

Drinfeld modules and their application to factor polynomials

by

Tovohery Hajatiana Randrianarisoa

*Thesis presented in partial fulfilment of the requirements for
the degree of Master of Science in Mathematics in the
Faculty of Science at Stellenbosch University*



Department of Mathematics,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Supervisor: Prof. Florian Breuer

December 2012

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Signature:
T.H. Randrianarisoa

Date: 2012/12/12

Copyright © 2012 Stellenbosch University
All rights reserved.

Abstract

Drinfeld modules and their application to factor polynomials

T.H. Randrianarisoa

*Department of Mathematics,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.*

Thesis: MSc (Maths)

December 2012

Major works done in Function Field Arithmetic show a strong analogy between the ring of integers \mathbb{Z} and the ring of polynomials over a finite field $\mathbb{F}_q[T]$. While an algorithm has been discovered to factor integers using elliptic curves, the discovery of Drinfeld modules, which are analogous to elliptic curves, made it possible to exhibit an algorithm for factorising polynomials in the ring $\mathbb{F}_q[T]$. In this thesis, we introduce the notion of Drinfeld modules, then we demonstrate the analogy between Drinfeld modules and Elliptic curves. Finally, we present an algorithm for factoring polynomials over a finite field using Drinfeld modules.

Uittreksel

Drinfeld modules en hul toepassings tot faktor polinome

(“Drinfeld modules and their application to factor polynomials”)

T.H. Randrianarisoa

*Departement Matematik,
Universiteit van Stellenbosch,
Privaatsak X1, Matieland 7602, Suid Afrika.*

Tesis: MSc (Wisk)

Desember 2012

'n Groot deel van die werk wat reeds in funksieliggaam rekenkunde voltooi is toon 'n sterk verband tussen die ring van heelgetalle, \mathbb{Z} , en die ring van polinome oor 'n eindige liggaam, $\mathbb{F}[T]$. Terwyl daar alreeds 'n algoritme, wat gebruik maak van elliptiese kurwes, ontwerp is om heelgetalle te faktoreer, het die ontdekking van Drinfeld modules, wat analoog is aan elliptiese kurwes, dit moontlik gemaak om 'n algoritme te konstrueer om polinome in die ring $\mathbb{F}[T]$ te faktoreer.

In hierdie tesis maak ons die konsep van Drinfeld modules bekend deur sekere aspekte daarvan te bestudeer. Ons gaan voort deur 'n voorbeeld te voorsien wat die analoog tussen Drinfeld modules en elliptiese kurwes illustreer. Uiteindelik, deur gebruik te maak van Drinfeld modules, bevestig ons hierdie analoog deur die algoritme vir die faktorisering van polinome oor eindige liggame te verskaf.

Acknowledgements

I would like to express my sincere gratitude to the following people and organisations. Without them this thesis would not have been written.

First of all, there is Prof. Florian Breuer, I would like to thank him for the support, patience and guidance through the realization of this thesis.

My thanks also to AIMS and the Stellenbosch University for their financial and material support.

I also would like to thank my family, friends for their support during the years of study. A special thanks to them for their support, comments, suggestions and help. Among them, there are my mother, father, brothers and sister. And also some friends: Frances, Andry, RONALDA and Darlison.

Finally, I thank **GOD**, the one who made everything possible.

Dedications

This thesis is dedicated to my parents.

“Live as you were to die tomorrow. Learn as if you were to live forever.”

M.Ghandi

Contents

Declaration	i
Abstract	ii
Uittreksel	iii
Acknowledgements	iv
Dedications	v
Contents	vi
1 Introduction	1
1.1 Elliptic curves and integer factorisation	1
1.1.1 ECM algorithm	1
1.2 Carlitz module	2
1.2.1 The Carlitz exponential function	3
1.3 Outline	7
2 Drinfeld modules over fields	8
2.1 Generalising the polynomial ring	8
2.2 Torsion modules	12
2.3 The notion of Drinfeld modules	14
2.3.1 The module structure	14
2.3.2 The category of Drinfeld modules	14
2.4 Analytic construction of Drinfeld modules	22
2.4.1 Complex theory	22
2.4.2 Lattices associated to Drinfeld modules	23
3 Analogy with elliptic curves	27
3.1 The Weierstrass function	27
3.2 On the side of elliptic curves	31
3.2.1 Tate module on Elliptic curves	32
3.3 On the side of Drinfeld modules	34
3.3.1 Tate module on Drinfeld modules	36

<i>CONTENTS</i>	vii
4 Factorisation of polynomials	38
4.1 Drinfeld modules over rings	38
4.2 Factorisation of polynomials	43
4.2.1 Algorithms	44
4.2.2 Complexity	48
5 Conclusion	55
Appendices	56
A Singular program	57
B Big example	65
List of References	69

Chapter 1

Introduction

Interest for factoring polynomials has increased as it has many applications in the field of Computer algebra, Coding theory, Cryptography. For example, it can be applied to compute discrete logarithms, which is an important problem in public-key cryptography, over finite fields of prime-power order.

There are already many algorithms for factoring polynomials over finite field but research still continues to develop better methods. The Berlekamp's and the Cantor-Zassenhaus' algorithms are examples of algorithms to factor polynomials over finite field. However since the development of the theory of Drinfeld modules, which is a "generalisation" of the notion of elliptic curves, a new algorithm was developed independently by A. Panchishkin and I. Potemine (Panchishkin and Potemine, 1989), and also by van der Heiden (van der Heiden, 2004).

1.1 Elliptic curves and integer factorisation

As we have said earlier, the notion of Drinfeld modules is a "generalisation" of the notion of Elliptic curves. Thus one might think if an analogous theory exists on the side of Drinfeld modules, if we have one in the case of elliptic. Indeed, the algorithm we will develop is analogous to the following algorithm, called *Lenstra elliptic curve factorization* or *elliptic curve factorization method* (ECM). So it is natural to first see that algorithm.

1.1.1 ECM algorithm

In this algorithm we will deal with an elliptic curve E of the generic form i.e. its equation is of the form

$$y^2 = x^3 + ax + b. \quad (1.1.1)$$

In addition to the points on the curve we also have another point \mathcal{O} and we can form an abelian group with identity \mathcal{O} . More explanation about this can be found in Silverman (2009).

Here are the steps of the algorithm. Suppose n is the integer to be factored and we assume that 2 or 3 doesn't divide n . We can also suppose that n is not a perfect power.

1. Choose an elliptic curve $y^2 = x^3 + ax + b \pmod{n}$ and a point $P = (x_0, y_0)$ on the curve. We choose the integer a in such a way that $\gcd(4a^3 + 27c^2, n) \neq n$.
2. If $\gcd(4a^3 + 27c^2, n) \neq 1$, then we get a proper factor of n . Otherwise go to the next step.
3. Choose e as a product of many small prime numbers and compute eP which is the e times sum of P w.r.t the group law.
4. eP is of the form $(\frac{p}{u^2}, \frac{q}{u^3})$ and we set $v = \gcd(u, n)$.
5. If $v \neq 1, n$, then we have a trivial factor of n . If $v = n$ we go to step 3 by choosing a smaller e . Otherwise for $v = 1$, we can either choose another curve in step 1 or increase e in step 3.

This algorithm uses the trial and error method. Namely, one execution of this algorithm gives us a proper factor for some choice of curve and also for some choice of e . Indeed, let us assume that E_p is the set of points satisfying the equation (1.1.1) modulo p , where p is a proper factor of n . Suppose also that $\#E_p$ divides e . Then, for a rational point P on the curve E , $e\bar{P} = \mathcal{O}$, where \bar{P} is the reduction of P modulo p . One shows that p divides u . Hence, we get a proper factor $\gcd(u, n)$, assuming that, for our choice of curve and e , n is not a divisor of u . Therefore, the algorithm gives a proper factor for appropriate choices of elliptic curve. For more details on this, we can refer to Silverman and Tate (1994, chap. IV).

1.2 Carlitz module

The notion of Elliptic modules was introduced by Drinfeld, in his paper Drinfeld (1974), as a “generalisation” of the notion of elliptic curves. Nowadays, this concept is known as Drinfeld modules. Although, the article was published in 1974, a particular case of Drinfeld modules was already studied by Carlitz in the 1930's (Carlitz, 1932a, 1935). This is a Drinfeld module of rank 1 and is called Carlitz modules.

So before we study the notion of Drinfeld modules, let us briefly see the simplest case which is the Carlitz module.

Define the ring $A = \mathbb{F}[T]$ as the ring of polynomials in the variable T with constants in \mathbb{F} , where \mathbb{F} is a finite field of prime characteristic p and cardinal q . Let $k = \mathbb{F}(T)$ be the fraction field of A . Let us denote by ∞ the place of k given by the element T^{-1} . Notice that, the ring A is exactly, the ring

of elements of k such that the only poles are at ∞ . The place ∞ induces a topology on k and let us denote by k_∞ the completion of k w.r.t. this topology. The algebraic closure \bar{k}_∞ of k_∞ is not complete but if we take the completion \mathbf{C}_∞ of \bar{k}_∞ , we see that \mathbf{C}_∞ is both complete and algebraically closed.

Remark 1.2.1. This setup has the following equivalence between number field and function field:

$$\begin{array}{l} \text{Number field: } \mathbb{Z} \quad \mathbb{Q} \quad \mathbb{R} \quad \mathbb{C} \quad \mathbb{C} \\ \text{Function field: } A \quad k \quad k_\infty \quad \bar{k}_\infty \quad \mathbf{C}_\infty \end{array}$$

1.2.1 The Carlitz exponential function

Let j be an integer. We define $[j] = T^{q^j} - T \in A$. Let us also define π by

$$\pi = \prod_{j=1}^{\infty} \left(1 - \frac{[j]}{[j+1]} \right).$$

We will soon see that this product is well defined in k_∞ . Let us first assume this fact, so that we can define an A -lattice, πA , of \mathbf{C}_∞ . This lattice is of dimension 1, so that the object we will construct is called of rank 1. To do the construction, let us work out the exponential function,

$$e_A(z) = z \prod_{\lambda \in A - \{0\}} \left(1 - \frac{z}{\lambda} \right).$$

Let n be a non-negative integer and let us denote the set of polynomials in A with degree less than n by $A_n = \{a \in A : \deg a < n\}$. We define for $n \geq 0$,

$$e'_{A_n}(z) = \prod_{a \in A_n} (z - a).$$

Definition 1.2.2. We define $L_0 = D_0 = 1$, and for $n \geq 1$,

$$L_n = \prod_{j=1}^n [j] \quad \text{and} \quad F_n = \prod_{j=0}^{n-1} [n-j]^{q^j}.$$

For the function e'_{A_n} , Carlitz has shown the following property (Carlitz, 1932b):

Theorem 1.2.3. *Let $n \geq 0$ be an integer. Then,*

$$e'_{A_n} = \sum_{i=0}^n (-1)^{n-i} z^{q^i} \frac{F_n}{F_i L_{n-i}^{q^i}}.$$

Taking some polynomials and their product in the ring A , we get the next results, as found in Goss (1997, chap. 3).

Proposition 1.2.4.

- $\prod_{\substack{a \text{ monic in } A \\ \deg a = n}} a = F_n,$
- $\prod_{\substack{a \in A - \{0\} \\ \deg a = n}} a = (-1)^n \frac{F_n}{L_n},$
- $F_n = \left(T^{q^i} - T\right) F_{n-1}^q.$

Now, as a and $-a$ are both in A_n , then we also have

$$e'_{A_n}(z) = \prod_{a \in A_n} (z - a) = \prod_{a \in A_n} (z + a). \quad (1.2.1)$$

We multiply the equality in theorem 1.2.3 by $(-1)^n \frac{L_n}{F_n}$. Using the proposition 1.2.4 and the equation (1.2.1), we have

$$z \prod_{\substack{a \in A - \{0\} \\ \deg a < n}} \left(\frac{z}{a} + 1\right) = \sum_{i=0}^n (-1)^i z^{q^i} \frac{L_n}{F_i L_{n-i}^{q^i}}.$$

Again, interchanging a and $-a$, we get

$$z \prod_{\substack{a \in A - \{0\} \\ \deg a < n}} \left(1 - \frac{z}{a}\right) = \sum_{i=0}^n (-1)^i z^{q^i} \frac{L_n}{F_i L_{n-i}^{q^i}}. \quad (1.2.2)$$

Moreover, as we will see later in the proposition 2.4.6,

$$e_{A_n}(z) := z \prod_{\substack{a \in A - \{0\} \\ \deg a < n}} \left(1 - \frac{z}{a}\right),$$

converges in \mathbf{C}_∞ when $n \rightarrow \infty$. But k_∞ is complete, then the limit must be in k_∞ . Hence, $\sum_{i=0}^n (-1)^i z^{q^i} \frac{L_n}{F_i L_{n-i}^{q^i}}$ converges in k_∞ .

Lemma 1.2.5. Suppose, $\pi_i := \frac{[1]_{q^{i-1}}}{L_i}$, then,

$$\pi_i = \prod_{j=1}^{i-1} \left(1 - \frac{[j]}{[j+1]}\right).$$

Hence, π_i converges to $\pi := \prod_{j=1}^{\infty} \left(1 - \frac{[j]}{[j+1]}\right)$.

Proof. We have,

$$\begin{aligned} \prod_{j=1}^{i-1} \left(1 - \frac{[j]}{[j+1]} \right) &= \prod_{j=1}^{i-1} \left(\frac{[j+1] - [j]}{[j+1]} \right) \\ &= \prod_{j=1}^{i-1} \left(\frac{[1]^{q^j}}{[j+1]} \right) \\ &= \frac{\prod_{j=0}^{i-1} [1]^{q^j}}{L_i} \\ &= \frac{[1]^{\frac{q^i-1}{q-1}}}{L_i}. \end{aligned}$$

What remains to show is the convergence since the limit will come automatically. But $\frac{[1]^{\frac{q^i-1}{q-1}}}{L_i}$ converges in k_∞ as it is a Cauchy sequence in that field which is complete. \square

Now, $e_{A_n}(z) = \sum_{i=0}^n (-1)^i z^{q^i} \frac{L_n}{F_i L_{n-i}^{q^i}}$, then, as $\pi_i \rightarrow \pi$, we get

$$\begin{aligned} e_{A_n}(z) &= \sum_{i=0}^n (-1)^i z^{q^i} \frac{\pi_{n-i}^{q^i} [1]^{\frac{q^n-1}{q-1}}}{[1]^{\frac{q^n-q^i}{q-1}} \pi_n F_i} \\ &= \frac{1}{\pi_n} \sum_{i=0}^n (-1)^i z^{q^i} \frac{\pi_{n-i}^{q^i} [1]^{\frac{q^i-1}{q-1}}}{F_i}. \end{aligned} \quad (1.2.3)$$

Obviously, $\lim e_{A_n} = e_A$. This suggest us the following theorem, which we will not prove here:

Theorem 1.2.6. *The series*

$$\frac{1}{\pi_n} \sum_{i=0}^n (-1)^i z^{q^i} \frac{\pi_{n-i}^{q^i} [1]^{\frac{q^i-1}{q-1}}}{F_i},$$

converges as $n \rightarrow \infty$ and

$$e_A(z) = \frac{1}{\pi} \sum_{i=0}^{\infty} (-1)^i z^{q^i} \frac{\pi^{q^i} [1]^{\frac{q^i-1}{q-1}}}{F_i}.$$

Remark 1.2.7. The theorem 1.2.6 does not follow directly from the equation (1.2.3). The problem is here that the index n is inside the summation as well as it is also the order of the summation. More details are in Goss (1997, chap. 3)

We now, set ξ to be a $(q-1)$ -th root of $[1]$, thus we get

$$\begin{aligned} e_A(z) &= \frac{1}{\pi} \sum_{i=0}^{\infty} (-1)^i z^{q^i} \frac{\pi^{q^i} [1]_{q-1}^{q^i-1}}{F_i} \\ &= \frac{1}{\pi [1]_{q-1}} \sum_{i=0}^{\infty} (-1)^i z^{q^i} \frac{\pi^{q^i} [1]_{q-1}^{q^i}}{F_i} \\ &= \frac{1}{\pi \xi} \sum_{i=0}^{\infty} (-1)^i z^{q^i} \frac{(\pi \xi)^{q^i}}{F_i}. \end{aligned}$$

From all of these, we may now define the Carlitz exponential function to be $e_C(z) := e_{\pi \xi A}(z)$.

Proposition 1.2.8. *The Carlitz exponential function satisfies*

$$\pi \xi e_A(z) = e_C(\pi \xi z).$$

Moreover it has the complex multiplication

$$e_C(Tz) = T e_C(z) - e_C(z)^q.$$

Proof. We have

$$e_A(z) = z \prod_{a \in A - \{0\}} \left(1 - \frac{z}{a}\right) = \frac{1}{\pi \xi} \sum_{i=0}^{\infty} (-1)^i z^{q^i} \frac{(\pi \xi)^{q^i}}{F_i}.$$

Now,

$$\begin{aligned} e_{\pi \xi A}(z) &= z \prod_{a \in A - \{0\}} \left(1 - \frac{z}{\pi \xi a}\right) \\ &= \pi \xi \frac{z}{\pi \xi} \prod_{a \in A - \{0\}} \left(1 - \frac{z}{\pi \xi a}\right) \\ &= \pi \xi e_A\left(\frac{z}{\pi \xi}\right). \end{aligned}$$

For the second assertion, we have, from above,

$$e_C(z) = \sum_{i=0}^{\infty} (-1)^i \frac{z^{q^i}}{F_i}.$$

Hence,

$$\begin{aligned} T e_C(z) - e_C(Tz) &= T \sum_{i=0}^{\infty} (-1)^i \frac{z^{q^i}}{F_i} - \sum_{i=0}^{\infty} (-1)^i T^{q^i} \frac{z^{q^i}}{F_i} \\ &= \sum_{i=0}^{\infty} (-1)^i \left(T - T^{q^i}\right) \frac{z^{q^i}}{F_i} \end{aligned}$$

By proposition 1.2.4, we get

$$\begin{aligned}
 Te_C(z) - e_C(Tz) &= \sum_{i=1}^{\infty} (-1)^{i-1} \frac{z^{q^i}}{F_{i-1}^q} \\
 &= \sum_{i=0}^{\infty} (-1)^i \frac{z^{q^{i+1}}}{F_i^q} \\
 &= \left(\sum_{i=0}^{\infty} (-1)^i \frac{z^{q^{i+1}}}{F_i^q} \right)^q \\
 &= e_C(z)^q.
 \end{aligned}$$

Note that $(-1)^{iq} = (-1)^i$ is obvious for an odd characteristic p . For the characteristic $p = 2$, we use the fact that $-1 = 1$. \square

As we will see later, such an elliptic module gives rise to a twisted polynomials $\phi_T = T - \tau$.

1.3 Outline

To conclude the first chapter let us now describe briefly the content of this thesis. We will generalise the two previous sections we have seen in this first chapter. In Chapter 2, we will introduce the notion of Drinfeld modules over an arbitrary field. There we will see how we can construct Drinfeld modules over the field \mathbf{C}_∞ . The analogy mentioned earlier will be studied in Chapter 3, where we will investigate it more closely for the Tate modules. Then, in Chapter 4, we will develop the algorithm for factoring polynomials which is equivalent to the ECM we have seen above; but before that we explain the notion of Drinfeld modules over rings. Finally we will conclude in Chapter 5 and then, in the appendix, we implement this algorithm using **SINGULAR** (Decker *et al.*, 2011). We will also give one example to explain some procedures in the program.

Chapter 2

Drinfeld modules over fields

Let \mathbb{F} be a finite field, of characteristic p , with $q = p^r$ elements and let k/\mathbb{F} be a function field with field of constants \mathbb{F} . We fix a place of k , which we denote by ∞ . The degree of ∞ is denoted by d_∞ . We set A to be the ring of all elements of k with the only poles at ∞ . After that, we assume L is an extension of the field \mathbb{F} . If we set τ to be the q -Frobenius endomorphism over \mathbb{F} , then all the polynomials in the variable τ form a non-commutative ring, the skew polynomial ring, which we denote by $L\langle\tau\rangle$. The multiplicative law of the later ring is defined as follow,

$$a\tau^m \cdot b\tau^n = ab^{q^m} \tau^{m+n}.$$

2.1 Generalising the polynomial ring

Generally, when we define Drinfeld modules, we do not restrict ourself to a ring $A = \mathbb{F}[T]$. Our construction of A is more general and we still have to keep some property for that ring. For example, we have the following proposition.

