & d \\ 0 & 0 & c & e \\ 0 & 0 & 0 & f \end{pmatrix} \text{ with } \deg_T b < \deg_T c \text{ and } \deg_T d,\ \deg_T e < \deg_T f.$$

Suitable row operations on M help to recover such a matrix N. We can therefore assume without loss of generality that

$$\mathcal{O} = \langle 1, \tilde{\omega_1}, \tilde{\omega_2}, \tilde{\omega_3} \rangle = \Big\{ \begin{pmatrix} \tilde{X} & \tilde{Y} & \tilde{Z} & \tilde{T} \end{pmatrix} H \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix}, \quad \tilde{X},\ \tilde{Y},\ \tilde{Z},\ \tilde{T} \in A \Big\}$$

The A-lattice $\mathcal{O}$ is actually an order if and only if it contains $\tilde{\omega_1}^2$, $\tilde{\omega_2}^2$, $\tilde{\omega_3}^2$, $\tilde{\omega_1}\tilde{\omega_2}$, $\tilde{\omega_1}\tilde{\omega_3}$ and $\tilde{\omega_2}\tilde{\omega_3}$.

$\tilde{\omega_1}^2 = (a\omega_1 + b\omega_2 + d\omega_3)^2 = a^2\omega_1^2 + b^2\omega_2^2 + d^2\omega_3^2 + 2ab\omega_1\omega_2 + 2ad\omega_1\omega_3 + 2bd\omega_2\omega_3$.

$\tilde{\omega_2}^2 = (c\omega_2 + e\omega_3)^2 = c^2\omega_2^2 + e^2\omega_3^2 + 2ec\omega_2\omega_3$.

$\tilde{\omega_3}^2 = (f\omega_3)^2 = f^2\omega_3^2$

$\tilde{\omega_1}\tilde{\omega_2} = (a\omega_1 + b\omega_2 + d\omega_3)(c\omega_2 + e\omega_3) = bc\omega_2^2 + ed\omega_3^2 + ac\omega_1\omega_2 + ae\omega_1\omega_3 + (dc + be)\omega_2\omega_3$.

$\tilde{\omega_1}\tilde{\omega_3} = (a\omega_1 + b\omega_2 + d\omega_3)f\omega_3 = df\omega_3^2 + af\omega_1\omega_3 + bf\omega_2\omega_3$.

$\tilde{\omega_2}\tilde{\omega_3} = (c\omega_2 + e\omega_3)f\omega_3 = ef\omega_3^2 + cf\omega_2\omega_3$. That is,

$$\begin{pmatrix} \tilde{\omega_1}^2 \\ \tilde{\omega_2}^2 \\ \tilde{\omega_3}^2 \\ \tilde{\omega_1}\tilde{\omega_2} \\ \tilde{\omega_1}\tilde{\omega_3} \\ \tilde{\omega_2}\tilde{\omega_3} \end{pmatrix} = \underbrace{\begin{pmatrix} a^2 & b^2 & d^2 & 2ab & 2ad & 2bd \\ 0 & c^2 & e^2 & 0 & 0 & 2ec \\ 0 & 0 & 0 & f^2 & 0 & 0 \\ 0 & bc & ed & ac & ae & dc+be \\ 0 & 0 & df & 0 & af & bf \\ 0 & 0 & ef & 0 & 0 & cf \end{pmatrix}}_{M_1} \begin{pmatrix} \omega_1^2 \\ \omega_2^2 \\ \omega_3^2 \\ \omega_1\omega_2 \\ \omega_1\omega_3 \\ \omega_2\omega_3 \end{pmatrix}$$

Using the following equalities
$\tilde{\pi} = \omega_1,\ \tilde{\pi}^2 = \omega_2,\ \tilde{\pi}^3 = -W - V\omega_1 - U\omega_2 + I\omega_3$ and $\tilde{\pi}^4 = -c_3 - c_2\omega_1 - c_1\omega_2$.
One shows that

$$\begin{pmatrix} \omega_1^2 \\ \omega_2^2 \\ \omega_3^2 \\ \omega_1\omega_2 \\ \omega_1\omega_3 \\ \omega_2\omega_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ -c_3 & -c_2 & -c_1 & 0 \\ X_0 & X_1 & X_2 & X_3 \\ -W & -V & -U & I \\ Y_0 & Y_1 & Y_2 & U \\ Z_0 & Z_1 & Z_2 & V. \end{pmatrix}}_{M_2} \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix} \text{ Where}$$

$$\begin{cases} X_0 = \frac{-2UVW+2UWc_1-U^2c_3-W^2+Wc_2-2Vc_3+c_1c_3}{I^2} \\ X_1 = \frac{-2UV^2+2UVc_1-U^2c_2-Vc_2+c_1c_2-2Uc_3}{I^2} \\ X_2 = \frac{-2U^2V+U^2c_1+V^2-2Vc_1+c_1^2-Uc_2-c_3}{I^2} \\ X_3 = \frac{2UV-2Uc_1+2W-c_2}{I} \end{cases}$$

$$\begin{cases} Y_0 = \frac{-c_3-UW}{I} \\ Y_1 = \frac{W-UV-c_2}{I} \\ Y_2 = \frac{V-U^2-c_1}{I} \end{cases} \quad \text{and} \quad \begin{cases} Z_0 = \frac{c_1W-c_3U-VW}{I} \\ Z_1 = \frac{c_1V-c_3-c_2U-V^2}{I} \\ Z_2 = \frac{W-VU-c_2}{I} \end{cases}$$

Therefore

$$\begin{pmatrix} \tilde{\omega_1}^2 \\ \tilde{\omega_2}^2 \\ \tilde{\omega_3}^2 \\ \tilde{\omega_1}\tilde{\omega_2} \\ \tilde{\omega_1}\tilde{\omega_3} \\ \tilde{\omega_2}\tilde{\omega_3} \end{pmatrix} = M_1 M_2 H^{-1} \begin{pmatrix} 1 \\ \tilde{\omega_1} \\ \tilde{\omega_2} \\ \tilde{\omega_3} \end{pmatrix}$$

Remark 5.10. *$\mathcal{O}$ is an order if and only if $M_1M_2H^{-1} \in \mathscr{M}_{6\times 4}(A)$*

Let us investigate the orders occurring as endomorphism ring of a rank 4 Drinfeld module in our chosen isogeny class.
We know as a necessary condition that for $\mathcal{O}$ to be the endomorphism ring of a Drinfeld module we must have in addition to the condition mention in the remark above, $\pi \in \mathcal{O}$. In other words there must exist $a_0,\ b_0,\ c_0$ and $d_0 \in A$

such that $\pi = a_0 + b_0\tilde{\omega_1} + c_0\tilde{\omega_2} + d_0\tilde{\omega_3}$. But $\tilde{\pi} = \dfrac{\pi + \frac{a_1}{4}}{g}$. That is,
$\pi = g\tilde{\pi} - \frac{a_1}{4} = g\omega_1 - \frac{a_1}{4}$ where $g = \gcd(g_1, g_2, g_3)$
as defined in remark 5.9. $\tilde{\omega_1} = a\omega_1 + b\omega_2 + d\omega_3$, $\tilde{\omega_2} = c\omega_2 + e\omega_3$ and $\tilde{\omega_3} = f\omega_3$. That is,
$g\omega_1 - \frac{a_1}{4} = a_0 + b_0 a\omega_1 + (b_0 b + c_0 c)\omega_2 + (b_0 d + c_0 e + d_0 f)\omega_3$. We have then $a_0 = -\frac{a_1}{4}$, $b_0 a = g$, $b_0 b = -c_0 c$ and $b_0 d = -c_0 e - d_0 f$.
Thus a must divide g, c must divide $\frac{g}{a}b$ and f must divide $-\frac{g}{a}d + \frac{gb}{ac}e$. Hence

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & b & d \\ 0 & 0 & c & e \\ 0 & 0 & 0 & f \end{pmatrix} \text{ with } \deg e < \deg f,\ a \mid g,\ c \mid \frac{g}{a}b \text{ and } f \mid -\frac{g}{a}d + \frac{gb}{ac}e.$$

We summarize our discussion in the following theorem.

Theorem 5.4. *$A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$.
Let $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$ be a Weil polynomial.
In order to get a simple form $x^4 + b_1x^2 + b_2x + b_3$ of the Weil polynomial $M(x)$,
let $b_1 = -\dfrac{3a_1^2}{4} + a_2$, $b_2 = \dfrac{a_1^3}{8} - \dfrac{a_1a_2}{2} + a_3$ and $b_3 = -\dfrac{3a_1^4}{256} + \dfrac{a_1^2a_2}{16} - \dfrac{a_1a_3}{4} + \mu Q$ whose square-free factorization are given by
$b_1 = \mu_1 \prod_{i=1}^{n_1} b_{1i}^i$, $b_2 = \mu_2 \prod_{i=1}^{n_2} b_{2i}^i$, $b_3 = \mu_3 \prod_{i=1}^{n_3} b_{3i}^i$.
In order to get the standard form (in the sense we defined in 5.3) $M_0(x) = x^4 + c_1x^2 + c_2x + c_3$ of $M(x)$, we consider
$g_1 = \prod_{i=1}^{n_1} b_{1i}^{\lfloor \frac{i}{2} \rfloor}$, $g_2 = \prod_{i=1}^{n_2} b_{2i}^{\lfloor \frac{i}{3} \rfloor}$, $g_3 = \prod_{i=1}^{n_3} b_{3i}^{\lfloor \frac{i}{4} \rfloor}$.
We take off the highest square, cubic and quartic common divisors of b_1, b_2 and b_3 by setting $c_1 = \dfrac{b_1}{g^2}$, $c_2 = \dfrac{b_2}{g^3}$ and $c_3 = \dfrac{b_3}{g^4}$ where $g = \gcd(g_1, g_2, g_3)$.
$\tilde{\pi} = \dfrac{\pi + \frac{a_1}{4}}{g}$ is a root of $M_0(x)$. Let $I = ind(\tilde{\pi})$, U, V and $W \in A$ such that the maximal order of the function field $k(\pi) = k(\tilde{\pi})$ is given by*

$$\mathcal{O}_{max} = \langle 1, \tilde{\pi}, \tilde{\pi}^2, \frac{\tilde{\pi}^3 + U\tilde{\pi}^2 + V\tilde{\pi} + W}{I} \rangle$$