Proposition 2.1.1. *A is integrally closed in k . And therefore A is a Dedekind domain.*

Proof. Let \mathcal{R} , be the integral closure of A in k . Let x be an element of \mathcal{R} such that the integral dependence for x over A is,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0. \quad (2.1.1)$$

First, we want to show that $v_P(x) \geq 0$ for all places P of k different from the ∞ . Suppose it is not the case for some place $P \neq \infty$ of k .

We know that $v_P(a_i) \geq 0$ for all $0 \leq i < n$. Therefore

$$(n-i)v_P(x) + iv_P(x) < v_P(a_i) + iv_P(x), \quad \text{for all } 0 \leq i < n.$$

Thus for all $0 \leq i < n$, we have $v_P(a_i x^i) > v_P(x^n)$. Hence,

$$\min_{0 \leq i \leq n-1} \{v_P(a_i x^i)\} > v_P(x^n). \quad (2.1.2)$$

From the equation (2.1.1),

$$v_P(x^n) = v_P(a_{n-1}x^{n-1} + \cdots + a_0).$$

By the property of valuation,

$$v_P(x^n) \geq \min \{v_P(a_{n-1}x^{n-1}), \dots, v_P(a_0)\}. \quad (2.1.3)$$

And we see that we have a contradiction between (2.1.2) and (2.1.3), therefore $v_P(x) \geq 0$. Thus, we have $\mathcal{R} \subset A$. The other inclusion is obvious so that finally we have $\mathcal{R} = A$ i.e. A is integrally closed.

For the second part of the theorem, Suppose a is an element of A having a pole only at ∞ . Then, as a matter of fact (see Zariski *et al.*, 1975, chap. V, Theorem. 19), the integral closure \mathcal{B} of $\mathbb{F}[a]$ in k is a Dedekind domain. We want to show that $\mathcal{B} = A$. We just show that A is integrally closed so that $\mathcal{B} \subset A$.

Notice that, for a place P different from ∞ , $A = \bigcap_{P \neq \infty} R_P$ so that $\mathcal{B} \subset R_P$, where R_P is the valuation ring of k at P . Recall that R_P has a unique maximal ideal P . As P is a maximal ideal of R_P , then P is a prime ideal of R_P . And we have $P \cap \mathcal{B}$ is a nonzero ideal because, if it is not the case, therefore, since the fraction field of \mathcal{R} is k , we have an inclusion of k into R_P/P . But since R_P/P is finite over \mathbb{F} , thus it would be the case for k , which is impossible since k is not algebraic over \mathbb{F} .

Therefore $P \cap \mathcal{B}$ is also a prime ideal of $R_P \cap \mathcal{B} = \mathcal{B}$, but \mathcal{B} is a Dedekind domain, then $P \cap \mathcal{B}$ is maximal in \mathcal{B} . Furthermore, the localisation, $\mathcal{B}_{P \cap \mathcal{B}}$, of \mathcal{B} at $P \cap \mathcal{B}$ is a subring of R_P . But this localisation is discrete valuation ring, then it should be maximal. Thus $\mathcal{B}_{P \cap \mathcal{B}} = R_P$.

Therefore we have

$$A = \bigcap_{P \neq \infty} \mathcal{B}_{P \cap \mathcal{B}}. \quad (2.1.4)$$

Implicitly, from a place of k which is not the place at infinity, we get a maximal ideal of \mathcal{B} . Now let us take a maximal ideal \mathcal{M} of \mathcal{B} , then $\mathcal{B}_{\mathcal{M}}$ is a place (here we refer to the place as the valuation ring not the maximal ideal!) of k . And this is different from the place at infinity since it contains a . Consequently, we have a one-to-one correspondence between the places of k different from the infinity and the maximal ideal of \mathcal{B} . And then, the equality (2.1.4) becomes

$$A = \bigcap_{\mathcal{M} \text{ maximal in } \mathcal{B}} \mathcal{B}_{\mathcal{M}}.$$

And from a property of a Dedekind domain, $\bigcap_{\mathcal{M} \text{ maximal in } \mathcal{B}} \mathcal{B}_{\mathcal{M}} = \mathcal{B}$ and therefore $A = \mathcal{B}$.

□

Generalising the ring A implies that we also generalise the notions from polynomial ring. Hence,

Lemma 2.1.2. *If A is a Dedekind domain contained in k and $a \in A$, then for a prime ideal I of A , if the localization of A at I gives a place of k with maximal ideal P , we have $v_P(a) = m$, where m is the power of I in the decomposition of (a) as factor of prime ideals of A .*

Proof. Suppose $(a) = I^m \prod_k J_k^{m_k}$ is the factorization of the ideal generated by (a) , then we have

$$aA_I = I^m \prod_k J_k^{m_k} A_I.$$

Now, $J_k A_I$ is an ideal of A_I . An element of P is of the form $\frac{i}{s}$, where $i \in I$ and $s \notin I$. Taking an element j of J_k which is not in I , we have $\frac{i}{s} = j \frac{i}{sj}$. And the last one is an element of $J A_I$. Thus $P \subset J_k A_I$. And since this inclusion is strict, by the maximality of P , we have $J_k A_I = A_I$.

Therefore $(a) A_I = I^m A_I = P^m$. And then $v_P(a) = m$. □

Definition 2.1.3. For an element a of A , we define $\deg a = -v_\infty(a) d_\infty$.

Remark 2.1.4. A place of k is given by a discrete valuation ring R with maximal ideal P . One show that we actually have a one-to-one correspondence between places different from ∞ and the prime ideals of A by the following correspondence:

$$P(\text{ideal of } A) \Leftrightarrow (A_P, P A_P).$$

From this correspondence, sometimes we refer to the place P as the prime ideal of A . Moreover, the lemma 2.1.2 and the fact that $A/P^m \cong A_P/(P A_P)^m$ allow us to define v_P and $\deg P$ with the same notions whenever we are thinking of P as a place of k , or a prime ideal of A .

Theorem 2.1.5. *If $a \in A$, then the dimension of $A/(a)$ over \mathbb{F} is equal to $\deg a$.*

Proof. If the factorisation of (a) is $\prod_P P^{v_P(a)}$, P running through the prime (thus maximal) ideals of A , then the Chinese remainder theorem gives us

$$A/(a) = \bigoplus_P A/P^{v_P(a)}.$$

Therefore the dimension of $A/(a)$ is equal to $\sum_P \dim_{\mathbb{F}} A/P^{v_P(a)}$, P is running through all the prime ideals of A .

Now, since P is a maximal ideal of A so that $A/P^{v_P(a)}$ is isomorphic to $A_P/(P A_P)^{v_P(a)}$, then

$$A/(a) = \bigoplus_P A_P/(P A_P)^{v_P(a)},$$

P is running through all the prime ideals of A .

Now, PA_P is a principal ideal, then $(PA_P)^{i-1} / (PA_P)^i \sim A_P / PA_P$. On the other hand

$$A_P / (PA_P)^{v_P(a)-1} \sim \left(A_P / (PA_P)^{v_P(a)} \right) / \left((PA_P)^{v_P(a)-1} / (PA_P)^{v_P(a)} \right).$$

But for two vectorial spaces $W \subset V$ over \mathbb{F} , we have $\dim_{\mathbb{F}} V/W = \dim_{\mathbb{F}} V - \dim_{\mathbb{F}} W$. And therefore,

$$\dim_{\mathbb{F}} A_P / (PA_P)^{v_P(a)} = v_P(a) \deg(PA_P),$$

(PA_P is actually the place corresponding to the prime P), and then we have

$$\dim_{\mathbb{F}} A / (a) = \sum_P v_P(a) \deg(PA_P).$$

As P running through all the prime ideals of A , then PA_P is running through all the places of k different from ∞ . And then

$$\dim_{\mathbb{F}} A / (a) = \sum_P v_P(a) \deg P,$$

where P is now running through all the places of k , different from ∞ . As the degree of the principal divisor (a) is equal to zero, then $\sum_P v_P(a) \deg P = -v_{\infty}(a) d_{\infty}$. Therefore

$$\dim_{\mathbb{F}} A / (a) = \deg a.$$

□

Proposition 2.1.6. *Let Cl_A denotes the class group of A as a Dedekind domain; \mathcal{D} , the group of divisors of k ; \mathcal{P} , the group of principal divisors; \mathcal{D}_0 , the group of divisors of degree zero. Then the following sequence is exact,*

$$(0) \longrightarrow \mathcal{D}_0 / \mathcal{P} \longrightarrow \text{Cl}_A \longrightarrow \mathbb{Z} / (d_{\infty}) \longrightarrow (0).$$

And thus, if $\#\text{Cl}_A = h_A$, then h_A is finite with $h_A = d_{\infty} h_k$, where h_k is the class number of k .

Proof. We saw, in remark 2.1.4, that there is a one-to-one correspondance between the prime ideals of A and the places of k different from ∞ . Thus, we can regard Cl_A as the subgroup of \mathcal{D} , generated by places different from ∞ , modulo the subgroup of principal divisors without ∞ (i.e. the elements $\prod_{P \neq \infty} P^{v_P(a)}, a \in k^*$). So we construct the second morphism in the sequence as $D = \prod_{P \neq \infty} P^{v_P(D)} \infty^{v_{\infty}(D)} \mapsto \prod_{P \neq \infty} P^{v_P(D)}$. And this is obviously injective. The third morphism is nothing else than the degree of a divisor modulo d_{∞} . Since the degree of a principal divisor is equal to zero, this morphism is well defined. And it is injective since, for $m \in \mathbb{Z} / (d_{\infty})$, we take $D = P^m$, where

P is a place of degree 1 (This exist by Schmidt's Theorem (Schmidt, 1931)). To complete the proof of the exactness of the sequence, we need to show that the image Im of the second morphism is equal to the kernel Ker of the third morphism. The degree of the element $\sum_{P \neq \infty} P^{v_P(D)} \infty^{v_\infty(D)} \in \mathcal{D}_0/\mathcal{P}$ being equal to zero, hence $Im \subset Ker$. If $\deg \prod_{P \neq \infty} P^{v_P(D)} = md_\infty$, then we just complete it by ∞^m to get the other inclusion.

The remaining part of the proposition follows as h_k is finite. \square

2.2 Torsion modules

It is normal that we study the torsion modules over a Dedekind domain. Let A , be a Dedekind domain and assume M is an A -module. Recall that a torsion submodule of M is, for a non-zero ideal \mathfrak{J} of A , defined by

$$M[\mathfrak{J}] = \{m \in M : mx = 0, \forall x \in \mathfrak{J}\}.$$

For two relatively prime ideals of A , \mathfrak{J}_1 and \mathfrak{J}_2 , there are some elements $x \in \mathfrak{J}_1$ and $y \in \mathfrak{J}_2$ such that $x + y = 1$. Thus any elements m of $M[\mathfrak{J}_1\mathfrak{J}_2]$ can be written as $mx + my = m$. By the definition of the torsion modules, we see that this sum is actually direct, i.e.

$$M[\mathfrak{J}_1\mathfrak{J}_2] = M[\mathfrak{J}_1] \oplus M[\mathfrak{J}_2]. \quad (2.2.1)$$

By induction, this implies

$$M[\mathfrak{J}_1^{k_1}\mathfrak{J}_2^{k_2} \dots \mathfrak{J}_n^{k_n}] = M[\mathfrak{J}_1^{k_1}] \oplus M[\mathfrak{J}_2^{k_2}] \oplus \dots \oplus M[\mathfrak{J}_n^{k_n}], \quad (2.2.2)$$

where the \mathfrak{J}_i 's are relatively prime.

Definition 2.2.1. Let \mathfrak{J} be a maximal ideal of A . We define the \mathfrak{J} -primary component of a module M , $M[\mathfrak{J}^\infty]$, to be the union of the torsion submodules of M given by the powers of \mathfrak{J} i.e.

$$M[\mathfrak{J}^\infty] = \cup_{l=1}^{\infty} M[\mathfrak{J}^l].$$

Proposition 2.2.2. *If the module M is also a torsion module, then it is a direct sum of all the $M[\mathfrak{J}^\infty]$, \mathfrak{J} maximal ideals of A i.e. , if \mathfrak{M} is the set of all maximal ideals of A , then,*

$$M = \bigoplus_{\mathfrak{J} \in \mathfrak{M}} M[\mathfrak{J}^\infty]. \quad (2.2.3)$$

Proof. For an element $m \in M$, we can find an element $x \in A$, such that $xm = 0$. Taking the torsion submodule given by the principal ideal (x) , we have from the identity in (2.2.2),

$$M[(x)] = M_\phi[\mathfrak{J}_1^{k_1}] \oplus M_\phi[\mathfrak{J}_2^{k_2}] \oplus \dots \oplus M_\phi[\mathfrak{J}_n^{k_n}],$$

where $\mathfrak{J}^{k_1} \mathfrak{J}^{k_2} \dots \mathfrak{J}^{k_n}$ is the prime decomposition of (x) . As m belongs to $M[(x)]$ and a prime ideal is maximal in a Dedekind domain, then we see that $m \in \sum_{\mathfrak{J} \in \mathfrak{M}} M[\mathfrak{J}^\infty]$. Thus we have we sum

$$M = \sum_{\mathfrak{J} \in \mathfrak{M}} M[\mathfrak{J}^\infty].$$

Now if $0 = \sum_{l=1}^r m_l$, with m_l belonging to some primary component $M[\mathfrak{J}_l^\infty]$, then we must have $m_l \in M[\mathfrak{J}_l^r]$. Thus, by (2.2.2), we must have $m_l = 0$ for all $1 \leq l \leq r$. Therefore the sum is direct. \square

Now let us have an exact sequence of torsion A -modules

$$(0) \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow (0)$$

If \mathfrak{J} is a maximal ideal of A , then this sequence induces an exact sequence on the \mathfrak{J} -primary components i.e. the following sequence is exact

$$(0) \longrightarrow M_1[\mathfrak{J}^\infty] \longrightarrow M_2[\mathfrak{J}^\infty] \longrightarrow M_3[\mathfrak{J}^\infty] \longrightarrow (0) \quad (2.2.4)$$

If we have a maximal ideal \mathfrak{J} of A , then let us take an uniformizer π of \mathfrak{J} . As $(\pi^l) = \mathfrak{J}^l \mathfrak{P}$, for some prime \mathfrak{P} relatively prime to \mathfrak{J} , we have by (2.2.1),

$$M[\pi^l] = M[\mathfrak{J}^l] \oplus M[\mathfrak{P}].$$

Then, we have

$$M[\pi^l][\mathfrak{J}^\infty] = M[\mathfrak{J}^l][\mathfrak{J}^\infty] \oplus M[\mathfrak{P}][\mathfrak{J}^\infty].$$

But $(M[\mathfrak{P}][\mathfrak{J}^\infty]) = (0)$, thus we have the following proposition:

Proposition 2.2.3. *For a maximal ideal \mathfrak{J} of A , and a uniformizer π of \mathfrak{J} ,*

$$M[\mathfrak{J}^l] = M[\pi^l][\mathfrak{J}^\infty].$$

Next, let us define the sequence,

$$(0) \longrightarrow M[\pi] \longrightarrow M[\pi^l] \xrightarrow{f} M[\pi^{l-1}] \longrightarrow (0),$$

where f is given by the multiplication by a uniformizer π of a maximal ideal \mathfrak{J} .

If M is divisible, then this sequence is exact. Thus, by (2.2.4) and the proposition 2.2.3, we have the following theorem, which is the result we need later when we work with Drinfeld modules:

Theorem 2.2.4. *For a divisible A -module M and a maximal ideal \mathfrak{J} of A , we have an exact sequence*

$$(0) \longrightarrow M[\mathfrak{J}] \longrightarrow M[\mathfrak{J}^l] \xrightarrow{f} M[\mathfrak{J}^{l-1}] \longrightarrow (0).$$

2.3 The notion of Drinfeld modules

Definition 2.3.1. Let L be a field. A field over A or simply an A -field is an \mathbb{F} -algebra morphism $\delta : A \rightarrow L$. We also say that L is an A -field.

The A -field δ induces a natural A -module structure on L . In practice this morphism is set to be the inclusion map or a reduction modulo a prime ideal of A .

Definition 2.3.2. Considering L as an A -module via δ , the A -characteristic of L is the kernel, $\ker \delta$, of the map δ . $\ker \delta$ is a prime ideal of the ring A .

Definition 2.3.3 (Drinfeld A -modules). Let δ be an A -field and suppose $D : L \langle \tau \rangle \rightarrow L$, $\sum l_n \tau^n \mapsto l_0$ is the derivative at zero.

A Drinfeld A -module ϕ over the field L is a \mathbb{F} -algebra homomorphism from A to the ring of twisted polynomials $L \langle \tau \rangle$ such that $D \circ \phi = \delta$, and $\phi(A) \not\subseteq L$.

For simplification we will denote the image of $a \in A$ by ϕ_a instead of $\phi(a)$ and we define the degree $\deg \phi_a$ as the degree of ϕ_a thought as a polynomial in τ .

Definition 2.3.4. Let ϕ be a Drinfeld module and suppose δ is the corresponding A -field, the characteristic $\text{char } \phi$ of the Drinfeld modules ϕ is the A -characteristic of L via δ .

2.3.1 The module structure

It is not clear why we are calling the map ϕ as a module. This comes from the fact that we can construct a new A -module structure on any L -algebra M , by defining the external product as

$$a.u = \phi_a(u), \quad \text{for all } a \in A, u \in M.$$

Usually, we denote the A -module as M_ϕ , if the module structure comes from ϕ .

Like many structure in algebra, we can then define a *torsion submodule* as

$$M_\phi[a] = \{u \in M_\phi : \phi_a(u) = 0\}.$$

Generally, we can define, for an ideal \mathfrak{J} of A ,

$$M_\phi[\mathfrak{J}] = \{u \in M_\phi : \phi_a(u) = 0, \forall a \in \mathfrak{J}\}.$$

2.3.2 The category of Drinfeld modules

In this section, we look a bit in the category formed by Drinfeld A -modules over L , where the morphisms are isogenies. Let us denote this category, for a fixed δ , by $\text{Drin}_L(A)$.

Proposition 2.3.5. *Suppose ϕ is a Drinfeld A -module. Then, for some positive rational number r_ϕ , $\deg \phi_a = -r_\phi v_\infty(a) d_\infty$, for all a in A . In other words, $\deg \phi_a = r_\phi \deg a$.*

Proof. If $v(a) = -\deg \phi_a$, v defines a valuation on A . Indeed,

- we can assume $v(0) = \infty$;
- $v(ab) = v(a) + v(b)$;
- and finally $v(a+b) \geq \min\{v(a), v(b)\}$.

Now, this valuation can be extended to a valuation on k which corresponds to the place ∞ , since only the valuations from this place are negative on A . The equivalence between these valuations yields, for some positive rational r_ϕ and all $a \in A$,

$$v(a) = r_\phi d_\infty v_\infty(a).$$

□

Definition 2.3.6. The number defined in the proposition 2.3.5 is called the rank of a Drinfeld module.

Now let us continue to the notion of height of a Drinfeld A -module. We assume that ϕ is a Drinfeld A -module with nonzero characteristic Q .

Definition 2.3.7. We define the map ω , such that $\omega(a)$ is the index of the smallest power of τ with nonzero coefficient in ϕ_a (we define $\omega(0) = \infty$).

We have the following theorem:

Proposition 2.3.8. *There is a positive rational number h_ϕ , such that*

$$\omega(a) = h_\phi v_Q(a) \deg Q, \forall a \in A.$$

Proof. The map ω defines a valuation on A , thus it extends to a valuation on k . The valuation rings given by this valuation corresponds to Q . Thus the two valuations ω and v_Q are equivalent. The result follows immediately. □

Definition 2.3.9. For a Drinfeld A -module ϕ of characteristic Q , if $Q \neq (0)$, we define the height as the unique positive rational number h_ϕ in the theorem 2.3.8. If $Q = (0)$, then we set $h_\phi = 0$.

One may ask which morphism can we define for us to have a category.

Definition 2.3.10. If ϕ, ψ are two Drinfeld A -modules, then we define a morphism from ϕ to ψ as an element $f \in L\langle\tau\rangle$ such that $f\phi_a = \psi_a f$ for all elements $a \in A$. The set of morphisms from ϕ to ψ is denoted by $\text{hom}_L(\phi, \psi)$.

In fact, when we take an algebraically closed field extension M of L , then as A -modules, f is an homomorphism from M_ϕ to M_ψ . Hence, like in the theory of Elliptic curves, we have the following notion.