Where the index $I = \sqrt{\frac{disc(M_0(x))}{disc(k(\pi))}}$. *We consider the matrix*

$$M_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ -c_3 & -c_2 & -c_1 & 0 \\ X_0 & X_1 & X_2 & X_3 \\ -W & -V & -U & I \\ Y_0 & Y_1 & Y_2 & U \\ Z_0 & Z_1 & Z_2 & V. \end{pmatrix} \quad \textit{Where}$$

$$\begin{cases} X_0 = \frac{-2UVW+2UWc_1-U^2c_3-W^2+Wc_2-2Vc_3+c_1c_3}{I^2} \\ X_1 = \frac{-2UV^2+2UVc_1-U^2c_2-Vc_2+c_1c_2-2Uc_3}{I^2} \\ X_2 = \frac{-2U^2V+U^2c_1+V^2-2Vc_1+c_1^2-Uc_2-c_3}{I^2} \\ X_3 = \frac{2UV-2Uc_1+2W-c_2}{I} \end{cases}$$

$$\begin{cases} Y_0 = \frac{-c_3-UW}{I} \\ Y_1 = \frac{W-UV-c_2}{I} \\ Y_2 = \frac{V-U^2-c_1}{I} \end{cases} \qquad \textit{and} \qquad \begin{cases} Z_0 = \frac{c_1W-c_3U-VW}{I} \\ Z_1 = \frac{c_1V-c_3-c_2U-V^2}{I} \\ Z_2 = \frac{W-VU-c_2}{I} \end{cases}$$

The endomorphism rings of Drinfeld modules in the isogeny class defined by the Weil polynomial $M(x)$ *are:*

$$\begin{aligned} \mathscr{O} = \quad & A + A \cdot \left[a\tilde{\pi} + b\tilde{\pi}^2 + d\frac{\tilde{\pi}^3 + U\tilde{\pi}^2 + V\tilde{\pi} + W}{I}\right] + \\ & A \cdot \left[c\tilde{\pi}^2 + e\frac{\tilde{\pi}^3 + U\tilde{\pi}^2 + V\tilde{\pi} + W}{I}\right] + A \cdot \left[f\frac{\tilde{\pi}^3 + U\tilde{\pi}^2 + V\tilde{\pi} + W}{I}\right] \end{aligned}$$

such that $M_1M_2H^{-1} \in \mathscr{M}_{6\times 4}(A)$. *Where*

$$M_1 = \begin{pmatrix} a^2 & b^2 & d^2 & 2ab & 2ad & 2bd \\ 0 & c^2 & e^2 & 0 & 0 & 2ec \\ 0 & 0 & 0 & f^2 & 0 & 0 \\ 0 & bc & ed & ac & ae & dc+be \\ 0 & 0 & df & 0 & af & bf \\ 0 & 0 & ef & 0 & 0 & cf \end{pmatrix} \quad \textit{and } H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & b & d \\ 0 & 0 & c & e \\ 0 & 0 & 0 & f \end{pmatrix}$$

$$\begin{cases} a & \textit{runs through the divisors of } g \\ c & \textit{runs through the divisors of } I \\ b & \textit{runs through the polynomials in } A \textit{ whose degree are less than} \\ & \deg c \textit{ and such that } c \mid \frac{g}{a}b \\ f & \textit{runs through the divisors of } I \textit{ and} \\ d & \textit{and } e \textit{ run through the polynomials in } A \textit{ whose degrees are less than} \\ & \deg f \textit{ and such that } f \mid -\frac{g}{a}d + \frac{gb}{ac}e \end{cases}$$

And if in addition

- *$\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \mid a_2$, we must have $gcd(\mathfrak{p}_v, acf) = 1$.*
- *$\mathfrak{p}_v \mid a_3$ and $\mathfrak{p}_v \nmid a_2$ there must exists $\alpha_0,\ \alpha_1,\ \alpha_2,\ \alpha_3 \in A/\mathfrak{p}_v^n$ such that $(\alpha_0 + \alpha_1\tilde{\omega_1} + \alpha_2\tilde{\omega_2} + \alpha_3\tilde{\omega_3})^2 = \delta_0$ (see proposition 5.7).*

Proof: The proof stems straightforwardly from the discussion we had before. Concerning the fact that c and f divide I, it comes from the following:

$$\begin{pmatrix} 1 \\ \tilde{\omega_1} \\ \tilde{\omega_2} \\ \tilde{\omega_3} \end{pmatrix} = H \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix}$$

That is, $disc\,(1, \tilde{\omega_1}, \tilde{\omega_2}, \tilde{\omega_3}) = (acf)^2 disc\,(1, \omega, \omega_2, \omega_3)$
But there exists $N \in \mathscr{M}_4\,(A)$ such that

$$\begin{pmatrix} 1 \\ \tilde{\pi} \\ \tilde{\pi}^2 \\ \tilde{\pi}^3 \end{pmatrix} = N \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix}$$

i.e. $disc\,(1, \tilde{\pi}, \tilde{\pi}^2, \tilde{\pi}^3) = (detN)^2\,(acf)^2 disc\,(1, \omega, \omega_2, \omega_3)$
Hence acf divides $I = ind(\tilde{\pi})$ and thus c and f divide I.
The condition $gcd(\mathfrak{p}_v, acf) = 1$ comes from the fact that the norm of the conductor of $\mathcal{O}$ must be prime to $\mathfrak{p}_v$. $\Diamond$

If $g_1,\ g_2$ and g_3 are relatively prime (i.e. g is a unit in A), in particular if $b_1 = -\dfrac{3a_1^2}{4} + a_2$ is square-free or $b_2 = \dfrac{a_1^3}{8} - \dfrac{a_1 a_2}{2} + a_3$ is cubic-free or $b_3 = -\dfrac{3a_1^4}{256} + \dfrac{a_1^2 a_2}{16} - \dfrac{a_1 a_3}{4} + \mu Q$ is quartic-free or $b_1,\ b_2$ and b_3 are relatively prime, then we have the following:

Corollary 5.3. *The orders occurring as endomorphism ring of a Drinfeld module in the isogeny class defined by $M(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + \mu Q$ (with standard form $M_0(x) = x^4 + c_1x^2 + c_2x + c_3$) are the ones given by*

$$\mathscr{O} = A + A\cdot\omega_1 + A\cdot(c\omega_2 + e\omega_3) + A\cdot f\omega_3$$

such that $M_1M_2H^{-1} \in \mathscr{M}_{6\times 4}\,(A)$. Where M_2 is the same matrix as before,

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & c^2 & e^2 & 0 & 0 & 2ec \\ 0 & 0 & 0 & f^2 & 0 & 0 \\ 0 & 0 & 0 & c & e & 0 \\ 0 & 0 & 0 & 0 & f & 0 \\ 0 & 0 & ef & 0 & 0 & cf \end{pmatrix} \quad \text{and } H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & c & e \\ 0 & 0 & 0 & f \end{pmatrix}$$

c and f run through the divisors of the index $I = ind(\tilde{\pi})$ and e runs through the polynomials in A whose degrees are less than $\deg f$. *And if in addition*

- $\mathfrak{p}_v \mid a_3$ *and* $\mathfrak{p}_v \mid a_2$, *we must have* $gcd(\mathfrak{p}_v, acf) = 1$.
- $\mathfrak{p}_v \mid a_3$ *and* $\mathfrak{p}_v \nmid a_2$ *there must exists* $\alpha_0,\ \alpha_1,\ \alpha_2,\ \alpha_3 \in A/\mathfrak{p}_v^n$ *such that* $(\alpha_0 + \alpha_1\tilde{\omega}_1 + \alpha_2\tilde{\omega}_2 + \alpha_3\tilde{\omega}_3)^2 = \delta_0$ *(see proposition 5.7).*

5.2.3 Isomorphism classes for rank 4 Drinfeld modules

$A = \mathbb{F}_3[T]$, $k = \mathbb{F}_3(T)$. $L = \mathbb{F}_{27} = \mathbb{F}_3(\alpha)$, where $\alpha^3 + 2\alpha + 1 = 0$, is the A-field defined by the ring homomorphism $\gamma : A \longrightarrow L$, $f(T) \longmapsto f(0)$.
The kernel of γ is given by $\langle \mathfrak{p}_v \rangle = Ker\gamma = \langle T \rangle = T \cdot A$.
We consider the polynomial $M(x) = x^4 + (T+1)x^2 + (T^2-1)x + T^3 \in A[x]$.
Claim: $M(x)$ is a Weil polynomial.
Indeed,
$M(x)$ already fulfils the restrictions on the coefficients of Weil polynomials.
Following our algorithm 2.1, we have in addition

- $s = \lceil \frac{\deg T^3}{4} \rceil = 1$ and
  $D = disc\,(M(x)) = T^9 + T^8 + 2T^7 + 2T^6 + 2T^5 + 2T^2 + 2$.
  i.e. $h = v_\infty(D) + sr(r-1) = -9 + 4 \times 3 + 1 = 4$.
  $M_0(x) = x^4 + \left(\frac{1}{T} + \frac{1}{T^2}\right)x^2 + \left(\frac{1}{T} - \frac{1}{T^3}\right)x + \frac{1}{T}$ is irreducible over the completion field k_∞ as Einsenstein polynomial.
  Therefore there is a unique place of $k(\pi)$ lying over the place at ∞ of k.
- $\mathfrak{p}_v = T$ does not divide $a_3 = T^2 - 1$.
  Thus there is a unique zero of π in $k(\pi)$ lying over the place v of k.

Hence $M(x)$ is a Weil polynomial.
We consider then the isogeny class of rank 4 Drinfeld modules defined by the Weil polynomial $M(x)$.
We aim to compute the isomorphism classes of Drinfeld modules lying in that isogeny class.
Following the same procedure we did for the rank 3 case, we implemented a SAGE code to compute first of all the Drinfeld modules in that isogeny class and we gathered them with respect to their J-invariants and fine isomorphy invariants, in order to get the isomorphism classes.
The results are given in the following tables:
Each table represents an isomorphism class.

$\phi_1(T)$
$\alpha^2\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + \alpha\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2)\tau + \alpha^2\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$2\alpha\tau + \tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + 2\tau^4$
$(2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+2)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + 2\alpha\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$\tau + (2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+1)\tau^4$

$\phi_2(T)$
$\alpha^2\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+2)\tau + \alpha^2\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+\alpha)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + 2\tau^4$
$2\alpha\tau + \tau^2 + (2\alpha^2+\alpha+1)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha+2)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + 2\alpha\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+1)\tau^4$
$\tau + (2\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + \alpha\tau^4$

$\phi_3(T)$
$\alpha^2\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + \alpha\tau^4$
$(\alpha^2+\alpha+1)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha^2+2)\tau + \alpha^2\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha+1)\tau^4$
$2\alpha\tau + \tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + 2\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha+2)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + 2\alpha\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+1)\tau^4$
$\tau + (2\alpha+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+2\alpha)\tau^4$

$\phi_4(T)$
$\alpha^2\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + 2\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+\alpha+1)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha^2+2)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + 2\alpha\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+2)\tau + (2\alpha+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha+1)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + \alpha\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + \alpha^2\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(2\alpha+2)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha+1)\tau^4$
$\tau + \tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+\alpha+2)\tau^4$