Definition 2.3.11. A non-zero morphism between two Drinfeld A -modules ϕ and ψ is called an isogeny. Thus, two Drinfeld A -modules are called isogenous if $\text{hom}_L(\phi, \psi)$ has a non-zero element.

The first property we have from two isogenous Drinfeld modules is about their rank and height:

Proposition 2.3.12. *Two isogenous Drinfeld modules ϕ, ψ have the same rank and height.*

Proof. If ϕ and ψ are isogenous, then for some non-zero $f \in L\langle\tau\rangle$, for all $a \in A$, $f\phi_a = \psi_a f$. Then $\deg f\phi_a = \deg \psi_a f$ so that $\deg \phi_a = \deg \psi_a$. Hence, by the definition of the rank we have, $r_\phi v_\infty(a) d_\infty = r_\psi v_\infty(a) d_\infty$. Simplifying, we get the result. For the height, $f\phi_a = \psi_a f$ also gives us $h_\phi v_Q(a) \deg Q = h_\psi v_{Q'}(a) \deg Q'$. Where Q and Q' are respectively the characteristic of ϕ and ψ . If we knew that $Q = Q'$, then we are done. So let us show that these characteristics are the same. If the constant term of f is 0, then we can remove some factor power of p , so that $f_1\phi'_a = \psi'_a f_2$, where both f_1, f_2 have constant coefficients different from 0. What we should notice is that the constant term of ϕ_a (resp. ψ_a) equals to zero is equivalent to the constant term of ϕ'_a (resp. ψ'_a) equals to zero. And the equality $Q = Q'$ follows immediately. \square

If $\phi \in \text{Drin}_L(A)$, then for an ideal \mathfrak{J} of A , the left ideal of $L\langle\tau\rangle$ generated by the image of \mathfrak{J} by ϕ is principal. We take this result from the fact that the left ideals of $L\langle\tau\rangle$ are principal (see Goss, 1997, chap. 1). Keeping these notations, we have the following definition:

Definition 2.3.13. The skew polynomial $\phi_{\mathfrak{J}}$ is defined to be the unique monic generating the left principal ideal generated by the image of an ideal \mathfrak{J} of A by the Drinfeld A -module ϕ .

Remark 2.3.14. If \mathfrak{J} is an ideal of A , then $\phi_{\mathfrak{J}}$ is a finite linear combination of ϕ_{a_i} , where $a_i \in \mathfrak{J}$. The same for ϕ_a , $a \in \mathfrak{J}$, it is a multiple of $\phi_{\mathfrak{J}}$. Thus $\phi_{\mathfrak{J}}$ vanishes if and only if ϕ_a vanishes for any a in \mathfrak{J} . Therefore, for an L -algebra M , we also have

$$M_\phi[\mathfrak{J}] = \{u \in M_\phi : \phi_{\mathfrak{J}}(u) = 0\}.$$

We have the following proposition:

Proposition 2.3.15. *If $\phi \in \text{Drin}_L(A)$, then for a nonzero ideal \mathfrak{J} of A , $\phi_{\mathfrak{J}}$ is an isogeny from $\phi \in \text{Drin}_L(A)$ to a unique $\psi \in \text{Drin}_L(A)$.*

Proof. $\langle \phi_{\mathfrak{J}} \rangle \phi_a \subset \langle \phi_{\mathfrak{J}} \rangle$ for any element a of A . Thus for $a \in A$, there exists a unique skew polynomial ψ_a such that $\phi_{\mathfrak{J}} \psi_a = \psi_a \phi_{\mathfrak{J}}$. This gives a \mathbb{F} -algebra $\psi : A \longrightarrow L \langle \tau \rangle$ and this is a Drinfeld A -module. What we didn't prove is that the F -algebra homomorphism $D \circ \psi : A \longrightarrow L$ is equal to δ i.e. ϕ and ψ has the same field over A . We will see this in the corollary 2.3.20. \square

We denote the Drinfeld A -module ψ in the proposition 2.3.15 by $\mathfrak{J} * \phi$. In fact, although we haven't yet proved that $\mathfrak{J} * \phi$ is actually in $\text{Drin}_L(A)$, we still can have this definition.

Here are some properties of this notion:

Proposition 2.3.16. *If $\phi \in \text{Drin}_L(A)$, and $\mathfrak{J}_1, \mathfrak{J}_2$ are ideals of A , then,*

- (a) $\phi_{\mathfrak{J}_1 \mathfrak{J}_2} = (\mathfrak{J}_1 * \phi)_{\mathfrak{J}_2} \phi_{\mathfrak{J}_1}$;
- (b) $\mathfrak{J}_1 * (\mathfrak{J}_2 * \phi) = \mathfrak{J}_1 \mathfrak{J}_2 * \phi$;
- (c) $\phi_{(a)} = l^{-1} \phi_a$, for $a \in A$, where l is the leading coefficient of ϕ_b .

Proof.

- (a) As $(\mathfrak{J}_1 * \phi)_{\mathfrak{J}_2} \phi_{\mathfrak{J}_1}$ is a monic, then to prove first assertion, we need to show that $(\mathfrak{J}_1 * \phi)_{\mathfrak{J}_2} \phi_{\mathfrak{J}_1}$ also generates the left ideal generated by $\{\phi_{\mathfrak{J}_1 \mathfrak{J}_2}\}$. Indeed,

$$\begin{aligned}
 (\mathfrak{J}_1 * \phi)_{\mathfrak{J}_2} \phi_{\mathfrak{J}_1} &= \sum_x (\mathfrak{J}_1 * \phi)_x \phi_{\mathfrak{J}_1}, \quad \text{for some finite } x \in \mathfrak{J}_2 \\
 &= \sum_x \phi_{\mathfrak{J}_1} \phi_x, \quad \text{by definition of “*”} \\
 &= \sum_x \sum_y \phi_y \phi_x, \quad \text{for some finite } y \in \mathfrak{J}_1 \\
 &= \sum_{x,y} \phi_{yx}.
 \end{aligned}$$

Thus $(\mathfrak{J}_1 * \phi)_{\mathfrak{J}_2} \phi_{\mathfrak{J}_1}$ belongs to the ideal generated by $\phi_{\mathfrak{J}_1 \mathfrak{J}_2}$. Conversely, let us prove that $\phi_{\mathfrak{J}_1 \mathfrak{J}_2}$ belongs to the ideal generated by $(\mathfrak{J}_1 * \phi)_{\mathfrak{J}_2} \phi_{\mathfrak{J}_1}$. We

have,

$$\begin{aligned}
 \phi_{\mathfrak{I}_1\mathfrak{I}_2} &= \sum_a \phi_a, \quad \text{for some finite } a \in \mathfrak{I}_1\mathfrak{I}_2 \\
 &= \phi_{\sum a}, \quad \text{but } \sum a \in \mathfrak{I}_1\mathfrak{I}_2, \text{ thus} \\
 &= \phi_{\sum yx}, \quad \text{for some finite } y \in \mathfrak{I}_1 \text{ and } x \in \mathfrak{I}_2 \\
 &= \sum_{y,x} \phi_y \phi_x \\
 &= \sum_{y,x} f_y \phi_{\mathfrak{I}_1} \phi_x, \quad \text{for some twisted polynomial } f_y \\
 &= \sum_{y,x} f_y (\mathfrak{I}_1 * \phi)_x \phi_{\mathfrak{I}_1}.
 \end{aligned}$$

As $(\mathfrak{I}_1 * \phi)_x$, for $x \in \mathfrak{I}_2$, belongs to the ideal generated by $(\mathfrak{I}_1 * \phi)_{\mathfrak{I}_2}$, the result follows.

(b) For the second point, by the first property, we have

$$\begin{aligned}
 \phi_{\mathfrak{I}_1\mathfrak{I}_2} \phi_a &= (\mathfrak{I}_1 * \phi)_{\mathfrak{I}_2} \phi_{\mathfrak{I}_1} \phi_a \\
 &= (\mathfrak{I}_1 * \phi)_{\mathfrak{I}_2} (\mathfrak{I}_1 * \phi)_a \phi_{\mathfrak{I}_1} \\
 &= (\mathfrak{I}_2 * (\mathfrak{I}_1 * \phi))_a (\mathfrak{I}_1 * \phi)_{\mathfrak{I}_2} \phi_{\mathfrak{I}_1} \\
 &= (\mathfrak{I}_2 * (\mathfrak{I}_1 * \phi))_a \phi_{\mathfrak{I}_1\mathfrak{I}_2}.
 \end{aligned}$$

But $\mathfrak{I}_1\mathfrak{I}_2 * \phi$ is the unique twisted polynomial satisfying this relation, then we have our result.

(c) The result is trivial.

□

We may notice that the first part of the proposition 2.3.16 is, somehow, a generalisation of the notion of $*$ from $\phi_a, a \in A$ to $\phi_{\mathfrak{I}}, \mathfrak{I}$ ideal of A . Like this, let us give a generalisation of the map ω in the definition 2.3.7.

Definition 2.3.17. We define a map $\omega : L \langle \tau \rangle \rightarrow \mathbb{Z}$ such that, for $f \in L \langle \tau \rangle$, $\omega(f)$ is the index of the smallest power of τ with nonzero coefficient in f . As, for an ideal \mathfrak{I} of A , $\phi_{\mathfrak{I}}$ is unique, then we can define $\omega(\mathfrak{I}) = \omega(\phi_{\mathfrak{I}})$.

Remark 2.3.18. Now, we have three different definitions of the map ω . The context allows us to determine which of these definitions we are talking about. Furthermore, if we are working with a fixed Drinfeld modules ϕ , then $\omega(a) = \omega(\phi_a)$. And this ω has an additive property, more precisely $\omega(\phi\psi) = \omega(\phi) + \omega(\psi)$.

This generalisation make us also ask if the property of rank and height from propositions 2.3.5 and 2.3.8 can be generalised from the element $a \in A$ to the ideal I in A . The answer of this question is yes as we can see from the following proposition:

Proposition 2.3.19. *Let \mathfrak{J} be a non-zero ideal of A , and let $\phi \in \text{Drin}_L(A)$ with rank r_ϕ and height h_ϕ . Then $\deg \phi_{\mathfrak{J}} = r_\phi \deg \mathfrak{J}$. Moreover, if the characteristic $Q = \text{char } \phi \neq (0)$, then $\omega(\phi_{\mathfrak{J}}) = h_\phi \deg Qv_Q(\mathfrak{J})$.*

Proof. Let us first prove the statements for \mathfrak{J} prime to Q . Given an element $a \in \mathfrak{J}$, we can factorize the principal ideal $(a) = \mathfrak{J}I$ for some ideal I of A . The proposition 2.3.16 gives us

$$\phi_{(a)} = (\mathfrak{J} * \phi)_I \phi_{\mathfrak{J}}.$$

As \mathfrak{J}, Q are relatively prime, then $a \notin Q$ and by definition of the height $\omega(a) = 0$. Now we can think of ω in different way:

$$\omega(\phi_{(a)}) = \omega(\phi_a) = \omega(a) = 0.$$

By the additive property, as $\phi_{(a)} = (\mathfrak{J} * \phi)_I \phi_{\mathfrak{J}}$, then

$$\omega((\mathfrak{J} * \phi)_I) + \omega(\phi_{\mathfrak{J}}) = 0.$$

Thus $\omega(\phi_{\mathfrak{J}}) = 0$. As 0 is the only multiple root of a skew polynomial, then, $\phi_{\mathfrak{J}}$ has distinct roots and thus, by the remark 2.3.14, we have $\sharp M_\phi[\mathfrak{J}] = q^{\deg \phi_{\mathfrak{J}}}$. We will see in the proof of the theorem 2.3.22 that $\sharp M_\phi[\mathfrak{J}] = q^{r_\phi \deg \mathfrak{J}}$, so that $r_\phi \deg \mathfrak{J} = \deg \phi_{\mathfrak{J}}$.

The case of the height is trivial since $\omega(\phi_{\mathfrak{J}}) = 0$ as well as $v_Q(\mathfrak{J}) = 0$.

Now assume that \mathfrak{J} is a non-zero ideal divisible by $Q \neq (0)$. Given two non-zero ideals I, J of A , the theory of Dedekind domain tells us that there is an ideal I' relatively prime to J , such that $II' = (a)$, for some $a \in A$ (see Ash, 2003). Suppose $\mathfrak{J} = \mathfrak{J}_1 Q^n$, with \mathfrak{J}_1 prime to Q . Then, applying the previous statement, for some Q' and $a \in A$, we have $Q^n Q' = (a)$. Hence $\mathfrak{J} Q' = (a) \mathfrak{J}_1$. Now, applying the previous statement again, for \mathfrak{J}_2 prime to Q and $b \in A$, $Q' \mathfrak{J}_2 = (b)$. Therefore, $(b) \mathfrak{J} = (a) \mathfrak{J}_1 \mathfrak{J}_2$. Setting $\mathfrak{J}_1 \mathfrak{J}_2 = \mathfrak{J}'$, we have \mathfrak{J}' prime to Q . Thus there are some $a, b \in A$ and a non-zero ideal \mathfrak{J}' prime to Q , such that $(b) \mathfrak{J} = (a) \mathfrak{J}'$. So we have,

$$\deg b + \deg \mathfrak{J} = \deg a + \deg \mathfrak{J}'.$$

Moreover, by the proposition 2.3.16,

$$(\mathfrak{J} * \phi)_{(b)} \phi_{\mathfrak{J}} = (\mathfrak{J}' * \phi)_{(a)} \phi_{\mathfrak{J}'}$$

As the degree of a product is the sum of the degree, then,

$$\deg(\mathfrak{J} * \phi)_{(b)} + \deg \phi_{\mathfrak{J}} = \deg(\mathfrak{J}' * \phi)_{(a)} + \deg \phi_{\mathfrak{J}'}$$

By the last part of proposition 2.3.16, we have

$$\deg(\mathfrak{J} * \phi)_b + \deg \phi_{\mathfrak{J}} = \deg(\mathfrak{J}' * \phi)_a + \deg \phi_{\mathfrak{J}'}$$

Using the proposition 2.3.12, and the first part of this proof, we get $r_{\phi} \deg b + \deg \phi_{\mathfrak{J}} = r_{\phi} \deg a + r_{\phi} \deg \mathfrak{J}'$. Thus we can conclude that, $\deg \phi_{\mathfrak{J}} = r_{\phi} \deg \mathfrak{J}$. The case of the height is similar, we get

$$h_{\phi} \deg Qv_Q(b) + \omega(\phi_{\mathfrak{J}}) = h \deg Qv_Q(a).$$

But $(b)\mathfrak{J} = (a)\mathfrak{J}'$ gives us

$$v_Q(b) + v_Q(\mathfrak{J}) = v_Q(a).$$

Hence $\omega(\phi_{\mathfrak{J}}) = h \deg Qv_Q(\mathfrak{J})$. □

Corollary 2.3.20. *If $\phi \in \text{Drin}_L(A)$, with field over A , δ , then the field other A , δ' , of the Drinfeld module $\mathfrak{J} * \phi$, where I is an ideal of A , is also equal to δ .*

Proof. As we have $\phi_{\mathfrak{J}}\phi_a = (\mathfrak{J} * \phi)_a\phi_{\mathfrak{J}}$, for $a \in A$, then comparing the coefficients of both sides of the equality, we get $\delta'(a) = \delta(a)^{q^{\omega(\phi_{\mathfrak{J}})}}$. If $Q = \text{char } \phi = (0)$, then $\omega(\phi_{\mathfrak{J}}) = 0$ and we are done. Otherwise, by the previous proposition $\delta'(a) = \delta(a)^{q^{h_{\phi} \deg Qv_Q(\mathfrak{J})}}$. But there, the image $\delta(A)$ is a subfield of L isomorphic to $A/\text{char } \phi$. The last one has cardinal $q^{\deg Q}$ and the result follows. □

The next lemma is useful for the next theorem:

Lemma 2.3.21. *For $\phi \in \text{Drin}_L(A)$ and $a \in A$, the number of distinct roots of $\phi_a(t)$, considered as a polynomial in t is equal to $q^{\deg \phi_a - \omega(a)}$.*

Proof. If $\phi_a(t)$ is separable, then the number of distinct roots is equal to the degree of $\phi_a(t)$, which is equal to $q^{\deg \phi_a}$. Now if $\omega(a) > 0$, then the smallest power of t in $\phi_a(t)$ is $t^{q^{\omega(a)}}$. Thus, 0 is a multiple root contradicting the fact that $\phi_a(t)$ is separable. This gives us the result.

Now if $\phi_a(t)$ is not separable, then, we can factor ϕ_a as

$$\phi_a = (c_{\omega}(a) + \dots + c_{\deg \phi_a} \tau^{\deg \phi_a - \omega(a)}) \tau^{\omega(a)},$$

where $c_{\omega}(a) + \dots + c_{\deg \phi_a} \tau^{\deg \phi_a - \omega(a)}$ is separable and has the same roots as ϕ_a . Thus the number of roots of ϕ_a is

$$q^{\deg(c_{\omega}(a) + \dots + c_{\deg \phi_a} \tau^{\deg \phi_a - \omega(a)})} = q^{\deg \phi_a - \omega(a)}.$$

□

Back to the rank and the height, we have the following theorem:

Theorem 2.3.22. *The rank and the height of a Drinfeld module are positive integers (Of course if the characteristic of the Drinfeld module is (0), the height is 0).*

Proof. Suppose we have a field M which contains L . Suppose furthermore that M is algebraically closed. For a Drinfeld A -module ϕ , defined over L with respect to $\delta : A \rightarrow L$, M_ϕ is an A -module.

Let P be a nonzero prime ideal of A . If a is an element of P , then $M_\phi[P] \subset M_\phi[a]$. The last one is finite by definition. Thus $M_\phi[P]$ is a finite A -module. As this is annihilated by P , then $M_\phi[P]$ is a vector space over A/P . And we know that $A/P \simeq A_P/PA_P$, so $\#A/P = q^{\deg P}$, thus, for some integer d ,

$$\#M_\phi[P] = q^{d \deg P}.$$

But the class group of A is finite (proposition 2.1.6). Thus, $P^m = (\alpha)$ for some integer m and $\alpha \in A$.

Now, by the theorem 2.2.4, the following sequence, for any positive integer m and where f is the multiplication by an uniformizer π at P , is exact:

$$(0) \longrightarrow M_\phi[P] \longrightarrow M_\phi[P^m] \xrightarrow{f} M_\phi[P^{m-1}] \longrightarrow (0) \quad (2.3.1)$$

This implies that $\#M_\phi[P^m] = \#M_\phi[P^{m-1}] \#M_\phi[P] = q^{m d \deg P}$. By induction on m , we get $\#M_\phi[P^m] = \#M_\phi[P]^m$. Thus

$$\#M_\phi[P^m] = q^{m d \deg P}. \quad (2.3.2)$$

On the other hand $\#M_\phi[P^m] = \#M_\phi[(\alpha)] = \#M_\phi[\alpha]$. Let us compute this last cardinal. By definition of the torsion submodule, and since M is algebraically closed, this is equal to the number of distinct roots of $\phi_\alpha(t)$, considered as a polynomial in the variable t . From the lemma 2.3.21, we have

$$\#M_\phi[P^m] = q^{\deg \phi_\alpha - \omega(\alpha)}. \quad (2.3.3)$$

The equations 2.3.2 and 2.3.3 yield

$$m d \deg P = \deg \phi_\alpha - \omega(\alpha).$$

If $\alpha \in Q$, then $P^m \subset Q$. Thus for $x \in P$, $x^m \in P^m$ so that $\delta(x)^m = \delta(x^m) = 0$. But since L is integral then $\delta(x) = 0$ which implies that $P \subset Q$. As A is a Dedekind domain, then both prime ideals P, Q are maximal i.e. $P = Q$.

Therefore, if $P \neq Q$, then $\delta(\alpha)$, which is the derivative of ϕ_α is different from 0. Thus $m d \deg P = \deg \phi_\alpha$, and by definition of the rank

$$m d \deg P = -r_\phi v_\infty(\alpha) d_\infty = r_\phi \deg \alpha.$$

Now from the theorem 2.1.5, we have

$$\begin{aligned} m d \deg (PA_P) &= r_\phi \dim_{\mathbb{F}} A/(a) \\ &= r_\phi \dim_{\mathbb{F}} A/(P^m). \end{aligned}$$

As we have seen, from the proof of theorem 2.1.5,

$$\dim_{\mathbb{F}} A/(P^m) = m \dim_{\mathbb{F}} A/(P),$$

thus

$$m d \deg P = r_{\phi} m \deg P.$$

Therefore, r_{ϕ} is a positive integer.