$\phi_5(T)$
$\alpha^2\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+\alpha+1)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + \alpha\tau^4$
$(2\alpha^2+2)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + 2\alpha\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (2\alpha+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha+1)\tau^4$
$(2\alpha+1)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + 2\tau^4$
$(2\alpha^2+\alpha+1)\tau + \alpha^2\tau^2 + (2\alpha^2+2\alpha)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha+2)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$\tau + \tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+1)\tau^4$

$\phi_6(T)$
$\alpha^2\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + 2\tau^4$
$(2\alpha^2+2)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+\alpha)\tau + 2\alpha\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(\alpha^2+2)\tau + (2\alpha+2)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha+1)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha^2+\alpha+1)\tau + \alpha^2\tau^2 + (2\alpha^2+1)\tau^3 + \alpha\tau^4$
$(2\alpha+2)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$\tau + \tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$

$\phi_7(T)$
$\alpha^2\tau+(\alpha+1)\tau^2+(2\alpha^2+2)\tau^3+(\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau+(2\alpha^2+\alpha)\tau^2+(2\alpha^2+2)\tau^3+(\alpha+1)\tau^4$
$(\alpha^2+\alpha+1)\tau+(2\alpha^2+1)\tau^2+(2\alpha^2+2)\tau^3+(\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2)\tau+(\alpha^2+2\alpha+2)\tau^2+(2\alpha^2+2)\tau^3+2\tau^4$
$(\alpha^2+\alpha)\tau+2\alpha^2\tau^2+(2\alpha^2+2)\tau^3+2\alpha^2\tau^4$
$(\alpha^2+2)\tau+(2\alpha^2+2\alpha)\tau^2+(2\alpha^2+2)\tau^3+(2\alpha^2+\alpha)\tau^4$
$2\alpha\tau+(2\alpha^2+\alpha+2)\tau^2+(2\alpha^2+2)\tau^3+(2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+1)\tau+2\tau^2+(2\alpha^2+2)\tau^3+(\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha+1)\tau+(\alpha^2+1)\tau^2+(2\alpha^2+2)\tau^3+(2\alpha^2+2\alpha)\tau^4$
$(2\alpha^2+\alpha+1)\tau+(\alpha+2)\tau^2+(2\alpha^2+2)\tau^3+(2\alpha^2+1)\tau^4$
$(2\alpha+2)\tau+(\alpha^2+\alpha+2)\tau^2+(2\alpha^2+2)\tau^3+\alpha\tau^4$
$(2\alpha^2+2\alpha+1)\tau+(2\alpha^2+2\alpha+2)\tau^2+(2\alpha^2+2)\tau^3+(\alpha+2)\tau^4$
$\tau+\alpha\tau^2+(2\alpha^2+2)\tau^3+(2\alpha^2+\alpha+2)\tau^4$

$\phi_8(T)$
$\alpha^2\tau+(\alpha+1)\tau^2+2\alpha^2\tau^3+(\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha)\tau+(2\alpha^2+\alpha)\tau^2+2\alpha^2\tau^3+(2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+\alpha+1)\tau+(2\alpha^2+1)\tau^2+2\alpha^2\tau^3+(2\alpha^2+1)\tau^4$
$(2\alpha^2+2)\tau+(\alpha^2+2\alpha+2)\tau^2+2\alpha^2\tau^3+\alpha\tau^4$
$(\alpha^2+\alpha)\tau+2\alpha^2\tau^2+2\alpha^2\tau^3+(\alpha+2)\tau^4$
$(\alpha^2+2)\tau+(2\alpha^2+2\alpha)\tau^2+2\alpha^2\tau^3+(2\alpha^2+\alpha+2)\tau^4$
$2\alpha\tau+(2\alpha^2+\alpha+2)\tau^2+2\alpha^2\tau^3+(\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+1)\tau+2\tau^2+2\alpha^2\tau^3+(\alpha+1)\tau^4$
$(\alpha^2+2\alpha+1)\tau+(\alpha^2+1)\tau^2+2\alpha^2\tau^3+(\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau+(\alpha+2)\tau^2+2\alpha^2\tau^3+2\tau^4$
$(2\alpha+2)\tau+(\alpha^2+\alpha+2)\tau^2+2\alpha^2\tau^3+2\alpha^2\tau^4$
$(2\alpha^2+2\alpha+1)\tau+(2\alpha^2+2\alpha+2)\tau^2+2\alpha^2\tau^3+(2\alpha^2+\alpha)\tau^4$
$\tau+\alpha\tau^2+2\alpha^2\tau^3+(2\alpha^2+2\alpha+2)\tau^4$

$\phi_9(T)$
$\alpha^2\tau + (\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha^2+2)\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+\alpha)\tau + 2\alpha^2\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+2)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+1)\tau^3 + \alpha\tau^4$
$2\alpha\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha+1)\tau + 2\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (\alpha+2)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha+1)\tau^4$
$(2\alpha+2)\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+1)\tau^3 + 2\tau^4$
$\tau + \alpha\tau^2 + (2\alpha^2+1)\tau^3 + 2\alpha^2\tau^4$

$\phi_{10}(T)$
$\alpha^2\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+\alpha+1)\tau + \alpha\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2)\tau + (\alpha+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + 2\tau^4$
$(\alpha^2+\alpha)\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+2)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+1)\tau + 2\alpha^2\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha+2)\tau + 2\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + \alpha\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (\alpha+2)\tau^4$
$\tau + (\alpha+2)\tau^2 + (2\alpha^2+2\alpha+2)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$