If $P = Q$, then

$$m d \deg P = r_{\phi} m \deg P - \omega(\alpha).$$

And by definition,

$$\omega(\alpha) = h_{\phi} v_P(\alpha) \deg P.$$

Moreover, $v_P(\alpha) = m$ so that

$$m d \deg P = r_{\phi} m \deg P - h_{\phi} m \deg P.$$

Therefore $d = r_{\phi} - h_{\phi}$, so that h_{ϕ} is an integer. □

2.4 Analytic construction of Drinfeld modules

2.4.1 Complex theory

Most of the results in this topic are presented without any proof. For more details, we can consult Goss (1997).

Recall that we have a function field k/\mathbb{F} and a fixed place at infinity ∞ . The valuation v_{∞} gives rise to an absolute value $|\cdot|_{\infty}$, which induces a topology on k . The field k_{∞} is the completion of k from that topology. Unfortunately, the field k_{∞} is not algebraically closed so that we take the algebraic closure \bar{k}_{∞} . Now, the absolute value on k_{∞} extends uniquely to an absolute value on \bar{k}_{∞} , by the mean of the following formula:

$$|\cdot| = \left| N_{K/k_{\infty}}(\cdot) \right|_{\infty}^{\frac{1}{[K:k_{\infty}]}} ,$$

where $|\cdot|_{\infty}$ is the absolute value on k_{∞} .

Again, this field is not good enough for us to work within it. More precisely, this field is not complete so that we need again to go to its completion which we denote by \mathbf{C}_{∞} . Finally, this field is algebraically closed as well as it is complete. In our case, this will take the place of the complex numbers \mathbb{C} and then we will take some notions from the complex theory. Some properties are much stronger than in the ordinary case as we can see from the following proposition:

Proposition 2.4.1. *Let $\sum a_n$ be a series in \mathbf{C}_{∞} . Then, $\sum a_n$ converges if and only if a_n converges to 0.*

The equivalence is due to the fact that the absolute value, obtained by the place at infinity, gives rise to a non-archimedean distance on \mathbf{C}_∞ .

Definition 2.4.2. A function $f : \mathbf{C}_\infty \rightarrow \mathbf{C}_\infty$ is called entire if there is a convergent series $\sum a_n z^n$ such that $f(z) = \sum a_n z^n$ for all z in \mathbf{C}_∞ .

Another difference between the ordinary complex number \mathbb{C} and our \mathbf{C}_∞ is about the property of entire function:

Proposition 2.4.3. *Only constant functions can be entire without zeros. Suppose two entire functions are expressed as a power series $\sum a_n z^n, \sum b_n z^n$, with $a_n, b_n \in \mathbf{C}_\infty$. If $a_1 = b_1$ and the two functions have the same set of roots (with multiplicity), then these functions are the same.*

As in the classical theory, we can factorize, the zero's in the following way: If $f(z_0) = 0$, for some z_0 , then f can be written uniquely as

$$f(z) = (z - z_0)^m g(z),$$

such that $g(z)$ is an entire function which doesn't vanish on z_0 . With the same notation, we define $\text{ord}_{z=z_0} f(z) = m$.

Finally, let us state the most important theorem in this section. This is similar to the Weierstrass Factorization theorem but now in the case of \mathbf{C}_∞ .

Theorem 2.4.4. *Let f be an entire function and suppose $\{z_1, z_2, \dots\}$ is the set of its non-zero roots (the same roots can appear many times in the set). Then:*

(a) $\lim_{i \rightarrow \infty} z_i = \infty$,

(b) for some constant c , if we set $n = \text{ord}_{z=0} f(z)$,

$$f(z) = cz^n \prod_{i=1}^{\infty} \left(1 - \frac{z}{z_i}\right).$$

Conversely, if $\lim_{i \rightarrow \infty} z_i = \infty$, then $cz^n \prod_{i=1}^{\infty} \left(1 - \frac{z}{z_i}\right)$ is an entire function on \mathbf{C}_∞ .

2.4.2 Lattices associated to Drinfeld modules

Definition 2.4.5. A lattice Λ is a finitely generated A -submodule of \mathbf{C}_∞ such that Λ is discrete with respect to the topology of \mathbf{C}_∞ . The rank of the lattice Λ is the dimension of the vector space Λk_∞ over the field k_∞ .

The property of the lattice Λ being discrete is very important. From this, we see that $|\lambda|$ tends to ∞ with λ going through the elements of the lattice Λ . Thus, applying the theorem 2.4.4, we get the following proposition.

Proposition 2.4.6. *Given a lattice Λ . The following function, which is called the exponential function associated to the lattice Λ , is entire on \mathbf{C}_∞ :*

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

This function has a linearity property:

Proposition 2.4.7. *Let Λ be a lattice and suppose e_Λ is its associated exponential function. Then, e_Λ is \mathbb{F} -linear i.e. for $z, t \in \mathbf{C}_\infty$ and $\alpha \in \mathbb{F}$,*

$$e_\Lambda(z + \alpha t) = e_\Lambda(z) + \alpha e_\Lambda(t).$$

Proof.

- First let us show that given a finite vector space V over the finite field \mathbb{F} , the polynomial $P_V(z) = \prod_{v \in V} (z - v)$ is \mathbb{F} -linear.

If $\dim V = 0$, then the statement is obviously true as $P_V(z) = z$. Assume the statement is true for a $n - 1$ dimensional vector subspace U of W . Let us show that the statement also holds for V . Assume, $V = U + \mathbb{F}a$, $a \in V$, and let us split P_V into two products depending on the coefficient of a . If $v = u + fa$, then

$$\begin{aligned} P_V(z) &= \prod_{v \in V} (z - v) \\ &= \prod_{\substack{v \in V \\ f=0}} (z - v) \prod_{\substack{v \in V \\ f \neq 0}} (z - v) \\ &= \prod_{u \in U} (z - u) \prod_{f \in \mathbb{F} - \{0\}} \left(\prod_{u \in U} (z - (u + fa)) \right) \\ &= P_U(z) \prod_{f \in \mathbb{F} - \{0\}} P_U(z - fa). \end{aligned}$$

By assumption, P_U is \mathbb{F} -linear, then

$$\begin{aligned} P_V(z) &= P_U(z) \prod_{f \in \mathbb{F} - \{0\}} (P_U(z) - fP_U(a)) \\ &= \prod_{f \in \mathbb{F}} (P_U(z) - fP_U(a)). \end{aligned}$$

\mathbb{F} is a finite field of cardinal q , computing the last term will give us,

$$P_V(z) = P_U(z)^q - P_U(a)^{q-1} P_U(z).$$

But P_U is \mathbb{F} -linear, then P_V is also \mathbb{F} -linear.

- Now, using the previous item, we get $P_V(z) = \prod_{v \in V} (-v) \prod_{v \in V} (1 - \frac{z}{v})$, is \mathbb{F} -linear. The first product is a constant. Dividing by this constant, we still have a \mathbb{F} -linear polynomial $\prod_{v \in V} (1 - \frac{z}{v})$. Now, given an integer N , the subset $\{l \in \Lambda, |l| \leq N\}$ of L is a finite vector space over \mathbb{F} . So applying the previous result,

$$\prod_{\substack{l \in \Lambda \\ |l| \leq N}} \left(1 - \frac{z}{v}\right)$$

is \mathbb{F} -linear. Letting $N \rightarrow \infty$, we finally get e_Λ is \mathbb{F} -linear.

□

Let $\Lambda \subset \Lambda'$ be two lattices of the same rank r . The polynomial $e_\Lambda(z)$, defined on Λ' vanishes on Λ . Thus, it induces an isomorphism from Λ'/Λ to $e_\Lambda(\Lambda')$, which are both \mathbb{F} -vector spaces. Moreover, Λ'/Λ is finite and then applying the same method as in the proof of the proposition 2.4.7, we have the following proposition:

Proposition 2.4.8. *Let $\Lambda \subset \Lambda'$ be two lattices of the same rank. Then the polynomial*

$$P(\Lambda'/\Lambda; z) = z \prod_{\lambda \in e_\Lambda(\Lambda'/\Lambda) - \{0\}} \left(1 - \frac{z}{\lambda}\right),$$

is \mathbb{F} -linear with degree $\#\Lambda'/\Lambda$.

Furthermore, it satisfies the following property.

Theorem 2.4.9. *Let $\Lambda \subset \Lambda'$ be two lattices of the same rank. Then $e_{\Lambda'}(z) = P(\Lambda'/\Lambda; e_\Lambda(z))$.*

Proof. This follows from the fact that both sides satisfy the same condition of uniqueness in the proposition 2.4.3. □

Now, we are ready to construct our Drinfeld A -modules over \mathbf{C}_∞ . Let $a \in A$, then $a^{-1}\Lambda$ is a lattice with the same rank as Λ such that $\Lambda \subset a^{-1}\Lambda$. Define $\phi_a^\Lambda(x) = aP(a^{-1}\Lambda/\Lambda; x)$.

Theorem 2.4.10. *Let Λ be a lattice with rank r . The map, where $\tau = x^q$,*

$$\begin{aligned} \phi^\Lambda : A &\longrightarrow \mathbf{C}_\infty \langle \tau \rangle \\ a &\longmapsto \begin{cases} 0 & \text{if } a = 0, \\ \phi_a^\Lambda & \text{otherwise,} \end{cases} \end{aligned}$$

is a Drinfeld A -modules over \mathbf{C}_∞ with rank equal to the rank of the lattice Λ .

To prove this theorem, we need the following lemma.

Lemma 2.4.11. *The map ϕ^Λ defined in the theorem 2.4.10 satisfies $\phi_{ab}^\Lambda(\tau) = \phi_a^\Lambda(\tau)\phi_b^\Lambda(\tau)$, for $a, b \in A$. Moreover it is \mathbb{F} -linear.*

Proof. Let $f \in \mathbb{F}$. If $f = 0$, then, by definition, we have $\phi_f^\Lambda = 0$. If $f \neq 0$, then $f^{-1}\Lambda = \Lambda$ so that $\phi_f^\Lambda(x) = fx$. So, ϕ^Λ fixes the elements of \mathbb{F} . We notice that $e_{a^{-1}\Lambda}(x)$ and $P(a^{-1}\Lambda/\Lambda; e_\Lambda(x))$ have the same zeros, and the same coefficient for x , thus by proposition 2.4.3, they are the same i.e. $e_{a^{-1}\Lambda}(x) = P(a^{-1}\Lambda/\Lambda; e_\Lambda(x))$. We also have $e_{a^{-1}\Lambda}(x) = a^{-1}e_\Lambda(ax)$. Hence $e_\Lambda(ax) = \phi_a^\Lambda(e_\Lambda(x))$, which we call *complex multiplication*. Thus we have:

$$\begin{aligned} \phi_{ab}^\Lambda(e_\Lambda(x)) &= e_\Lambda(abx) \\ &= \phi_a^\Lambda(e_\Lambda(bx)) \\ &= \phi_a^\Lambda(\phi_b^\Lambda(e_\Lambda(x))). \end{aligned}$$

and

$$\begin{aligned} \phi_{a+b}^\Lambda(e_\Lambda(x)) &= e_\Lambda((a+b)x) \\ &= e_\Lambda(ax) + e_\Lambda(bx) \\ &= \phi_a^\Lambda(e_\Lambda(x)) + \phi_b^\Lambda(e_\Lambda(x)), \end{aligned}$$

The distributivity of ϕ^Λ w.r.t the product and the addition follows from the surjectivity of e_Λ . \square

Proof of Theorem 2.4.10.

- The map $\delta : A \rightarrow \mathbf{C}_\infty$ is just the inclusion.
- The property of derivative D is also satisfied: The first term of the power series $P(a^{-1}/L; x)$ is x , so that, multiplying by a , we get $D \circ \phi_a^\Lambda = a$.
- By the lemma 2.4.11, ϕ is a \mathbb{F} -algebra homomorphism.
- The rank is equal to the rank of Λ : Suppose Λ is an A -module of rank r . Then Λ is a direct sum of r fractional ideals of A . But for a fractional ideal \mathfrak{J} , we have the isomorphism $a^{-1}\mathfrak{J}/\mathfrak{J} \sim a^{-1}A/A \sim A/aA$. Hence, $\sharp a^{-1}\Lambda/\Lambda = (\sharp A/aA)^r = q^{r \deg a}$. But we know that $\deg \phi_a(x) = \sharp a^{-1}\Lambda/\Lambda$, as a polynomial in x . As a twisted polynomial in $\tau = x^a$, we have $\deg \phi_a = \log_q(\sharp a^{-1}\Lambda/\Lambda)$. Therefore, $\deg \phi_a = r \deg a$ and we are done.

\square

Chapter 3

Analogy with elliptic curves

In his original papers (Drinfeld, 1974) V. Drinfeld called the Drinfeld modules as Elliptic modules. This chapter will explain us how do we have this name. Indeed, there is an analogy between the theory of elliptic curves and the Drinfeld modules of rank 2.

3.1 The Weierstrass function

To begin let us recall some notions from the theory of Elliptic curves. Let us assume that K is a field.

Definition 3.1.1. An elliptic curve over K is a non-singular cubic curve C together with an extra point \mathcal{O} , called point at infinity, and we write C/K , such that its equation has coefficients in K .

Remark 3.1.2.

- The notation $C(F)$ for a field F means that, $C(F)$ is the set of points of $F \times F$ solution to the equation of the curve. Adding the point at the infinity, then, $C(F)$ has a group structure (see Silverman, 2009).
- If $\text{char } K \neq 2$, then by some change of variables (see Silverman, 2009), our curve is equivalent to a curve with equation $y^2 = x^3 + ax^2 + bx + c$.
- If, moreover, $\text{char } K \neq 3$, then this equation can be reduced to $y^2 = x^3 + ax + b$ (see Silverman, 2009).
- We can take any point to be the identity of the group. But usually, the point at infinity \mathcal{O} is taken to be the identity.

From these remarks, we will restrict ourselves to elliptic curves with equation in the form $y^2 = x^3 + ax + b$. After that, we are interested in elliptic curves defined over \mathbb{C} .

Suppose Λ is a rank 2 \mathbb{Z} -lattice of \mathbb{C} i.e. there are two elements l_1 and l_2 of \mathbb{C} such that $\Lambda = \mathbb{Z}l_1 + \mathbb{Z}l_2$. Note that there are many possible choices for l_i , but as we have a rank 2 lattice, then l_1, l_2 must satisfy $l_1/l_2 \notin \mathbb{R}$. The fundamental parallelogram is defined to be the subset $P = \{al_1 + bl_2 : 0 \leq a, b < 1\}$. We notice that there is a natural bijection between $P \rightarrow \mathbb{C}/\Lambda$ as any elements of \mathbb{C} can be obtained with a translation of P by multiples of l_1 and l_2 .

Definition 3.1.3. Two lattices Λ and Λ' are homothetic if there is a non-zero element $\lambda \in \mathbb{C}$ such that $\lambda\Lambda = \Lambda'$.

Definition 3.1.4. Given a lattice Λ , we call the Weierstrass \wp -function the series $\wp(z, \Lambda)$, or $\wp(z)$ if Λ is understood, defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{l \in \Lambda - \{0\}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right).$$

Theorem 3.1.5. Let Λ be a lattice. The corresponding \wp -function is meromorphic on \mathbb{C} with the only poles at Λ . And it is double periodic with periods l_1 and l_2 .

We postpone the proof of this theorem for later.

Remark 3.1.6. From theorem 3.1.5, the \wp -function is meromorphic on \mathbb{C} and $\wp(z+l) = \wp(z)$ for all $z \in \mathbb{C}$ and all $l \in \Lambda$. Such a function is called an elliptic function w.r.t the lattice Λ and we denote their set by \mathcal{E}_Λ . One property of \mathcal{E}_Λ is that the derivative f' of an elliptic function f is still an elliptic function. Moreover, \mathcal{E}_Λ is a field.

Theorem 3.1.7. If an elliptic function has no pole in the fundamental parallelogram P , then it is a constant function.

Proof. Without poles, the function must be bounded in P as P is compact. But the whole elements of \mathbb{C} can be obtained by translation of elements of P by multiples of l_1 and l_2 , and we are in the case of elliptic function, thus the value of that function is determined by the value of the function in the fundamental parallelogram P . Hence we have a function bounded on the whole complex plane. As it is meromorphic there, then by a property from Liouville, this should be a constant function. \square

Definition 3.1.8. We define the order of an elliptic function as the number of its poles, multiplicity being counted, in a fundamental parallelogram.

As an example, we see immediately that the Weierstrass \wp -function is of order 2.

Lemma 3.1.9. Given a lattice Λ , the Weierstrass \wp -function converges absolutely and uniformly on every compact subset of $\mathbb{C} - \Lambda$.

Proof. Let $z \in \mathbb{C} - \Lambda$. We have,

$$\frac{1}{(z-l)^2} - \frac{1}{l^2} = \frac{z(2l-z)}{(z-l)^2 l^2}.$$

When l is large enough, then, by means of convergence, the sum

$$\sum_{l \in \Lambda - \{0\}} \frac{z(2l-z)}{(z-l)^2 l^2},$$

is equivalent to $\sum_{l \in \Lambda - \{0\}} \frac{1}{l^3}$. So we are reduced to showing that the last one converges absolutely.

Let us split the sum into annuli $A_n = \{l \in \Lambda : n < |l| \leq n+1\}$, $n = 1, 2, \dots$. There is a constant C depending on Λ such that the cardinal of each annulus A_n is strictly less than C . Thus,

$$\sum_{l \in \Lambda - \{0\}} \frac{1}{|l|^3} < \sum_{n \geq 1} \frac{\#A_n}{n^3} < C \sum_{n \geq 1} \frac{1}{n^2}.$$

The later one converges thus the Weierstrass \wp -function converges absolutely and hence uniformly on every compact subset of $\mathbb{C} - \Lambda$. \square

Proof of the theorem 3.1.5. From the lemma 3.1.9 we see that the Weierstrass \wp -function is holomorphic on $\mathbb{C} - \Lambda$. The points on the lattice Λ , which are the poles, are isolated so that \wp is now meromorphic on \mathbb{C} . Furthermore, this function is obviously even. The derivative of the \wp -function is,

$$\wp'(z) = \frac{d}{dz} \left(\frac{1}{z^2} + \sum_{l \in \Lambda - \{0\}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) \right) = -2 \sum_{l \in \Lambda} \frac{1}{(z-l)^3}. \quad (3.1.1)$$

l_1 and l_2 are clearly periods of \wp' and hence we have $\wp'(z+l_i) = \wp'(z)$. Integrating, we get $\wp(z+l_i) = \wp(z) + C_i$. If we take $z = -\frac{1}{2}l_i$, then $\wp(\frac{1}{2}l_i) = \wp(-\frac{1}{2}l_i) + C_i$. But \wp is an even function, thus $C_i = 0$. \square

Now, the following theorem tells us how this Weierstrass \wp -function is related to elliptic curves.

Theorem 3.1.10. *Let $G_k(\Lambda)$, or simply G_k if the lattice Λ is understood, be the infinite sum given by,*

$$G_k = \sum_{l \in \Lambda - \{0\}} l^{-k}.$$

Then the Laurent series of \wp is

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2(k+1)} z^{2k}.$$

After that, for $z \in \mathbb{C} - \Lambda$, the tuple $(x, y) = (\wp(z), \wp'(z))$ is solution to the equation

$$y^2 = 4x^3 - 60G_4x - 140G_6. \quad (3.1.2)$$

Remark 3.1.11. The series G_k is absolutely convergent for $k > 2$ as we may prove like we did for the case of $k = 3$ in the proof of Lemma 3.1.9. When k is odd we see that G_k is equal to zero as the terms from l and $-l$ cancel each other.

Proof of theorem 3.1.10 . If $|z| < |l|$, then,

$$\begin{aligned} \frac{1}{(z-l)^2} - \frac{1}{l^2} &= \frac{1}{l^2} \left(\frac{1}{\left(1 - \frac{z}{l}\right)^2} - 1 \right) \\ &= \sum_k^{\infty} (k+1) \frac{z^k}{l^{k+2}}. \end{aligned}$$

Thus,

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{l \in \Lambda - \{0\}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) \\ &= \frac{1}{z^2} + \sum_{l \in \Lambda - \{0\}} \sum_{k=1}^{\infty} (k+1) \frac{z^k}{l^{k+2}} \\ &= \frac{1}{z^2} + \sum_{k=1}^{\infty} (k+1) z^k \sum_{l \in \Lambda - \{0\}} l^{-(k+2)} \\ &= \frac{1}{z^2} + \sum_{k=1}^{\infty} (k+1) G_k z^k. \end{aligned}$$

Finally, the remark 3.1.11 tells us, that,

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2(k+1)} z^{2k}.$$

For the next part, let us denote $\omega(z) = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6 - \wp'(z)^2$. If we compute the Laurent expansion of the right-hand side using the Laurent expansion of \wp , we see that this is holomorphic at 0 with $\omega(0) = 0$. It has no pole in P , the fundamental parallelogram, and is an elliptic function (both \wp and \wp' are elliptic functions). Thus by theorem 3.1.7, it is a constant which must be equal to 0. \square

In fact every elliptic function is a rational expression of \wp and \wp' . More precisely, even elliptic functions are rational expressions of \wp . But we will not go

further as we already got what we needed. Namely, Given a lattice Λ , we get a Weierstrass \wp -function which in turn gives rise to, as we will see, an elliptic curves of the form $y^2 = ax^3 + bx + c$. From this we can see that there is an analogy with Drinfeld modules as, there too, a lattice also gives rise to a Drinfeld module.

3.2 On the side of elliptic curves

We have seen that given a lattice Λ , we get an equation of the form $y^2 = ax^3 + bx + c$. The following proposition asserts that this is in fact an equation of some elliptic curves.

Proposition 3.2.1. *Let Λ be a lattice, if we set $g_2 = 60G_4$ and $g_3 = 140G_6$, then the equation $y^2 = 4x^3 + g_2x + g_3$ defines an elliptic curves.*

Proof. What we need to show here is that the curve given by this equation is non-singular. That is obtained by showing that the polynomial $p(z) = 4x^3 + g_2x + g_3$ has three distinct roots in \mathbb{C} namely $\wp\left(\frac{l_1}{2}\right)$, $\wp\left(\frac{l_2}{2}\right)$ and $\wp\left(\frac{l_1+l_2}{2}\right)$. If we look at the derivative \wp' in the equation (3.1.1), we see that it is an odd function so that, for $a \in \left\{\frac{l_1}{2}, \frac{l_2}{2}, \frac{l_1+l_2}{2}\right\}$, $\wp'(a) = -\wp'(-a)$, but l_1, l_2 are periods of \wp' , thus $\wp'(a) = -\wp'(a)$. This implies that $\wp'(a) = 0$ or equivalently $p(\wp(a)) = 0$. Now, for $a \in \left\{\frac{l_1}{2}, \frac{l_2}{2}\right\}$, $\wp(z) - \wp(a)$ vanishes at two points a and $-a$. Moreover, \wp is of order 2, thus there cannot be another zeros of $\wp(z) - \wp(a)$ on the fundamental parallelogram. Thus $\wp(b) - \wp(a) \neq 0$ for $b \in \left\{\frac{l_1}{2}, \frac{l_2}{2}, \frac{l_1+l_2}{2}\right\} - \{a\}$. Hence we have three distinct roots for $p(x)$: $\wp\left(\frac{l_1}{2}\right)$, $\wp\left(\frac{l_2}{2}\right)$ and $\wp\left(\frac{l_1+l_2}{2}\right)$. \square

So now, from a lattice we get an elliptic curve $C(\mathbb{C})$ with equation $y^2 = 4x^3 + g_2x + g_3$. In fact we have an isomorphism,

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\longrightarrow C(\mathbb{C}) \\ z &\longmapsto [\wp(z) : \wp'(z) : 1] \end{aligned} \tag{3.2.1}$$

Definition 3.2.2.

- (i) If $\lambda\Lambda \subset \Lambda'$, then we call an isogeny from $\mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda'$, the morphism induced by the previous inclusion.
- (ii) Two lattices Λ and Λ' are said to be equivalent if they are homothetic.

Assume λ gives an isogeny with $\lambda\Lambda \subset \Lambda'$, then the isomorphism (3.2.1) induces the following commutative diagram:

$$\begin{array}{ccccc} \mathbb{C} & \longrightarrow & \mathbb{C}/\Lambda & \xrightarrow{\phi} & C(\mathbb{C}) \\ \downarrow \lambda & & \downarrow \lambda & & \downarrow f \\ \mathbb{C} & \longrightarrow & \mathbb{C}/\Lambda' & \xrightarrow{\phi} & C'(\mathbb{C}) \end{array} \tag{3.2.2}$$

where the map λ is the multiplication by λ and the map f is just changing the variable by

$$[\wp(z, \Lambda) : \wp'(z, \Lambda) : 1] \rightarrow [\wp(\lambda z, \Lambda) : \wp'(\lambda z, \Lambda) : 1].$$

Moreover, as we can check in Silverman (2009, VI.4), there is a one to one correspondence between the maps in each column and the map f is an isogeny from $C(\mathbb{C}) \rightarrow C'(\mathbb{C})$ in the following sense:

Definition 3.2.3. An isogeny of two elliptic curves, $f : C(\mathbb{C}) \rightarrow C'(\mathbb{C})$, is a morphism such that $f(\mathcal{O}) = \mathcal{O}'$ where \mathcal{O} and \mathcal{O}' are respectively the identity for the groups $C(\mathbb{C})$ and $C'(\mathbb{C})$. In this case the two elliptic curves are called isogenous. The set of isogenies from an elliptic curve C_1 to an elliptic curve C_2 is denoted by $\text{hom}(C_1, C_2)$.

Remark 3.2.4. Given two elliptic curves C_1 and C_2 , if we associate to the set $\text{hom}(C_1, C_2)$, the addition defined by $(\phi + \psi)(P) = \phi(P) + \psi(P)$, for $P \in C_1$ and $\phi, \psi \in \text{hom}(C_1, C_2)$, then we have an abelian group $\text{hom}(C_1, C_2)$. In addition, this is a torsion-free \mathbb{Z} -module.

The commutative diagram (3.2.2) tells us that f is a group homomorphism. As a consequence of all of these, we see that two elliptic curves are isomorphic if the lattices giving them are homothetic.

Remark 3.2.5. The isogeny $\phi : C_1 \rightarrow C_2$ gives rise a morphism of function fields $\phi^* : K(C_2) \rightarrow K(C_1)$. Thus we have an extension $K(C_1)/\phi^*(K(C_2))$ and thus we can define a map $\text{deg} : \text{hom}(C_1, C_2) \rightarrow \mathbb{Z}$ such that $\text{deg } \phi = [K(C_1) : \phi^*(K(C_2))]$.

3.2.1 Tate module on Elliptic curves

In this section, we shall not stay on the field \mathbb{C} , we will work on a general field K with algebraic closure \overline{K} . Let p be a prime different to the characteristic of K . Let C/K be an elliptic curve defined over K . The subgroup, of points of $C(\overline{K})$ with order dividing p^m , denoted by $C[p^m]$, with m positive integer, is called the p^m -torsion subgroup of $C(\overline{K})$. It turns out that the group $C[p^m]$ is isomorphic to $\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ (see Silverman, 2009, III.6.4). From this consideration, it also has a structure $\mathbb{Z}/p^m\mathbb{Z}$ -module.

Definition 3.2.6.

- (a) The inverse limit of the sequence, where the map p is just the multiplication by p ,

$$C[p] \xleftarrow{p} C[p^2] \xleftarrow{p} C[p^3] \xleftarrow{p} \dots$$

is the set $\varprojlim C[p^n]$ of all $P = (P_n)_n$, with $P_n \in C[p^n]$ and $p(P_{n+1}) = P_n$ for $n \geq 1$.

(b) We denote $T_p(C)$, the inverse limit $\varprojlim C[p^n]$ above and we call it the Tate module as it is a \mathbb{Z}_p -module, where \mathbb{Z}_p is the ring of p -adic integers.

Since for all n , $C[p^n]$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ as groups, then we get a natural isomorphism of \mathbb{Z}_p -modules $T_p(C) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Hence, for two elliptic curves C_1, C_2 , and choosing appropriate bases, $\text{hom}(T_p(C_1), T_p(C_2))$ is isomorphic to $\mathcal{M}_2(\mathbb{Z}_p)$, the set of matrices 2×2 with coefficients in \mathbb{Z}_p .

Using the Tate modules, we can see some properties of morphisms between elliptic curves. Let C_1 and C_2 be two elliptic curves defined over a field K . Suppose ϕ is a isogeny from C_1 to C_2 . Since $\phi(\mathcal{O}) = \mathcal{O}$, then this isogeny gives rise to maps $\phi : C_1[p^n] \rightarrow C_2[p^n]$, for $n \geq 1$. These last maps induce, by taking the image component by component, a morphism $\phi : T_p(C_1) \rightarrow T_p(C_2)$. We see directly that this map is \mathbb{Z}_p -linear so that we can define homomorphism of \mathbb{Z}_p -modules. Thus we have an homomorphism we which denote by $\mathcal{T}_p : \text{hom}(C_1, C_2) \rightarrow \text{hom}(T_p(C_1), T_p(C_2))$, where the two sets are set of morphism w.r.t the appropriate structures.

Lemma 3.2.7. *Let C_1 and C_2 be two elliptic curves defined over a field K . If H is a finitely generated subgroup of $\text{hom}(C_1, C_2)$, then H^* is finitely generated, where,*

$$H^* = \{\phi \in \text{hom}(C_1, C_2) : p\phi \in H \text{ for some integer } p \geq 1\}.$$

Proof. For $\phi \in H^*$, we have, for some $p \geq 1$ and $h \in H$, $p\phi = h$. So we might think of ϕ as a product rh where $r \in \mathbb{R}$ and $h \in H$. To do this we take the tensor product $H \otimes \mathbb{R}$ as \mathbb{Z} -modules. As $\text{hom}(C_1, C_2)$ is a torsion free \mathbb{Z} -module, we can think of H^* as a subset of $\mathbb{R}H$ by the natural inclusion $H^* \hookrightarrow \mathbb{R} \otimes H$. We now adjoin to $\mathbb{R} \otimes H$, which is a finite dimensional vector space over \mathbb{R} , the topology induced by the one from \mathbb{R} . We then extend the map deg on $\text{hom}(C_1, C_2)$ to a continuous map deg on $\mathbb{R} \otimes H$ and hence we have an open set $V = \{\phi \in \mathbb{R} \otimes H : \text{deg } \phi < 1\}$. This is now an open neighbourhood of 0 such that $H^* \cap V = \{0\}$. Hence we have a discrete subgroup H^* of $\mathbb{R} \otimes H$. As the last one is a finite-dimensional vector space, then H^* is finitely generated. \square

Now, we are ready to go to the main result of this section:

Theorem 3.2.8. *Let C_1, C_2 be two elliptic curves defined over a field K . If p is a prime different to the characteristic of K then we have an injection, which we also denote by \mathcal{T}_p ,*

$$\mathcal{T}_p : \text{hom}(C_1, C_2) \otimes \mathbb{Z}_p \rightarrow \text{hom}(T_p(C_1), T_p(C_2)).$$

Proof. The lemma 3.2.7 tells us that any finitely generated subgroup H of $\text{hom}(C_1, C_2)$ gives rise to a finitely generated subgroup which we denoted H^* . Again, as $\text{hom}(C_1, C_2)$ is a torsion free \mathbb{Z} -module then H^* is also torsion-free. Thus we have some generator $\phi_1, \phi_2, \dots, \phi_n$ of H^* .

Now, let $\phi \in \text{hom}(C_1, C_2) \otimes \mathbb{Z}_p$ such that $\mathcal{T}_p(\phi) = 0$, we want to show that $\phi = 0$. Choose H such that $\phi \in H \otimes \mathbb{Z}_p$. With the above consideration, we have

$$\phi = a_1\phi_1 + \cdots + a_n\phi_n, \quad a_i \in \mathbb{Z}_p.$$

For an arbitrary integer n , we can change our a_i in such a way that $a_i \in \mathbb{Z}$ by taking the modulo p^n . We keep the same notation but we should remember that the modulo of the old a_i in $\mathbb{Z}/p^n\mathbb{Z}$ are the new a_i . We now get a new morphism $\phi' = a_1\phi_1 + \cdots + a_n\phi_n$ where the coefficients are now in \mathbb{Z} and this satisfies, $\phi'(C_1[p^n]) = 0$. This is also satisfied by the multiplication by p^n . So by factorisation (see Silverman, 2009, III.4.11), we have $\phi' = p^n\psi$ and hence $\psi \in H^*$. Thus all the new, hence the old, a_i are multiple of p^n , for all $n \geq 1$. This is possible only when the $a_i, i = 1, \dots, n$ are all equal to zero and thus $\phi = 0$. \square

Recall again that $\text{hom}(C_1, C_2)$ is torsion free, so that

$$\text{rank}_{\mathbb{Z}}(\text{hom}(C_1, C_2)) = \text{rank}_{\mathbb{Z}_p}(\text{hom}(C_1, C_2)) \otimes \mathbb{Z}_p.$$

The injectivity in theorem 3.2.8 yields,

$$\text{rank}_{\mathbb{Z}}(\text{hom}(C_1, C_2)) \otimes \mathbb{Z}_p \leq \text{rank}_{\mathbb{Z}_p}(\text{hom}(T_p(C_1), T_p(C_2))).$$

We know that $\text{hom}(T_p(C_1), T_p(C_2)) \simeq \mathcal{M}_2(\mathbb{Z}_p)$, we thus obtain the following corollary:

Corollary 3.2.9. *For two elliptic curves C_1 and C_2 defined over a field K , the \mathbb{Z} -module $\text{hom}(C_1, C_2)$ is free of rank $r \leq 4$.*

3.3 On the side of Drinfeld modules

Let us see the analogous in the case of Drinfeld modules. When we dealt with elliptic curves, we were always using lattices of rank 2. Like this, when we talk about isogenies, isomorphism between Drinfeld modules, we must stay in a fixed rank. For that, we may remember the proposition 2.3.12, which says that two isogenous Drinfeld modules must have the same rank.

Given a function field k/\mathbb{F} , recall that A is the ring of all elements of k with the only poles at a fixed place ∞ .

Let Λ be a lattice of rank r . We saw that the exponential function associated the lattice Λ is

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

We have seen that this is \mathbb{F} -linear so that now, we have a surjective homomorphism of abelian group $e_{\Lambda} : \mathbf{C}_{\infty} \rightarrow \mathbf{C}_{\infty}$. Furthermore its kernel is Λ so that we now have an isomorphism $e_{\Lambda} : \mathbf{C}_{\infty}/\Lambda \rightarrow \mathbf{C}_{\infty}$.

Suppose that we have two lattices Λ and Λ' , of the same rank r of course, satisfying $c\Lambda \subset \Lambda'$, for some constant $c \in \mathbf{C}_\infty$. This induces a morphism from Λ to Λ' by multiplication by c .

Proposition 3.3.1. *With the same hypothesis as above, if ϕ^Λ and $\phi^{\Lambda'}$ are respectively the Drinfeld modules associated to Λ and Λ' , then there is a twisted polynomial $f(\tau)$ such that $f\phi_a^\Lambda = \phi_a^{\Lambda'}f$ for any element $a \in A$.*

Proof. First, $\Lambda \subset c^{-1}\Lambda'$. Then, $c^{-1}\Lambda'/\Lambda$ is finite because both lattices have the same rank r . So the function f , defined as follows, is well defined

$$f(x) = cx \prod_{l \in c^{-1}\Lambda'/\Lambda - \{0\}} \left(1 - \frac{x}{e_\Lambda(l)}\right).$$

Now, $f(x)$ is an \mathbb{F} -linear entire function. And $f(e_L(x))$ vanishes exactly on $c^{-1}\Lambda'$. Moreover the coefficient of x is c . These are exactly the property of the entire function $e_{\Lambda'}(cx)$. By the proposition 2.4.3, we get $e_{\Lambda'}(cx) = f(e_\Lambda(x))$. We show again the complex multiplication for a lattice Λ :

$$e_\Lambda(ax) = \phi_a^\Lambda(e_\Lambda(x)).$$

The above equality gives us, for $a \in A$, $e_{\Lambda'}(acx) = f(e_\Lambda(ax))$. Hence, by the complex multiplication,

$$f(\phi_a^\Lambda(e_\Lambda(x))) = \phi_a^{\Lambda'}(e_{\Lambda'}(cx)).$$

And thus,

$$f(\phi_a^\Lambda(e_\Lambda(x))) = \phi_a^{\Lambda'}(f(e_\Lambda(x))).$$

We now apply the surjectivity of e_Λ to get

$$f(\phi_a^\Lambda(x)) = \phi_a^{\Lambda'}(f(x)).$$

□

Thus we have a diagram equivalent to the one in 3.2.2:

$$\begin{array}{ccccc} \mathbf{C}_\infty & \longrightarrow & \mathbf{C}_\infty/\Lambda & \xrightarrow{e_\Lambda} & \mathbf{C}_\infty \\ \downarrow c & & \downarrow c & & \downarrow f \\ \mathbf{C}_\infty & \longrightarrow & \mathbf{C}_\infty/\Lambda' & \xrightarrow{e_{\Lambda'}} & \mathbf{C}_\infty \end{array} \quad (3.3.1)$$

The difference between the two Diagrams is that in the second we don't see the Drinfeld modules. That is because in the definition of Drinfeld modules we are not dealing with set of points but with the map itself. But this is clear if we think in such a way that the polynomial f , as we saw in the proposition 3.3.1, gives an isogeny from the Drinfeld modules ϕ^Λ to $\phi^{\Lambda'}$.

Now, let us go the notion of isomorphism. Let $P \in \mathbf{C}_\infty \langle \tau \rangle$ be a morphism between two Drinfeld modules ϕ and ψ defined over \mathbf{C}_∞ , that is $P\phi_a = \psi_a P$ for all $a \in A$. We need P to be invertible; since only constant polynomials are invertible in $\mathbf{C}_\infty \langle \tau \rangle$, P must be a constant in $\mathbf{C}_\infty \langle \tau \rangle$. So, when we work with Drinfeld modules defined over \mathbf{C}_∞ , we have the following proposition:

Proposition 3.3.2. *Let $\lambda \in \mathbf{C}_\infty$ and suppose Λ, Λ' are two lattices of the same rank r . If the two lattices Λ and Λ' are homothetic w.r.t λ i.e. $\Lambda' = \lambda\Lambda$, then λ is an isogeny from ϕ^Λ to $\phi^{\Lambda'}$ i.e. for all $a \in A$, $\lambda\phi_a^\Lambda = \phi_a^{\Lambda'}\lambda$.*

Proof. If $\Lambda' = \lambda\Lambda$, then, in the proof of proposition 3.3.1,

$$\begin{aligned} f(x) &= \lambda x \prod_{l \in \lambda^{-1}\Lambda'/\Lambda - \{0\}} \left(1 - \frac{x}{e_\Lambda(l)}\right) \\ &= \lambda x \prod_{l \in \Lambda/\Lambda - \{0\}} \left(1 - \frac{x}{e_\Lambda(l)}\right) \\ &= \lambda x. \end{aligned}$$

Thus $f(\tau) = \lambda$ and hence $\lambda\phi^\Lambda = \phi^{\Lambda'}\lambda$.

□

3.3.1 Tate module on Drinfeld modules

Continuing with our analogy, we will also show that we can define the Tate module on the Drinfeld modules. In this section we set L to be an extension of \mathbb{F} and we define M to be an algebraic closure of L . We know that a Drinfeld A -module induces a new A -module structure on M by the $a * u = \phi_a(u)$, $u \in M$, $a \in A$, and in that case we denote the module by M_ϕ . We also defined a torsion submodule of M , for an ideal \mathfrak{J} of A different to $\text{char } \phi$, as

$$M_\phi[\mathfrak{J}] = \{u \in M_\phi : \phi_{\mathfrak{J}}(u) = 0\}.$$

Like in the case of elliptic curves, we have the following definition.

Definition 3.3.3. Let ϕ be a Drinfeld module and let \mathfrak{J} be a prime ideal of A different to $\text{char } \phi$. The Tate module of ϕ at \mathfrak{J} is the inverse limit

$$T_{\mathfrak{J}}(\phi) = \varprojlim M_\phi[\mathfrak{J}^n].$$

Let $k_{\mathfrak{J}}$ be the completion of k w.r.t. the valuation induced by \mathfrak{J} . We denote by $A_{\mathfrak{J}} = \varprojlim A/\mathfrak{J}^n$, the ring of \mathfrak{J} -adic integers at \mathfrak{J} in $k_{\mathfrak{J}}$.