$\phi_{11}(T)$
$\alpha^2\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+\alpha+1)\tau + \alpha\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha^2+2)\tau + (\alpha+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + \alpha\tau^4$
$(\alpha^2+\alpha)\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+1)\tau + 2\alpha^2\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + 2\tau^4$
$(2\alpha+2)\tau + 2\tau^2 + (2\alpha^2+2\alpha)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$\tau + (\alpha+2)\tau^2 + (2\alpha^2+2\alpha)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$

$\phi_{12}(T)$
$\alpha^2\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + \alpha\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha^2+2)\tau + (\alpha+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+\alpha)\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+2)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + \alpha\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha+1)\tau + 2\alpha^2\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha+1)\tau^4$
$(2\alpha+2)\tau + 2\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + 2\tau^4$
$\tau + (\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + 2\alpha^2\tau^4$

$\phi_{13}(T)$
$\alpha^2\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha^2+2)\tau + 2\alpha^2\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+\alpha)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+2)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + \alpha\tau^4$
$2\alpha\tau + 2\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha+1)\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha+1)\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + \alpha\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + 2\tau^4$
$\tau + (\alpha+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + 2\alpha^2\tau^4$

$\phi_{14}(T)$
$\alpha^2\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2)\tau + 2\alpha^2\tau^2 + (2\alpha^2+\alpha)\tau^3 + 2\tau^4$
$(\alpha^2+\alpha)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+2)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$2\alpha\tau + 2\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+1)\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + \alpha\tau^4$
$(2\alpha^2+2\alpha+1)\tau + \alpha\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha+2)\tau^4$
$\tau + (\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$

$\phi_{15}(T)$
$\alpha^2\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha^2+2)\tau + 2\alpha^2\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + \alpha\tau^4$
$(\alpha^2+\alpha)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$2\alpha\tau + 2\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+1)\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + 2\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha^2+2\alpha+1)\tau + \alpha\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$\tau + (\alpha+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$

$\phi_{16}(T)$
$\alpha^2\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha+2)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2)\tau^3 + 2\tau^4$
$(2\alpha^2+2)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+\alpha)\tau + \alpha\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(\alpha^2+2)\tau + (\alpha+1)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$2\alpha\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha+1)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha^2+\alpha+1)\tau + 2\alpha^2\tau^2 + (2\alpha^2+2)\tau^3 + \alpha\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$\tau + 2\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$

$\phi_{17}(T)$
$\alpha^2\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + 2\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha^2+2)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + \alpha\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+2)\tau + (\alpha+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$2\alpha\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha+1)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + \alpha\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha^2+\alpha+1)\tau + 2\alpha^2\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha+1)\tau^4$
$\tau + 2\tau^2 + (2\alpha^2+\alpha+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$

$\phi_{18}(T)$
$\alpha^2\tau + (\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + \alpha\tau^4$
$(2\alpha^2+2)\tau + (2\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + \alpha\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (\alpha+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$2\alpha\tau + (2\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha+1)\tau^4$
$(2\alpha+1)\tau + (2\alpha^2+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha^2+2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + 2\tau^4$
$(2\alpha^2+\alpha+1)\tau + 2\alpha^2\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (2\alpha^2+\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$\tau + 2\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+1)\tau^4$

$\phi_{19}(T)$
$\alpha^2\tau + (2\alpha+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + \alpha\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha^2+2)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + \alpha^2\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha+1)\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha+1)\tau + \tau^2 + (2\alpha^2+\alpha+2)\tau^3 + 2\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (\alpha^2+1)\tau^4$
$\tau + 2\alpha\tau^2 + (2\alpha^2+\alpha+2)\tau^3 + (2\alpha^2+2\alpha)\tau^4$

$\phi_{20}(T)$
$\alpha^2\tau + (2\alpha+2)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha+1)\tau^4$
$(2\alpha^2+2)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + \alpha^2\tau^2 + (2\alpha^2+2)\tau^3 + 2\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+2)\tau^3 + 2\alpha^2\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha+1)\tau + \tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2)\tau^3 + (2\alpha^2+1)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2)\tau^3 + \alpha\tau^4$
$\tau + 2\alpha\tau^2 + (2\alpha^2+2)\tau^3 + (\alpha+2)\tau^4$

$\phi_{21}(T)$
$\alpha^2\tau + (2\alpha+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+\alpha+1)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(2\alpha^2+2)\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+\alpha)\tau + \alpha^2\tau^2 + (2\alpha^2+\alpha)\tau^3 + \alpha\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha+2)\tau^4$
$2\alpha\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(2\alpha+1)\tau + \tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha+1)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (2\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha+2)\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + 2\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+\alpha)\tau^3 + 2\alpha^2\tau^4$
$\tau + 2\alpha\tau^2 + (2\alpha^2+\alpha)\tau^3 + (2\alpha^2+\alpha)\tau^4$

$\phi_{22}(T)$
$\alpha^2\tau + (2\alpha^2+2\alpha+1)\tau^2 + 2\alpha^2\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+\alpha+1)\tau^2 + 2\alpha^2\tau^3 + (\alpha^2+1)\tau^4$
$(\alpha^2+\alpha+1)\tau + 2\alpha\tau^2 + 2\alpha^2\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(2\alpha^2+2)\tau + (2\alpha+2)\tau^2 + 2\alpha^2\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+\alpha)\tau + (\alpha^2+2\alpha)\tau^2 + 2\alpha^2\tau^3 + \alpha\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+2)\tau^2 + 2\alpha^2\tau^3 + (\alpha+2)\tau^4$
$2\alpha\tau + (2\alpha^2+\alpha+1)\tau^2 + 2\alpha^2\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(2\alpha+1)\tau + \alpha^2\tau^2 + 2\alpha^2\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha^2+\alpha)\tau^2 + 2\alpha^2\tau^3 + (\alpha+1)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (\alpha^2+2\alpha+1)\tau^2 + 2\alpha^2\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(2\alpha+2)\tau + \tau^2 + 2\alpha^2\tau^3 + 2\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + 2\alpha^2\tau^3 + 2\alpha^2\tau^4$
$\tau + (2\alpha+1)\tau^2 + 2\alpha^2\tau^3 + (2\alpha^2+\alpha)\tau^4$