From the proof of theorem 2.3.22, $M_\phi[\mathfrak{J}^n]$ is a module over A/\mathfrak{J}^n of rank r_ϕ . This induces an $A_{\mathfrak{J}}$ -module structure on $T_{\mathfrak{J}}(\phi)$ thus we have the following proposition:

Proposition 3.3.4. *Let ϕ be a Drinfeld A -module of rank r_ϕ . With the same notations as above, $T_{\mathfrak{J}}(\phi)$ is a free $A_{\mathfrak{J}}$ -module of rank r_ϕ .*

Again, like in the case of elliptic curves, a morphism $f : \phi \rightarrow \psi$ gives rise to a map $f : T_{\mathfrak{J}}(\phi) \rightarrow T_{\mathfrak{J}}(\psi)$. And, thus, we have a natural additive groups homomorphism:

$$\mathcal{T}_{A_{\mathfrak{J}}} : \text{hom}_L(\phi, \psi) \rightarrow \text{hom}_{A_{\mathfrak{J}}}(T_{\mathfrak{J}}(\phi), T_{\mathfrak{J}}(\psi)).$$

In the proposition 3.3.1, we have seen that a homothety $c \in \mathbf{C}_\infty$ between two lattices gives rise to an isogeny of Drinfeld modules. The construction of the isogeny allows us to carry the A -module structure of \mathbf{C}_∞ to the isogenies: For $a \in A$, ac also gives rise to another isogeny. Though we are in a smaller A -module L , we can also have the same situation: $\text{hom}_L(\phi, \psi)$ is an A -module. Hence we can think about tensoring with ${}_{\mathfrak{J}}A$, w.r.t to the ring A , and we get the following proposition:

Proposition 3.3.5. *If \mathfrak{J} is a prime ideal of A different to the characteristic of two Drinfeld modules ϕ and ψ , then the map,*

$$\mathcal{T}_{A_{\mathfrak{J}}} : \text{hom}_L(\phi, \psi) \otimes_A A_{\mathfrak{J}} \rightarrow \text{hom}_{A_{\mathfrak{J}}}(T_{\mathfrak{J}}(\phi), T_{\mathfrak{J}}(\psi))$$

is injective.

The proof of this proposition is the same as in the case of elliptic curves but now in the category of Drinfeld modules. Some step in the proof are shown in the following remark:

Remark 3.3.6.

- If the image of $f \in \text{hom}_L(\phi, \psi)$ is zero, then f vanishes on all $M_\phi[\mathfrak{J}^i]$, $i \geq 0$. The class group of A being finite, then a power of \mathfrak{J} is principal, say it is equal to (a) . Hence, f vanishes on all $M_\phi[b^i]$, $i \geq 0$.
- This allows us to factorize f as $f = b^i g_i$, for all $i \geq 0$ and where g_i is an isogeny from ϕ to ψ .

And the following result now comes:

Corollary 3.3.7. *For two Drinfeld modules ϕ and ψ of the same rank r , the A -module $\text{hom}_L(\phi, \psi)$ is free of rank at most r^2 .*

Chapter 4

Factorisation of polynomials

In the last chapter we have seen some analogy between Elliptic curves and Drinfeld modules. We continue to develop a theory in Drinfeld modules from the ones in Elliptic curves. Van der Heiden has developed an algorithm for factoring polynomials over a finite field (see van der Heiden, 2004). Again, it has its equivalent in the theory of Elliptic curves which we have already seen in the Introduction of this thesis.

Nevertheless, we are in a particular case of Drinfeld modules, more precisely, the ring A will be the polynomial ring $\mathbb{F}[T]$, where \mathbb{F} is, let us recall, a finite field of characteristic p (prime) of cardinality q . Moreover, the Drinfeld modules will be defined over rings.

4.1 Drinfeld modules over rings

Let R be a ring and suppose $\delta : A \rightarrow R$ is an \mathbb{F} -linear ring homomorphism. This gives an A -algebra structure on R . Denote by $D : R\langle\tau\rangle \rightarrow R$, the derivative at zero.

Definition 4.1.1. A Drinfeld A -module over the ring R is a ring homomorphism $\phi : A \rightarrow R\langle\tau\rangle$ such that $D \circ \phi = \delta$. Moreover, it has to be non-trivial i.e. $\phi_a \notin R$ for some $a \in A$.

Being \mathbb{F} -linear, ϕ is completely determined by its value ϕ_T at T . We see that, like in the case of Drinfeld modules over fields, R admit an A -module structure via the ϕ by setting $a * x = \phi_a(x)$.

For each $a \in A$, ϕ_a is just a particular \mathbb{F} -linear endomorphism. In fact every $\sum_i a_i \tau^i \in R\langle\tau\rangle$ induces a \mathbb{F} -linear endomorphism $R \rightarrow R$ by $\tau(x) = x^q$. Hence, we have a ring homomorphism,

$$R\langle\tau\rangle \longrightarrow \text{End}_{\mathbb{F}}(R). \quad (4.1.1)$$

We define the rank of ϕ as an integer r such that $\deg \phi_a = -rv_\infty(a)d_\infty$, for all $a \in A$. Now, $d_\infty = 1$, so we define r by the expression of ϕ_T . More precisely, this tells us that ϕ_T is of the form $b_r\tau^r + \dots + b_1\tau + b_0$, where $b_r \neq 0$.

Remark 4.1.2. In fact, the relation $\deg \phi_a = -rv_\infty(a)d_\infty$ is not always true like in the case of Drinfeld modules over fields. Namely, a field is an integral domain so that the relation remain true for any $a \in A$. But, in the case of ring, if we take b_r to be nilpotent, then this is not true anymore for some $a \in A$. So, we define the rank only when b_r is not nilpotent.

Having defined the Drinfeld modules over the ring $\mathbb{F}[T]$, let us move to some simplification due to some parts of our algorithm. Namely, like the algorithm of Cantor-Zassenhaus, we will also keep the beginning of the algorithm of Berlekamp (Berlekamp, 1970).

The polynomial to be factored is denoted by f . We remove the multiple factor by working with the *formal derivative* of f . If the formal derivative of

f is identically zero, then $f = \left(\sum_{k=0}^{n/p} a_k^{q/p} t^k \right)^p$, where f must have the form

$f = \sum_{k=0}^{n/p} a_k t^{kp}$. If f' is not zero then, we just divide f by $\gcd(f, f')$ and we get a square-free polynomial.

Remark 4.1.3. In the remark 4.1.2, we assumed the leading coefficient of ϕ_T to be non-nilpotent to be able to define the rank. From the previous consideration, we now, may assume that this leading coefficient is always non-nilpotent. Namely, the ring R will be defined as the quotient A/fA so that if there is a nilpotent element in R , then f must have repeated factor.

Remark 4.1.4. There is a problem in the last part of the previous method. Suppose we are in \mathbb{F}_8 , which is of characteristic 2 and let us take $f = T^3 + T^2$. The derivative is $f' = T^2$ so that the gcd is T^2 . But then dividing f by T^2 gives us $T + 1$ which obviously doesn't contain one of the factor of the original f : T ! In general, this occurs when f is of the form $g^p h$, as the characteristic kills the derivative of g^p . We will give an appropriate algorithm to solve this.

Lemma 4.1.5. *The product of all irreducible monic polynomials in $\mathbb{F}_q[T]$, of degree dividing d , is equal to $T^{q^d} - T$.*

This lemma allows us to do more; given a polynomial $f(T) \in A$, we can factorize it in such a way that all the factors are product of irreducible polynomials with the same degree. How is that possible? We take $f_1 = f$ and for $n \geq 1$, we set $g_n(T) = \gcd(f_n(T), T^{q^n} - T)$ and $f_{n+1} = f_n/g_n$. By the previous lemma, each $g_n, n \geq 1$ only contains irreducible factors of degree n (see Berlekamp, 1970). Then we only have to factor the g'_n s.

Thus our factorization is reduced to a simple case where our polynomial f is a factor of distinct irreducible polynomial of the same degree. From now on, we

assume this and we also set d to be the degree of each factor while the degree of f is n .

Earlier in this work, we said that we may take the homomorphism δ as just the reduction. This is exactly our case in this chapter. Namely, as we said above, we take the A -algebra R to be A/fA , where f is the polynomial to be factored. R is not necessary a field, unless f is irreducible, but R is just an A -algebra. With all these hypotheses, we have the following proposition:

Proposition 4.1.6. *Let $\phi : A \rightarrow R \langle \tau \rangle$ be a Drinfeld module, then ϕ is given by $\phi_T = \sum_{i=0}^r b_r \tau^r$ where $b_r \neq 0$ and $b_0 = T \pmod{f}$. Moreover, if $b_r \notin R^*$, then $\gcd(f, b_r)$ is a proper divisor of f .*

Proof. The first part of the proposition is already given above. By our choice of δ , we have $b_0 = T \pmod{f}$. Now, suppose $b_r \notin R^*$, let us show that $\gcd(f, b_r) \neq f, 1$. Indeed, if it is equal to 1, then for some polynomial u and v , $fu + b_r v = 1$ so that $b_r v = 1$ in R . This contradict the fact that b_r is not invertible. The gcd cannot also be equal to f , as b_r would be a multiple of f and therefore $b_r = 0$ in R . \square

This allows us to add one more condition on the choice of the Drinfeld module: we assume that $b_r \in R^*$.

Now, assume $f = f_1 \cdots f_m$, where the f_i are distinct, so that $dm = n$, with d the degree of each f_i . By the Chinese remainder theorem,

$$R \simeq \bigoplus_{i=1}^m A/f_i A. \quad (4.1.2)$$

Proposition 4.1.7. *With the above hypothesis, suppose $A/f_i A = R_i$. Then the restriction, to R_i , for each i , of the Frobenius map on R , τ , is a Frobenius map on R_i .*

Proof. Let i be a fixed integer. We define $\tau(b \pmod{f_i}) = \tau(b) \pmod{f_i}$. This is well defined as, if $b = b' \pmod{f_i}$, then

$$\begin{aligned} \tau(b \pmod{f_i}) &= \tau(b) \pmod{f_i} \\ &= \tau(b' \pmod{f_i}) \pmod{f_i} \\ &= \tau(b' + cf_i) \pmod{f_i} \quad \text{for some polynomial } c \\ &= (\tau(b') + \tau(cf_i)) \pmod{f_i} \\ &= \tau(b') + c^q f_i^q \pmod{f_i}. \end{aligned}$$

And thus $\tau(b \pmod{f_i}) = \tau(b' \pmod{f_i})$. \square

As a consequence of this, we have the following corollary.

Corollary 4.1.8. *With the same hypothesis as in the previous proposition, we have*

- R_i is invariant under τ ,
- As A -modules, $R \simeq \bigoplus_{i=0}^m R_i$, where the A -module structures are induced by ϕ .

Proof. The first part is obvious. And hence the second part follows by the equality (4.1.2) and using the A -module structure induced by ϕ . \square

We also have the following results:

Corollary 4.1.9.

- Any operators in $R\langle\tau\rangle$ leave each R_i invariant,
- τ^d is the identity on each R_i and hence on R .

Proof. The first part follows from the first part of the previous corollary. To show the second part, we know that for each i , A/f_iA is a finite field with cardinal q^d and the result follows. \square

Lemma 4.1.10. *Let L/K be a Galois extension of degree n . If $\{\lambda_1, \dots, \lambda_n\}$ is the generator of L as a K -vector space and $\{\sigma_1, \dots, \sigma_n\}$ are the elements of the Galois group $\text{Gal}(L/K)$, then $\{\lambda_i\sigma_j, 1 \leq i, j, \leq n\}$ is a generator of $\text{End}_K(L)$ as a K -vectorial space.*

Proof. We know that $\text{End}_K(L)$ is a K -vector space of dimension n^2 , so it suffice to show that $\lambda_i\sigma_j, 1 \leq i, j, \leq n$ are linearly independent over K . By the linear independence of character (see Lang, 2002, Theorem. 4.1), the σ_j 's are linearly independent over L . And with the fact that the λ_i 's are also linearly independent over K , we see that the $\lambda_i\sigma_j$'s are linearly independent over K . Namely, if

$$\sum_{i,j} a_{ij}\lambda_i\sigma_j = 0,$$

then

$$\sum_j \left(\sum_i a_{ij}\lambda_i \right) \sigma_j = 0,$$

so that

$$\sum_i a_{ij}\lambda_i = 0, \quad \forall j.$$

But then, for each j ,

$$a_{ij} = 0.$$

\square

The ring morphism (4.1.1) has as kernel the two sided ideal $(\tau^d - 1)$. Furthermore, this homomorphism gives us the following proposition:

Proposition 4.1.11.

- (a) $R\langle\tau\rangle / (\tau^d - 1) \simeq \prod_{i=1}^m \text{End}_{\mathbb{F}}(R_i)$ so that the image of the map (4.1.1) is isomorphic to $\prod_{i=1}^m \text{End}_{\mathbb{F}}(R_i)$.
- (b) Each coset in the quotient ring $R\langle\tau\rangle / (\tau^d - 1)$ contains ϕ_T , for some Drinfeld module ϕ of rank less or equal to d .

Proof.

- (a) As $R \simeq \bigoplus_{i=1}^m R_i$, then we have

$$R\langle\tau\rangle / (\tau^d - 1) \simeq \prod_{i=1}^m R_i\langle\tau\rangle / (\tau^d - 1).$$

So if we can show that, for each i , $R_i\langle\tau\rangle / (\tau^d - 1)$ is isomorphic to $\text{End}_{\mathbb{F}}(R_i)$, then we are done.

Now, we have seen that $R_i \simeq \mathbb{F}_{q^d}$, then, by the lemma 4.1.10, we see that

$$\text{End}_{\mathbb{F}}(R_j) \simeq \text{End}_{\mathbb{F}}(\mathbb{F}_{q^d}) \simeq \bigoplus_{\sigma \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F})} R_i\sigma.$$

But the later galois group is generated by some σ , so that

$$\text{End}_{\mathbb{F}}(R_j) \simeq \bigoplus_{j=0}^{d-1} R_i\sigma^j.$$

On the other hand, we have a surjective map from $R_i\langle\tau\rangle$ onto $\bigoplus_{j=0}^{d-1} R_i\sigma^j$ by sending τ to σ . And as a surjective map is bijective if the dimension of the two sets are equal, then we have an isomorphism $R_i\langle\tau\rangle / (\tau^d - 1) \simeq \bigoplus_{j=0}^{d-1} R_i\sigma^j$. Hence,

$$R_i\langle\tau\rangle / (\tau^d - 1) \simeq \bigoplus_{j=0}^{d-1} \text{End}_{\mathbb{F}}(R_j).$$

- (b) Suppose $\lambda = \sum_{i=0}^{d-1} \lambda_i \tau^i$ is representing the coset $\bar{\lambda} \in R\langle\tau\rangle / (\tau^d - 1)$. We construct $\phi_T = \sum_{i=0}^d b_i \tau^i$ in the following way:

- $b_i = \lambda_i$ for $1 \leq u \leq d - 1$,
- $b_0 = T \pmod{f}$,
- $b_d = \lambda_0 - b_0$.

Hence the rank of the constructed Drinfeld module is at most d .

□

Remark 4.1.12. Notice that as each R_i is isomorphic to a finite field with order q^d . Then the ring $\text{End}_{\mathbb{F}}(R_j)$ is isomorphic to the ring $\mathcal{M}_d(\mathbb{F})$ of matrices with entries in \mathbb{F} .

We will make use of all of these in the following section.

4.2 Factorisation of polynomials

In the previous section, the second part of the proposition 4.1.11 tells us that every element in the ring $R\langle\tau\rangle/(\tau^d - 1)$ corresponds to a Drinfeld module ϕ by ϕ_T . Thus by the map (4.1.1) modulo $(\tau^d - 1)$, this gives us an \mathbb{F} -linear operator on R . Now by the first part of proposition 4.1.11, this also gives us an \mathbb{F} -linear operator on each R_i , for $i = 1, \dots, m$. These operators satisfy the following proposition.

Proposition 4.2.1. *Let P be the characteristic polynomial of the linear operator on R induced by the map (4.1.1) modulo $(\tau^d - 1)$. Similarly, let, respectively, P_i be the characteristic polynomial of the induced linear operator on R_i , $i = 1, \dots, m$. Then,*

(a) $P = P_1 P_2 \cdots P_m,$

(b) *Let Q be the product of all irreducible P_i . If Q is a proper divisor of P , then, for all $b \in R^*$, $\text{gcd}(\phi_Q(b), f)$ is a proper divisor of f .*

Remark 4.2.2.

- (i) First, note that any linear operator always have characteristic polynomial, so that P and the P_i 's exist. Also, P is of degree n and the P_i 's are of degree d .
- (ii) For $d = 1$, all P_i 's are all of degree one so that $Q = P$. And we cannot apply the previous proposition. But in this case, f splits into linear factors which are easy to find.

Lemma 4.2.3. *If F is a field and P, Q are polynomials in $F[T]$, then there are two polynomials R, S in $F[T]$ such that $R \circ P = QS$.*

Proof. We can assume that P, Q are monic. Let r_1, \dots, r_n be the roots of Q in an algebraic closure of F (some r_i 's can be the same depending on the multiplicity), then we have to find R , such that $R \circ P(r_i) = 0$, for $0 \leq i \leq n$. But if we set $p_i = P(r_i)$, then we see that $R' = \prod_i (T - p_i)$ satisfies the condition $R' \circ P = Q$ (They are equal because they have the same roots, with multiplicities, in the algebraic closure of F). The problem is only that R' ,

might not be in $F[T]$. Now, let us take R the LCM of the minimal polynomial of each p_i in $F[T]$. Thus $R = R''R'$ for some R'' where $R \in F[T]$. Thus

$$R \circ P = (R' \circ P)(R'' \circ P) = Q(R'' \circ P).$$

We take $S = R'' \circ P$, so that $R \circ P = QS$. And this equality tells us that $S \in F[T]$. \square

Let us now prove the proposition 4.2.1.

Proof of proposition 4.2.1.

(a) This comes from the fact that R is a direct sum of each R_i . The first part of the proposition 4.1.11 implies that the operator ϕ_T on R can be expressed as a diagonal of block matrices where each block represents the linear operator ϕ_T on each component R_i of R . Using the usual formula $\det(Mx - I)$, for a matrix M representing the operator, we see that $P(x) = P_1(x) \cdots P_m(x)$.

(b) If $Q \neq 1$, then for each factor P_i in Q , we have, as endomorphism of R_i ,

$$\phi_Q = Q(\phi_T) = 0.$$

Thus for each $b \in R^*$, we have $\phi_Q(b) = 0 \in R_i$. Hence $\phi_Q(b)$ is a multiple of each f_i . Thus $\gcd(\phi_Q(b), f) \neq 1$. It remains to show that this is not equal to f . Indeed, this is true by proving that if P_i is not a factor of Q , then f_i is not a factor of $\phi_Q(b)$. To show this, let i be an index such that P_i is not a factor of Q . Lemma 4.2.3 tells us that there is an element $a \in A$, such that $a \circ \phi_T(b)$ is a multiple of f_i . Thus, $\phi_a(b) = a(\phi_T(b)) = 0 \pmod{f_i}$. Suppose a is a polynomial with minimal degree satisfying this condition. As P_i also satisfies this condition then its degree is greater than the degree of a . Also, $\phi_{\gcd(a, P_i)}(b) = 0 \pmod{f_i}$. Therefore, as $1 \neq \gcd(a, P_i)$ and a is of minimal degree, then this gcd is equal to a , hence $a \mid P_i$. This means that $\gcd(a, Q) = 1$ and thus $\phi_Q(b) \neq 0 \pmod{f_i}$.

\square

4.2.1 Algorithms

The proposition 4.2.1 tells us that if we are lucky, then choosing a Drinfeld module will give us a factor of f . Using this fact, let us develop an algorithm to factor polynomials.

Step 1. Removing multiple factors. We keep the same notation as in the previous section. This step is, as in the Berlekamp's algorithm, done by comparing f with its formal derivative f' . If f' is equal to zero

then as we have seen f is a power of p and we have already seen how to compute the p -th root of f . Also, $\gcd(f, f')$ is a divisor of f . Suppose we are given a polynomial f to factor without any assumed condition. The pseudo-code is in Algorithm 1.