$\phi_{23}(T)$
$\alpha^2\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + 2\tau^4$
$(\alpha^2+\alpha+1)\tau + 2\alpha\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + 2\alpha^2\tau^4$
$(2\alpha^2+2)\tau + (2\alpha+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(\alpha^2+\alpha)\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+1)\tau^4$
$2\alpha\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$(2\alpha+1)\tau + \alpha^2\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+1)\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + \alpha\tau^4$
$(2\alpha^2+\alpha+1)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha+2)\tau^4$
$(2\alpha+2)\tau + \tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$\tau + (2\alpha+1)\tau^2 + (2\alpha^2+2\alpha+1)\tau^3 + (\alpha+1)\tau^4$

$\phi_{24}(T)$
$\alpha^2\tau + (2\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + \alpha\tau^4$
$(\alpha^2+2\alpha)\tau + (\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha+2)\tau^4$
$(\alpha^2+\alpha+1)\tau + 2\alpha\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+\alpha+2)\tau^4$
$(2\alpha^2+2)\tau + (2\alpha+2)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+2\alpha+2)\tau^4$
$(\alpha^2+\alpha)\tau + (\alpha^2+2\alpha)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha+1)\tau^4$
$(\alpha^2+2)\tau + (\alpha^2+2)\tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+\alpha+2)\tau^4$
$2\alpha\tau + (2\alpha^2+\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + 2\tau^4$
$(2\alpha+1)\tau + \alpha^2\tau^2 + (2\alpha^2+1)\tau^3 + 2\alpha^2\tau^4$
$(\alpha^2+2\alpha+1)\tau + (\alpha^2+\alpha)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+\alpha)\tau^4$
$(2\alpha^2+\alpha+1)\tau + (\alpha^2+2\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+2\alpha+2)\tau^4$
$(2\alpha+2)\tau + \tau^2 + (2\alpha^2+1)\tau^3 + (\alpha^2+1)\tau^4$
$(2\alpha^2+2\alpha+1)\tau + (2\alpha^2+2)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+2\alpha)\tau^4$
$\tau + (2\alpha+1)\tau^2 + (2\alpha^2+1)\tau^3 + (2\alpha^2+1)\tau^4$

Conclusion

Let us recall that we aimed in this work to classify the rank r Drinfeld modules in the sense of answering the questions below. For $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$

1. What are the Weil polynomials (or Weil numbers) in $A[x]$ defining the isogeny classes of rank r Drinfeld modules?

2. Given that the endomorphism algebra $End\phi \otimes_A k$ is an isogeny invariant, describe and list the orders in the endomorphism algebra corresponding to a given isogeny class, occurring as endomorphism ring of a Drinfeld module in that chosen isogeny class.

3. Describe the L-isomorphism classes in a given isogeny class of rank r Drinfeld modules defined over the finite field L.

Concerning the first question, we picked a degree r_1 polynomial (r_1 divisor of r) and we investigated following the definition of a Weil number and it comes out that the rank r Weil polynomials are the polynomials in $A[x]$ of the form

$$M(x) = x^{r_1} + a_1 x^{r_1-1} + \cdots + a_{r_1-1}x + \mu \mathfrak{p}_v^{\frac{m}{r_2}} \in A[x] \quad \text{with } r = r_1 \cdot r_2 \text{ and } \mu \in \mathbb{F}_q^*.$$

Where $M(x)$ can be assumed WLOG to be a separable polynomial and such that the following conditions are fulfilled.

- $\deg a_i \leq \frac{im \deg \mathfrak{p}_v}{r}$ and $r_2 \mid m$.

- for $s = \lceil \frac{m \deg \mathfrak{p}_v}{r} \rceil$ and $h = -\deg(disc\,(M(x))) + sr(r-1) + 1$ we have $M_0(x) = x^{r_1} + \frac{a_1}{T^s} x^{r_1-1} + \cdots + \frac{a_{r_1-1}}{T^{s(r_1-1)}} x + \mu \frac{\mathfrak{p}_v^{\frac{m}{r_2}}}{T^{sr_1}}$ is irreducible modulo $\frac{1}{T^h}$.

- for $n = v\,(disc\,(M(x))) + 1$ and for any irreducible factor $f_0(x)$ of $M(x) \mod \mathfrak{p}_v^n$, we have $Res\left(f_0(x), \frac{M(x)}{f_0(x)}\right) \not\equiv 0 \mod \mathfrak{p}_v$.