Algorithm 1 Removing multiple factor

```

procedure DECOMPOSEMULTIPLE( $f, m$ )
   $i \leftarrow 1$ 
   $Output \leftarrow \emptyset$ 
   $g \leftarrow f'$ 
  if  $g=0$  then
     $f \leftarrow f^{\frac{1}{p}}$ 
     $Output \leftarrow$  DECOMPOSEMULTIPLE( $f, p$ )
  else
     $h \leftarrow \gcd(f, g)$ 
     $u \leftarrow f/h$ 
    while  $u \neq 1$  do
       $v \leftarrow \gcd(u, h)$ 
       $t \leftarrow u/v$ 
      if  $t \neq 1$  then  $Output \leftarrow Output \cup [t, i]$ 
      end if
       $i \leftarrow i + 1$ 
       $u \leftarrow v$ 
       $h \leftarrow h/v$ 
    end while
  end if
  if  $h \neq 1$  then
     $h \leftarrow h^{\frac{1}{p}}$ 
     $Output \leftarrow Output \cup$  DECOMPOSEMULTIPLE( $h, p$ )
  end if
  for all  $[p, i] \in Output$  do
     $i \leftarrow i * m$ 
  end for
  return  $Output$ 
end procedure

```

How does the Algorithm 1 work? Dividing f by $\gcd(f, f')$ gives us all factors with multiplicity not of the form pk , where k is an integer and p the characteristic of our ground field. By successive gcd elimination, all the factors with the same multiplicity will be separated, starting with the smallest multiplicity. At the end we get only the factors with a power multiple of p . So we apply the procedure again to the

p -th root of these factors. To understand this, let us see the following brief example.

Example 4.2.4. Assume we are in characteristic 3. Suppose f, g, h are square-free factors of F , where $F = f^3g^5h$. Moreover, assume that these three factors are relatively prime.

At the beginning $i = 1$ and the derivative is not 0. The first while loop, will give us $z = h, i = 1$. Following the algorithm, we will see that $z = 1$ until $i = 5$, where z is now equal to g . After this step we get the condition which tells us to go out of the while loop. Before that, we compute $c = f^3$. Hence $(f^3)^{\frac{q}{3}} = f$ and finally we check that this is square free. Therefore the decomposition we get is $h \times g^5 \times f^3$.

Step 2. Grouping irreducible factors of the same degree. We assume that we have a square-free polynomial and we want to group all factors w.r.t to their degree. The method to do this was already explained earlier but let us write it in the form of pseudo-code which is Algorithm 2. Let us just precise that we don't have to run through all the integers less than the degree of f , we can stop only at the half of the degree of f .

Algorithm 2 Grouping factors of the same degree

```

procedure GROUPSAMEDEGREE( $f$ )
   $i \leftarrow 1$ 
   $Output \leftarrow \emptyset$ 
  while  $f \nrightarrow \text{constant}$  do
    if  $i > (\deg f)/2$  then
      return  $Output \cup [f, \deg(f)]$ 
    end if
     $g = \gcd(f, T^{q^i} - T)$ 
    if  $g \neq 1$  then
       $Output \leftarrow Output \cup [g, i]$ 
    end if
     $i \leftarrow i + 1$ 
     $f = f/g$ 
  end while
  return  $Output$ 
end procedure

```

Step 3. Separating factors of the same degree. We can now assume that the polynomial f is product of irreducible polynomials of the same degree d . Moreover, from 4.2.2, we assume that $d \neq 1$. Suppose that the degree of f is equal to n . To separate the irreducible factors, we

follow the Algorithm 3 (which is not a pseudo-algorithm). The code is in Appendix A.

Algorithm 3 Separating factors of the same degree

- a) We choose a twisted polynomial $\lambda_0 + \lambda_1\tau + \dots + \lambda_{d-1}\tau^{d-1}$ which is equal to ϕ_T modulo $(\tau^d - 1)$, for some Drinfeld module ϕ .
 - b) Compute $\phi_T(1), \phi_T(T), \dots, \phi_T(T^{n-1})$ to construct the matrix representing ϕ_T .
 - c) Compute the characteristic polynomial P of ϕ_T .
 - d) As each P_i are of the same degree d (see remark 4.2.2), we can compute Q , by using the same algorithm as in **Step 2** to separate the irreducible P_i of the same degree d .
 - e) Compute the gcd of $\phi_Q(b)$ and f , where b is any element of R (We can for example choose $b = 1$).
 - f) In case we don't get a proper divisor of f , then choose another Drinfeld module as in **Step 3a**. Otherwise, go to the next factorisation.
-

Remark 4.2.5. We are not guaranteed that each irreducible factor of P has multiplicity one. Hence, in **Step 3d**, we need a slight modification of the algorithm in **Step 2** as that algorithm applies only for square-free polynomials.

Example 4.2.6. Let us factorize, $T^4 + T^3 + T - 1$, which we should know in advance to be a product of polynomials of degree 2, in $\mathbb{F}_3[T]$. We choose $\lambda_0 = T^3 + T$ and $\lambda_1 = T^2 + T$. Hence, by the proof of proposition 4.1.11, our Drinfeld module is, defined by

$$\phi_T = T + (T^2 + T)\tau + T^3\tau^2.$$

We compute

- $\phi_T(1) = T^3 + T^2 - T$,
- $\phi_T(T) = -T^3 + 1$,
- $\phi_T(T^2) = -T + 1$,
- $\phi_T(T^3) = T^3 - 1$,

Thus, the matrix of the endomorphism given by ϕ_T is

$$\begin{pmatrix} 0 & 1 & 1 & -1 \\ -1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 1 \end{pmatrix}.$$

The characteristic polynomial of this matrix is $T^4 - T^3 + T^2 - T$ with only factor of degree 2: $Q = T^2 + 1$. Now, computing $\phi_Q(1)$, we get,

$$\phi_Q(1) = -T^3 - T.$$

The final *gcd* with f is $T^2 + 1$.

4.2.2 Complexity

Looking at the previous algorithm we might ask the following questions:

- Does there always exist a Drinfeld module such that the algorithm gives a factor?
- If so, how many Drinfeld modules? What is the chance that our choice of Drinfeld module is good, i.e. we get a factor at the end of the **Step 3**.

The first question allow us to say whether this algorithm works or not. For the second question we are asking what is the chance for us to choose a good Drinfeld module. The later is important as this tells us what is the efficiency of the algorithm. Let us see the answers in the following.

Proposition 4.2.7. *Let ϕ be a Drinfeld module, f the polynomial to be factored and Q be the product of all irreducible characteristic polynomials from the linear operator induced by ϕ on each R_i . Suppose the characteristic polynomial of the linear operator induced by ϕ on R is P . Thus Q is a factor of P . There is some endomorphism $M \in \text{End}_{\mathbb{F}}(R)$ such that the corresponding Q is a proper divisor of P where P is the characteristic polynomial of M .*

Proof. We construct the endomorphism on each R_i in such a way that some corresponding characteristic polynomial is irreducible and some reducible. By the first part of the proposition 4.1.11, we construct the endomorphism on R by glueing the endomorphism on each R_i together. \square

Reducing the endomorphism M , in the previous proposition, modulo $\tau^d - 1$, we see that there is always a Drinfeld module to factor f if f is reducible. Hence the answer of the first question is positive.

We now investigate how efficient is our algorithm. First of all, we know that our Algorithm, by Algorithm 3, is a probabilistic algorithm, hence let us first compute the probability that a choice of Drinfeld modules gives proper factor of the polynomial we have to factor.

Let us recall the following results from linear algebra:

Proposition 4.2.8. *Let F be a field and let $\text{GL}_d(F)$ be the set of all non-singular $d \times d$ matrices in $\mathcal{M}_d(F)$.*

- (a) For an irreducible subset S of $\mathcal{M}_d(F)$ (i.e. $\{0\}$ and F^n are the only invariant subspace of F^n by the operators in S), we have the equality between centralizers $C_{\text{GL}_d(F)}(S) = C_{\mathcal{M}_d(F)}(S) - \mathbf{0}$,
- (b) Let M be a matrix in $\mathcal{M}_d(F)$, then $C_{\mathcal{M}_d(F)}(M) = F[M]$ if and only if the characteristic polynomial of M is irreducible over F .
- (c) All matrices in $\mathcal{M}_d(F)$ with the same irreducible characteristic polynomials are conjugate.

Remark 4.2.9. The last result of the previous proposition comes from the fact that the characteristic polynomial is irreducible. Namely, two matrices are conjugate if and only if they have the same rational canonical form (Curtis, 1986, 25.15). The two first results can be found in (Suprunenko and Tyshkevich, 1968, chap. 1).

Assuming these results, we get the following corollary:

Corollary 4.2.10. *If f is an irreducible polynomial over \mathbb{F} of degree d , then, there are exactly $\prod_{i=1}^{d-1} (q^d - q^i)$ matrices in $\mathcal{M}_d(\mathbb{F})$ with characteristic polynomial f .*

Proof. Let us operate $\text{GL}_d(F)$ by conjugation on $\mathcal{M}_d(\mathbb{F})$. For a matrix $M \in \mathcal{M}_d(\mathbb{F})$ with characteristic polynomial f , we have

$$|\text{Orb}(M, \text{GL}_d(F))| = [\text{GL}_d(F) : \text{Stab}(M, \text{GL}_d(F))]. \quad (4.2.1)$$

We have $\text{Stab}(M, \text{GL}_d(F)) = C_{\text{GL}_d(F)}(M)$, but since f is irreducible, then the linear operator M must be irreducible, hence by the proposition 4.2.8 a, $\text{Stab}(M, \text{GL}_d(F)) = C_{\mathcal{M}_d(\mathbb{F})}(M) - \mathbf{0}$. By the proposition 4.2.8 b, and the fact that f is irreducible of degree d , we have $C_{\mathcal{M}_d(\mathbb{F})}(M)$ is of dimension d over \mathbb{F} . Hence,

$$\text{Stab}(M, \text{GL}_d(F)) = q^d - 1. \quad (4.2.2)$$

By the proposition 4.2.8 c, the number of matrices with f as characteristic polynomial is $|\text{Orb}(M, \text{GL}_d(F))|$. Finally $|\text{GL}_d(F)| = \prod_{i=0}^{d-1} (q^d - q^i)$, so combining this with the equations (4.2.1) and (4.2.2), we get the expected result. \square

It is well known (see Rosen, 2002, chap. 2) that the number of monic irreducible polynomials of degree d over the finite field \mathbb{F} is equal to

$$N_d = \frac{1}{d} \sum_{l|d} \mu(l) q^{\frac{d}{l}}, \quad (4.2.3)$$

where q is the cardinal of \mathbb{F} and μ is the Möbius function.

Given a monic polynomial f of degree d , we can always find a matrix (the companion matrix) with f as characteristic polynomial. As $R_i \langle \tau \rangle / (\tau^d - 1)$

is isomorphic to $\text{End}_{\mathbb{F}}(R_i)$, then choosing a Drinfeld module (by defining ϕ_T) the probability that the characteristic polynomial is irreducible, viewing ϕ_T as endomorphism on R_i , is equal to

$$p_d = N_d \frac{\prod_{i=1}^{d-1} (q^d - q^i)}{q^{d^2}}.$$

Computing this, we have

$$p_d = \frac{1}{dq^d} \left(\prod_{i=1}^{d-1} (1 - q^{i-d}) \right) \left(\sum_{l|d} \mu(l) q^{\frac{d}{l}} \right).$$

Hence, we have the following proposition:

Proposition 4.2.11. *The probability that a randomly chosen Drinfeld module gives a factor is equal to $1 - p_d^m - (1 - p_d)^m$, where m is the number of factors, each of degree d and*

$$p_d = \frac{1}{dq^d} \left(\prod_{i=1}^{d-1} (1 - q^{i-d}) \right) \left(\sum_{l|d} \mu(l) q^{\frac{d}{l}} \right). \quad (4.2.4)$$

Most of the algorithms for factoring large polynomials over finite field, like Berlekamp and Cantor-Zassenhaus, contain the algorithms 2 and 1. The difference is only in the way to separate the factors of the same degree, and hence it is natural to compare the third step to the other algorithms. It is not obvious to compute the running time, as it depends on the way we implement it and there are many of them. But, using classical techniques of computing the running time, by counting the number of multiplication (see van der Heiden, 2004), one finds that, given a Drinfeld module, this is equal to $O(dn^3 + n^2 \log q)$, where q is the cardinal of the underlying field, n the degree of the polynomial to factor, d the degree of each factor.

4.2.2.1 Analysis

The most popular algorithm for factoring polynomials over finite field is the algorithm by Cantor-Zassenhaus (see Cantor and Zassenhaus, 1981). So let us see some analysis of our algorithm and then we will compare it to Cantor-Zassenhaus's algorithm.

Let us approximate the probability p_d . First, by the Möbius inversion formula we have,

$$q^d = \sum_{l|d} l N_l.$$

Hence we have,

$$N_d < \frac{q^d}{d}. \quad (4.2.5)$$

Next,

$$\begin{aligned} q^d - dN_d &\leq \left| \sum_{l|d, l>1} \mu(l) q^{\frac{d}{l}} \right| \\ &\leq \sum_{i=1}^{n/2} q^i \\ &\leq \frac{q}{q-1} q^{n/2}. \end{aligned}$$

Finally we get a lower bound of N_d , which is, after calculation,

$$N_d > \frac{q^d}{d} \left(1 - \frac{q}{q-1} q^{-d/2} \right). \quad (4.2.6)$$

In fact we have the following approximations.

$$N_d \sim \frac{q^d}{d} + O\left(\frac{q^{d/2}}{d}\right).$$

Moreover, $1 - \frac{q}{q-1} q^{-d/2}$ tends to 1 when q is big enough. Hence, the equations (4.2.6) and (4.2.5) tell us that, for large q , $N_d \sim \frac{q^d}{d}$.

For the expression $\prod_{i=1}^{d-1} (1 - q^{i-d})$, we know that it is less than 1, and by direct analysis, the bigger q is, the expression tends to 1.

Therefore, for large q , the probability, p_d is approximately $\frac{1}{d}$.

We now take a simple look at the probability that choosing a Drinfeld module, we get a proper factor. In the proposition 4.2.11, we saw that t_s is equal to $1 - p_d^m - (1 - p_d)^m$. Plotting this with respect to the variables (p_d, m) , with m the number of irreducible factor on the vertical axis, we have the figure 4.1.

Analysing this, we see that the larger m is and the closer p_d is to $\frac{1}{2}$, more we have a chance of finding a proper factor. This is clearly, true as:

- We need the Drinfeld module to give us irreducible as well as reducible characteristic polynomials,
- the more we have factors, more we have a chance of finding one of them.

Example 4.2.12. Let us see some example for $d = 2, 3$.

$d = 2$ A monic polynomial of degree 2 over \mathbb{F} is of the form $T^2 + AT + B$, $A, B \in \mathbb{F}$. Hence there are q^2 of them. Such a polynomial is reducible if it is of the form $(T + a)(T + b)$, $a, b \in \mathbb{F}$. A combination method shows that there are $\binom{q+1}{2} = \frac{q(q+1)}{2}$ of them. Thus, confirming the formula 4.2.3, there are $N_2 = \frac{q^2 - q}{2}$ irreducible polynomials of degree 2 in $\mathbb{F}[T]$.

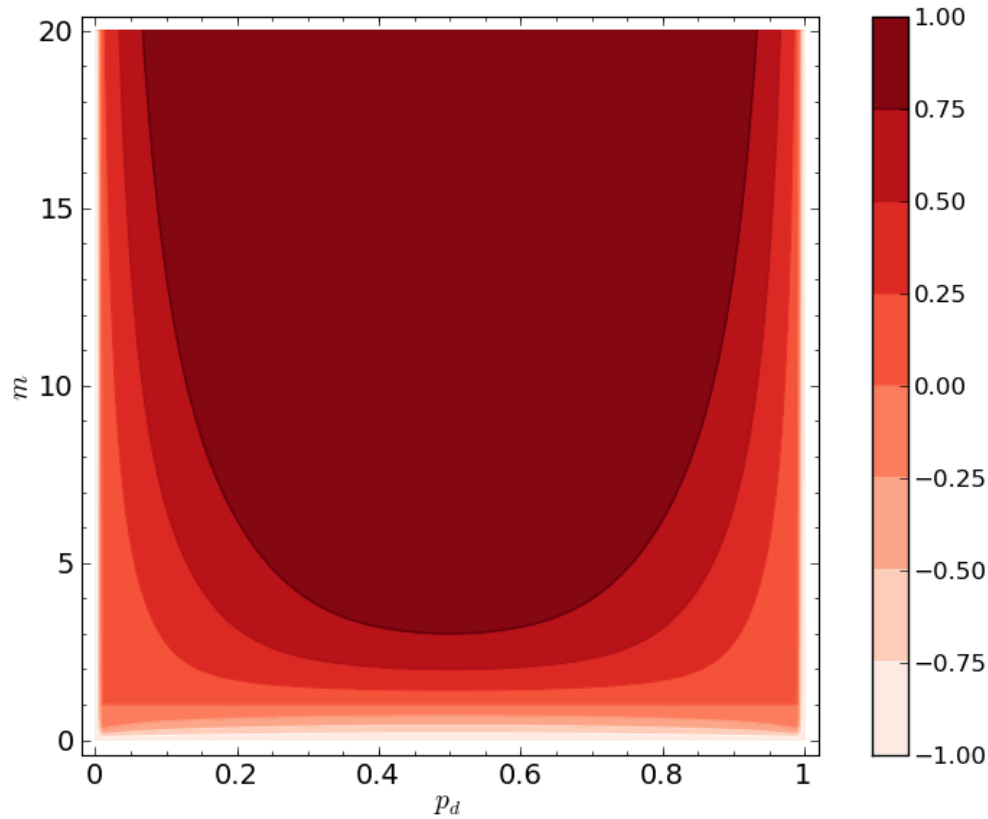


Figure 4.1: Probability of a successful choice of Drinfeld module

Finally, we have the probability

$$p_2 = \frac{(q-1)^2}{2q^2}.$$

$d = 3$ A monic polynomial of degree 3 over \mathbb{F} is of the form $T^3 + AT^2 + BT + C$, $A, B, C \in \mathbb{F}$ and thus we have q^3 of them. A monic is reducible only in the two following cases, $a, b, c \in \mathbb{F}$:

- $(T + a)(T + b)(T + c)$. The combination method tells us that there are $\binom{q+2}{3} = \frac{q(q+1)(q+2)}{6}$ possibilities,
- $(T + a)(T^2 + bT + c)$, with the later factor irreducible. We just said above that there are $\frac{q^2-q}{2}$ possibilities of the later factor so that in total we have $\frac{q^3-q^2}{2}$ possibilities for $(T + a)(T^2 + bT + c)$.

So we have $\frac{2q^3+q}{3}$ reducible polynomials and thus $N_3 = \frac{q^3-q}{3}$ irreducible polynomials, as we can check from the formula 4.2.3.

Hence we have the probability

$$p_3 = \frac{(q-1)^3 (q+1)^2}{3q^5}.$$

To conclude these examples, we see obviously that p_d is approximately equal to $\frac{1}{d}$ with large q and then, finding small factors is not difficult for our method.

4.2.2.2 Comparisons

We finally, compare our algorithm to the Algorithm designed by Cantor-Zassenhaus. The first thing we want to compare is, of course, the running time of Step 3. Recall, that for our algorithm, this is $O(dn^3 + n^2 \log q)$. As seen in Cantor and Zassenhaus (1981), the running time for the Cantor-Zassenhaus algorithm is, asymptotically, $O(n^3 + n^2 \log q)$. If we still keep the condition that q is large compared to n (and thus to d), then these running times are asymptotically the same. Thus for large q , these algorithms present the same advantage.

Since both algorithms are probabilistic algorithms. It is also natural to compare the probability of finding factors within one of Step 3. Recall the setup of the polynomial to be factored: d is the degree of each factor, q is the characteristic of the field, n : is the degree of the polynomial to be factored and $m = n/d$ is the number of factors. Now, the probabilities, denoted by \mathcal{P}_i , are,

- Method using Drinfeld modules:

$$\mathcal{P}_1 = 1 - p_d^m - (1 - p_d)^m,$$

with

$$p_d = \frac{1}{dq^d} \left(\prod_{i=1}^{d-1} (1 - q^{i-d}) \right) \left(\sum_{l|d} \mu(l) q^{\frac{d}{l}} \right)$$

- Cantor-Zassenhaus algorithm (Cantor and Zassenhaus, 1981):

$$\mathcal{P}_2 = 1 - \frac{2r^m - q + 1}{q^n - q}, \quad \text{for odd } q,$$

and

$$\mathcal{P}_2 = 1 - \frac{3r^m - q + 1}{q^n - q}, \quad \text{for even } q,$$

where

$$r = \frac{q^d - 1}{2}.$$

Again, we estimate these values for large q . We already saw that p_d is approximately equal to $\frac{1}{d}$. Thus $\mathcal{P}_1 \sim 1 - \frac{1}{d^m} - \left(1 - \frac{1}{d}\right)^m$. Looking at \mathcal{P}_2 , we have either $\mathcal{P}_2 \sim 1 - \frac{1}{2^{m-1}}$ or $\mathcal{P}_2 \sim 1 - \frac{3}{2^m}$. We may think that \mathcal{P}_2 is greater than \mathcal{P}_1 , and then Cantor-Zassenhaus is better but as far as $\mathcal{P}_1 > 1/2$, we can always say that our algorithm is not bad. If we look at the figure 4.1, with the fact that $p_d \sim \frac{1}{d}$, \mathcal{P}_1 is less than half for large d (compared to m). Hence, our algorithm is not suited to find very large factor if there are not many of them. Combining all of these, our algorithm is better suited for the cases where we are working in a very large field. Moreover, more the factors we have and the smaller they are we have more chance to find them with our method using Drinfeld modules.

Chapter 5

Conclusion

This work contains some theory in the area of algebraic and arithmetic geometry. In Chapter 2, we introduced the notion of Drinfeld modules of general rank r . This is a generalization of the Carlitz module which we have seen in Chapter 1. Namely, the Carlitz module is also a Drinfeld A -module where the ring A is the polynomial ring $\mathbb{F}[T]$ and its rank is 1 as it is given by $\phi_T = \tau + T$. Also, in Chapter 2, we investigated the analytic construction of Drinfeld modules from lattices in \mathbb{C}_∞ . As shown in Chapter 3, that construction is analogous to the construction of elliptic curves from lattices in \mathbb{C} . We studied more about that analogy by working about the Tate modules on both sides of elliptic curves and Drinfeld modules.

This analogy gives us an idea, of how to develop an algorithm to factor polynomial using Drinfeld modules, like the algorithm to factor integer in Chapter 1. That is done from the fact that while using elliptic curves to factor integer in \mathbb{N} , we use Drinfeld modules to factor polynomial in $\mathbb{F}[T]$. To do so, in Chapter 4, we defined the notion of Drinfeld modules over ring and we applied it to the ring $\mathbb{F}[T]$ to develop our algorithm. After that, we analyzed the efficiency of this algorithm and we gave some comparison with the algorithm of Cantor-Zassenhaus. Like the algorithm of Cantor-Zassenhaus, we have seen that such an algorithm is better suited for polynomials over large fields. Moreover, our algorithm is good to find small factors. These estimations are just asymptotic but in practice, one never knows which one is the best algorithm for factoring any polynomials. To conclude this Thesis, Cantor and Zassenhaus said:

“The asymptotically best algorithms frequently turn out to be worst on all problems for which they are used”.

Finally, to make this work more complete, we implemented the algorithm using **SINGULAR**. The code is in the Appendix A.

Appendices

Appendix A

Singular program

Here, we give a code for factoring polynomials using Drinfeld modules. This is implemented using Singular. After loading the file, these are the following commands to execute it.

```
> ring = 3,x,lp;
> poly f= (x^2+1)*(x^2+1);
> drinfeldFactor(f);
```

Below is the code.

```
1 LIB "linalg.lib";

proc randomPoly(int d)
{
  int i,j;
6  int q=size(basering);
  int p=char(basering);
  def x=var(1);
  poly s=0;
  if(q==p)
11 {
    for(i=0;i<=d;i++)
    {
      s=s+random(0,p-1)*x^i;
    }
16 }
  else
  {
    number prim=par(1);
    for(i=0;i<=d;i++)
21 {
      j=random(0,q);
```

```

    if(j!=q)
    {
26      s=s+(prim^j)*x^i;
    }
  }
}
return(s);
}
31
proc randomListPoly(int d)
{
  int i;
  list l=list();
36  for(i=1;i<=d;i++)
  {
    l=l+list(randomPoly(d));
  }
  return(l);
41 }

proc charRoot(poly f)
{
46  def r=basing;
  def x=var(1);
  int q=size(r);
  int p=char(r);
  int d=deg(f);
  int n=d/p;
51  def c=coeffs(f,x);
  f=0;
  for(int i=0;i<=n;i++)
  {
56    f=f+c[i*p+1,1]^(q/p)*x^i;
  }
  return(f);
}

proc powerXmod(int q, int i, poly f)
61 {
  int j,k;
  def x=var(1);
  poly h;
  poly g=x;
66  for(j=1;j<=i;j++)

```

```

    {
        h=1;
        for (k=1;k<=q;k++)
        {
71         h=reduce(g*h, std(f));
        }
        g=h;
    }
    return(g);
76 }

proc eGcd(poly f, poly g)
{
    poly r, q, h;
81  if (deg(f)<deg(g))
    {
        h=f;
        f=g;
        g=h;
86  }
    while (g != 0)
    {
        r=reduce(f, std(g));
        f=g;
91  g=r;
    }
    return(simplify(f, 1));
}

96 proc decomposeMultiple(poly f, int m)
{
    def p=char(basing);
    def x=var(1);
    int i=1;
101 list output=list();
    poly g=diff(f, x);
    poly h, u, t, v;
    if (g==0)
    {
106  f =charRoot(f);
        output = decomposeMultiple(f, p);
    }
    else
    {

```

```

111  h = eGcd (f, g);
    u =division(f,h)[1][1,1];
    while( u != 1)
    {
116  v =eGcd (u, h);
    t = division(u,v)[1][1,1];
    if(t != 1)
    {
        output = output+list(list(t, i));
    }
121  i=i+1;
    u=v;
    h = division(h,v)[1][1,1];
    }
    if( h != 1)
126  {
        h = charRoot(h);
        output = output+decomposeMultiple (h, p);
    }
    for(int j=1;j<=size(output);j++)
131  {
        output[j][2]=output[j][2]*m;
    }
    }
    return(output);
136 }

proc groupSameDegree(poly f)
{
141  int i=1;
    int q=size(basing);
    def x=var(1);
    list output=list();
    poly g,w;
146  while(deg(f)!=0)
    {
        if(i>deg(f)/2)
        {
            return(output+list(list(f, deg(f))));
151  }
        w=powerXmod(q,i,f)-x;
        g = eGcd(f, w);
        if(g != 1)

```

```

156   {
      output = output+list ( list (g, i));
    }
    i=i+1;
    f =division (f,g)[1][1,1];
  }
161  return(output);
}

166  proc MatrixPolynomial(poly Q, matrix M)
    {
      int i;
      int n=ncols(M);
      list l=coeffs(Q,x);
171  matrix b[n][1]=1;
      matrix Pow=freemodule(n)*b;
      matrix A=diag(l[1][1,1],n)*b;
      for (i=2;i<=size(l[1]);i++)
      {
176  Pow=M*Pow;
      A=A+l[1][i,1]*Pow;
      }
      return(A);
    }
181

proc factoringTrial(poly f, list a)
{
  poly s,Q,phiQ;
  int q,n,i,j,d;
186  q=size(basing);
  def x=var(1);
  n=deg(f);
  d=size(a);
  def b=a[1];
191  a[1]=x;
  a=a+list(b-a[1]);
  list l=list();
  for (i=0;i<n;i++)
  {
196  s=0;
      for (j=0;j<=d;j++)
      {

```

```

    s=s+a [ j +1]*(powerXmod(q , j , f))^ i ;
    }
201 l=l+list ( reduce ( s , std ( f ) ) ) ;
    }
    for ( i =1;i<=n ; i++)
    {
    l [ i]=matrix ( coeffs ( l [ i ] , x ) , n , 1 ) ;
206 }
    matrix M [ n ] [ n ] ;
    for ( i =1;i<=n ; i++)
    {
    for ( j =1;j<=n ; j++)
211 {
        M [ i , j]=l [ j ] [ i , 1 ] ;
    }
    }
    poly P=charpoly ( M ) ;
216 for ( i =1;i<=d -1 ; i++)
    {
    s=powerXmod ( q , i , P ) - x ;
    Q=eGcd ( P , s ) ;
    while ( Q !=1 )
221 {
        P=division ( P , Q ) [ 1 ] [ 1 , 1 ] ;
        Q=eGcd ( P , s ) ;
    }
    }
226 s=powerXmod ( q , d , P ) - x ;
    Q=eGcd ( P , s ) ;
    matrix v=MatrixPolynomial ( Q , M ) ;
    phiQ=0 ;
    for ( i =1;i<=n ; i++)
231 {
        phiQ=phiQ+v [ i , 1 ] * x ^ ( i - 1 ) ;
    }
    return ( eGcd ( f , phiQ ) ) ;
}
236
proc separateSameDegree ( poly f , int d )
{
    poly g , h ;
    list a , output ;
241 if ( d ==1 )
    {

```

```

output=list ();
def x=var (1);
int q=size (basing );
246 int p=char (basing );
if (p!=q)
{
number prim=par (1);
int i=0;
251 while (deg (f)>1)
{
if (subst (f ,x ,prim ^i)==0)
{
256 g=f;
h=x-prim ^i;
output=output+list (h);
f=division (g ,h) [1] [1 ,1];
}
i++;
261 }
output=output+list (f);
}
else {
int i=0;
266 while (deg (f)>1)
{
if (subst (f ,x ,i)==0)
{
271 g=f;
h=x-i;
output=output+list (h);
f=division (g ,h) [1] [1 ,1];
}
i++;
276 }
output=output+list (f);
}
return (output);
}
281 if (deg (f)!=d)
{
a=randomListPoly (d);
g=factoringTrial (f ,a);
while (g==1 || g==f)
286 {

```

```

    a=randomListPoly(d);
    g=factoringTrial(f,a);
  }
291  output=separateSameDegree(division(f,g)[1][1,1],d)+
      separateSameDegree(g,d);
  }
  else
  {
296  output=list(f);
  }
  return(output);
}

301 proc drinfeldFactor(poly f)
  {
    if(deg(f)==0||deg(f)==-1)
    {
306    return(f);
    }
    def constant=leadcoef(f);
    f=f/constant;
    int i,j,k;
    list L=list();
311  list l1=list();
    list output=list(constant);
    list l=decomposeMultiple(f,1);
    poly g;
    for(i=1;i<=size(l);i++)
316  {
      L=groupSameDegree(l[i][1]);
      for(j=1;j<=size(L);j++)
      {
321  l1=separateSameDegree(L[j][1],L[j][2]);
        for(k=1;k<=size(l1);k++)
        {
          output=output+list(list(l1[k],l[i][2]));
        }
      }
    }
326  }
  return(output);
}

```


Appendix B

Big example

Let us explain the main procedures in this program by illustrating them with one example. We will work in the field \mathbb{F}_{81} with a polynomial of degree 50. We first load the program and define the polynomial ring by the following command:

```
> <"singular.sing";
> load("singular.sing");
> ring r=(81,a),x,lp;
```

Assuming that a is the primitive element of the field, our polynomial is

$$\begin{aligned}
 & a^{37}x^{50} + a^{56}x^{49} + a^{45}x^{48} + a^{36}x^{47} + a^{37}x^{46} + a^{51}x^{44} - x^{43} + a^{24}x^{42} + \\
 & a^5x^{41} + a^8x^{40} + a^{77}x^{39} + a^{61}x^{38} + a^{23}x^{37} + a^{55}x^{36} + a^{34}x^{35} + \\
 & a^{47}x^{34} + a^{79}x^{33} + a^{79}x^{32} + a^{19}x^{31} + a^{75}x^{30} + a^{14}x^{29} + a^{49}x^{28} + \\
 & a^{60}x^{27} + a^{62}x^{26} + a^{64}x^{25} + a^9x^{24} + a^{55}x^{23} + a^{54}x^{22} + a^{64}x^{21} + \\
 & a^{11}x^{20} + a^{14}x^{19} + a^{33}x^{18} + a^{33}x^{17} + a^{23}x^{16} + a^{70}x^{15} + a^{69}x^{14} + \\
 & a^{50}x^{13} + a^{35}x^{12} + a^{21}x^{11} + a^{76}x^{10} + a^{71}x^9 + a^{43}x^8 + a^{47}x^7 + \\
 & a^{77}x^6 + a^{21}x^5 + a^{23}x^4 + a^{28}x^3 + a^{71}x^2 + a^{27}x + a^{29} \quad (\text{B.0.1})
 \end{aligned}$$

In singular we define this polynomial with the command:

```
> poly f= a37*x50+a56*x49+a45*x48+a36*x47+a37*x46+a51*x44-x43
+a24*x42+a5*x41+a8*x40+a77*x39+a61*x38+a23*x37+
a55*x36+a34*x35+a47*x34+a79*x33+a79*x32+a19*x31+
a75*x30+a14*x29+a49*x28+a60*x27+a62*x26+a64*x25+
a9*x24+a55*x23+a54*x22+a64*x21+a11*x20+a14*x19+
a33*x18+a33*x17+a23*x16+a70*x15+a69*x14+a50*x13+
a35*x12+a21*x11+a76*x10+a71*x9+a43*x8+a47*x7+a77*x6+
a21*x5+a23*x4+a28*x3+a71*x2+a27*x+a29;
```

Now to factorize this polynomial, we use the command:

```
> drinfeldFactor(f);
```

This gives us the following output:

```
[1]:
  a37
[2]:
  [1]:
    x4+a65*x3+a75*x2+a26*x+a14
  [2]:
    1
[3]:
  [1]:
    x6+a17*x5+a63*x4+a18*x3+a60*x2+a59*x+a25
  [2]:
    1
[4]:
  [1]:
    x6+a28*x5+a37*x3+a75*x2+a63*x+a50
  [2]:
    1
[5]:
  [1]:
    x6+a10*x5+a14*x4+a31*x3+a27*x2+a57*x+a12
  [2]:
    1
[6]:
  [1]:
    x9+a78*x8+a78*x7+a49*x6+a78*x5+a12*x4+a65*x3+a49*x2+
    a46*x+a67
  [2]:
    1
[7]:
  [1]:
    x19+a3*x18+a4*x17+a77*x16+a63*x15+x14+a72*x13+a47*x12+
    a11*x11+x10+a25*x9+a42*x8+a9*x7+a11*x6+a67*x5+a57*x4+
    a67*x3+a26*x2+a26*x+a64
  [2]:
    1
```

This means that the factors of the polynomial B.0.1 are:

- a^{37} is the constant,
- $x^4 + a^{65}x^3 + a^{75}x^2 + a^{26}x + a^{14}$ has multiplicity 1,
- $x^6 + a^{17}x^5 + a^{63}x^4 + a^{18}x^3 + a^{60}x^2 + a^{59}x + a^{25}$ has multiplicity 1,
- $x^6 + a^{28}x^5 + a^{37}x^3 + a^{75}x^2 + a^{63}x + a^{50}$ has multiplicity 1,
- $x^6 + a^{10}x^5 + a^{14}x^4 + a^{31}x^3 + a^{27}x^2 + a^{57}x + a^{12}$ has multiplicity 1,
- $x^9 + a^{78}x^8 + a^{78}x^7 + a^{49}x^6 + a^{78}x^5 + a^{12}x^4 + a^{65}x^3 + a^{49}x^2 + a^{46}x + a^{67}$ has multiplicity 1,

-

$$x^{19} + a^3x^{18} + a^4x^{17} + a^{77}x^{16} + a^{63}x^{15} + x^{14} + a^{72}x^{13} + a^{47}x^{12} + a^{11}x^{11} + x^{10} + a^{25}x^9 + a^{42}x^8 + a^9x^7 + a^{11}x^6 + a^{67}x^5 + a^{57}x^4 + a^{67}x^3 + a^{26}x^2 + a^{26}x + a^{64}$$

has multiplicity 1.

Now let us see how it works inside the command `drinfeldFactor`. We notice that all factors are of multiplicity 1 so that we don't need to remove multiple factors with the command `decomposeMultiple`. The next step is to separate the factors of the same degree. We do the following command.

```
> groupSameDegree(f);
```

The output is:

```
[1]:
[1]:
  x4+a65*x3+a75*x2+a26*x+a14
[2]:
  4
[2]:
[1]:
  x18+a71*x17+a4*x16+a22*x15+a31*x14+a64*x13+
  a79*x12+a24*x11+a8*x10+a67*x9+a15*x8+a37*x7+
  a48*x6+a70*x5+a32*x4+a14*x3+a60*x+a7
[2]:
  6
[3]:
[1]:
  x9+a78*x8+a78*x7+a49*x6+a78*x5+a12*x4+a65*x3+
  a49*x2+a46*x+a67
```

```

[2]:
  9
[4]:
[1]:
  x19+a3*x18+a4*x17+a77*x16+a63*x15+x14+a72*x13+
  a47*x12+a11*x11+x10+a25*x9+a42*x8+a9*x7+a11*x6+
  a67*x5+a57*x4+a67*x3+a26*x2+a26*x+a64
[2]:
  19

```

We notice that we have:

- A polynomial of degree 4 such that the irreducible factors are of degree 4. Hence, this polynomial is already irreducible.
- A polynomial of degree 18 such that the factors are of degree 6. Hence we still have to factor this polynomials.
- A polynomial of degree 9 such that the irreducible factors are of degree 9. This polynomial is irreducible too.
- A polynomial of degree 19 such that the irreducible factors are of degree 19. Again, this must be irreducible.

Finally our last task is to separate the factors in the third polynomial. The command is,

```

> poly g=x18+a71*x17+a4*x16+a22*x15+a31*x14+a64*x13+
  a79*x12+a24*x11+a8*x10+a67*x9+a15*x8+a37*x7+
  a48*x6+a70*x5+a32*x4+a14*x3+a60*x+a7;
> separateSameDegree(g, 6);

```

Finally the output to give us the other factors of B.0.1 is,

```

[1]:
  x6+a28*x5+a37*x3+a75*x2+a63*x+a50
[2]:
  x6+a10*x5+a14*x4+a31*x3+a27*x2+a57*x+a12
[3]:
  x6+a17*x5+a63*x4+a18*x3+a60*x2+a59*x+a25

```

List of References

- Ash, R. (2003). *A Course In Algebraic Number Theory*. Department of Mathematics, University of Illinois at Urbana-Champaign.
- Berlekamp, I. (1970). Factoring polynomials over large finite fields. *Mathematics of computation*, vol. 24, pp. 713–735.
- Cantor, D. and Zassenhaus, H. (1981). New algorithm for factoring polynomials over finite fields. *Math. Comput.*, vol. 36, no. 154, pp. 587–592.
- Carlitz, L. (1932*a*). The arithmetic of polynomials in a Galois field. *American Journal of Mathematics*, vol. 54, no. 1, pp. 39–50.
- Carlitz, L. (1932*b*). On polynomials in a Galois field. *Bulletin (New Series) of the American Mathematical Society*, vol. 38, no. 10, pp. 736–744.
- Carlitz, L. (1935). On certain functions connected with polynomials in a Galois field. *Duke Mathematical Journal*, vol. 1, no. 2, pp. 137–168.
- Curtis, C.W. (1986). *Linear Algebra*. Springer Verlag.
- Decker, W., Greuel, G.-M. and Pfister, G. and Schönemann, H. (2011). SINGULAR 3-1-3. <http://www.singular.uni-kl.de>. A computer algebra system for polynomial computations.
- Drinfeld, V. (1974). Elliptic modules. *Mathematics of the USSR-Sbornik*, vol. 23, p. 561.
- Goss, D. (1997). *Basic structures of function field arithmetic*, vol. 35. Springer Verlag.
- Lang, S. (2002). *Algebra*, vol. 211. Springer Verlag.
- Panchishkin, A. and Potemine, I. (1989). An algorithm for the factorization of polynomials using elliptic modules. In: *Proceedings of the Conference “Constructive methods and algorithms in number theory”*, p. 117.
- Rosen, M. (2002). *Number theory in function fields*, vol. 210. Springer Verlag.
- Schmidt, F. (1931). Analytische Zahlentheorie in Körpern der Charakteristik p . *Mathematische Zeitschrift*, vol. 33, no. 1, pp. 1–32.

- Silverman, J. (2009). *The arithmetic of elliptic curves*, vol. 106. Springer Verlag.
- Silverman, J.H. and Tate, J. (1994). *Rational Points on Elliptic Curves*. Graduate texts in Mathematics. Springer-Verlag.
- Suprunenko, D. and Tyshevich, R. (1968). *Commutative matrices*. Academic Press.
- van der Heiden, G. (2004). Factoring polynomials over finite fields with Drinfeld modules. *Mathematics of computation*, vol. 73, no. 245, pp. 317–322.
- Zariski, O., Samuel, P. and Cohen, I. (1975). *Commutative algebra*, vol. 1. Springer.