For the second question, we have restricted ourselves to the isogeny classes for which the corresponding endomorphism algebra is a field. For this case, the corresponding Weil polynomial we have described in the first question has the form

$$M(x) = x^r + a_1x^{r-1} + \cdots + a_{r-1}x + \mu\mathfrak{p}_v^m.$$

We have basically shown that an order $\mathcal{O}$ in our endomorphism algebra is the endomorphism ring of a Drinfeld module in that chosen isogeny class if and only if $\mathcal{O}$ contains the Frobenius endomorphism π and $\mathcal{O}$ is maximal at the unique zero v_0 of π in $k(\pi)$ lying over the place v of k.
We have also listed for the case $r = 3$ and the case $r = 4$ all the possible orders of $k(\pi)$ that are endomorphism rings of Drinfeld modules.
Concerning the last question, we came out with the isomorphism invariants we called fine isomorphy invariants, which together with the (already known) J-invariants describe the L-isomorphism classes in a given isogeny class of rank r Drinfeld modules defined over the finite field L. We have also explained for some concrete examples how the isomorphism classes can be computed.

One can notice for the second question that we made a restriction to isogeny classes for which the endomorphism algebra is a field. As a consequence of this, we have worked with very special types of Weil polynomials. As perspectives for future works, it would be good to extend the investigation to the general case. That is, what happen for the isogeny classes whose endomorphism algebra is not a field? What are the orders occurring as endomorphism rings of Drinfeld modules? A good starting point could be to look at the rank 4 Weil polynomials of the form $x^2 + ax + \mu\mathfrak{p}_v^{\frac{m}{2}}$ (see 5.2.1). The endomorphism algebra here is a quaternion algebra over the quadratic extension (defined by our Weil Polynomial) $k(\pi)$ of k. One should first of all describe that quaternion algebra. The next step is to compute the maximal orders in such a quaternion algebra and for a fixed maximal order, describe and compute all the orders occurring as endomorphism ring of a Drinfeld module in our rank 4 isogeny class.

Bibliography

[1] Samuele Anni and Vladimir Dokchitser. Constructing hyperelliptic curves with surjective galois representations. *Transactions of the American Mathematical Society*, 2019.

[2] Tobias Bembom. Arithmetic problems in cubic and quartic function fields. *arXiv preprint arXiv:1007.1319*, 2010.

[3] Simon R Blackburn, Carlos Cid, and Steven D Galbraith. Cryptanalysis of a cryptosystem based on drinfeld modules. *IACR Cryptology ePrint Archive*, 2003:223, 2003.

[4] Nicolas Bourbaki. *Eléments de mathématique: Chapitres 3 et 4*. Hermann, 1962.

[5] Ching-Li Chai, Brian Conrad, and Frans Oort. *Complex multiplication and lifting problems*, volume 195. American Mathematical Soc., 2013.

[6] Keith Conrad. Lecture notes in galois theory, August 2014. `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/separable1.pdf`.

[7] Sumita Garai and Mihran Papikian. Computing endomorphism rings and frobenius matrices of drinfeld modules. *arXiv preprint arXiv:1908.01805*, 2019.

[8] Ernst-Ulrich Gekeler. Frobenius distributions of drinfeld modules over finite fields. *Transactions of the American Mathematical Society*, 360(4):1695–1721, 2008.

[9] Roland Gillard, Franck Leprevost, Alexei Panchishkin, and Xavier-François Roblot. Utilisation des modules de drinfeld en cryptologie. *Comptes Rendus Mathematique*, 336(11):879–882, 2003.

[10] David Goss. *Basic Structures of Function Field Arithmetic*, volume 35. Springer, 1998.

[11] Urs Hartl. Uniformizing the stacks of abelian sheaves. In *Number fields and function fieldstwo parallel worlds*, pages 167–222. Springer, 2005.

[12] Antoine Joux and Anand Kumar Narayanan. Drinfeld modules are not for isogeny based cryptography.

[13] Sudesh K Khanduja and Sanjeev Kumar. On irreducible factors of polynomials over complete fields. *Journal of Algebra and its Applications*, 12(01):1250125, 2013.

[14] Nikolas Kuhn and Richard Pink. Finding endomorphisms of drinfeld modules. *arXiv preprint arXiv:1608.02788*, 2016.

[15] Eric Landquist, Pieter Rozenhart, Renate Scheidler, Jonathan Webster, and Qingquan Wu. An explicit treatment of cubic function fields with applications. *Canadian Journal of Mathematics*, 62:787–807, 2010.

[16] Pascual Llorente and Enric Nart. Effective determination of the decomposition of the rational primes in a cubic field. *Proceedings of the American Mathematical Society*, 87(4):579–585, 1983.

[17] David Mumford, Chidambaran Padmanabhan Ramanujam, and IU I Manin. *Abelian varieties*, volume 108. Oxford university press Oxford, 1974.

[18] Jürgen Neukirch. *ALGEBRAIC NUMBER THEORY*, volume 322. Springer, 1999.

[19] Igor Yu Potemine. Minimal terminal -factorial models of drinfeld coarse moduli schemes. *Mathematical Physics, Analysis and Geometry*, 1(2):171–191, 1998.

[20] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2013.

[21] Renate Scheidler. Algorithmic aspects of cubic function fields. In *International Algorithmic Number Theory Symposium*, pages 395–410. Springer, 2004.

[22] Henning Stichtenoch. *Algebraic Function Fields and Codes*. Springer, 2009.

[23] M Van Der Put, Gekeler Eu, and M Reversat. *Drinfeld Modules, Modular Schemes And Applications*. World Scientific, 1997.

[24] Joachim von Zur Gathen and Silke Hartlieb. *Factorization of polynomials modulo small prime powers.* Univ.-Gesamthochsch.-Paderborn, Fachbereich Mathematik-Informatik, 1996.

[25] Qingquan Wu and Renate Scheidler. An explicit treatment of biquadratic function fields. *Contributions to Discrete Mathematics*, 2(1), 2007.

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