5-2009

Construction of a Dimension Two Rank One Drinfeld Module

Catherine Trentacoste
Clemson University, trentac@clemson.edu

CONSTRUCTION OF A DIMENSION TWO RANK ONE DRINFELD MODULE

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master's
Mathematical Science

---

by
Catherine M Trentacoste
May 2009

Accepted by:
Dr. Kevin James, Committee Chair
Dr. Hui Xue, Committee Chair
Dr. Hiren Maharaj

Abstract

Consider $\mathbb{F}_r[t]$ where $r = p^m$ for some prime p and $m \in \mathbb{N}$. Let $f(t)$ be an irreducible square-free polynomial with even degree in $\mathbb{F}_r[t]$ so that the leading coefficient is not a square mod $\mathbb{F}_r$. Let $\mathbb{A} = L = \mathbb{F}_r[t]\left[\sqrt{f(t)}\right]$.

We will examine the basic set-up required for a dimension two rank one Drinfeld module over L along with an explanation of our choice of $f(t)$. In addition we will show the construction for the exponential function.

Acknowledgments

I would like to acknowledge the advice and guidance of my committee chairs Kevin James and Hui Xue. I would also like to thank Dr. Hiren Maharaj for being a member of my committee and taking the time to work with me on this endeavor.

Table of Contents

Chapter 1

Introduction

Consider $\mathbb{F}_r[t]$ where $r = p^m$ for some prime p and $m \in \mathbb{N}$. Let $f(t)$ be an irreducible square-free polynomial with even degree in $\mathbb{F}_r[t]$ so that the leading coefficient is not a square mod $\mathbb{F}_r$. Let $\mathbb{A} = L = \mathbb{F}_r[t]\left[\sqrt{f(t)}\right]$. We will examine the basic set-up required for this dimension two rank one Drinfeld module along with an explanation of our choice of $f(t)$. In addition we will show the construction for the exponential function.

In 1973, Vladimir Drinfeld invented Elliptic modules commonly referred to as Drinfeld modules. The following year he produced a proof of Langlands conjecture for GL_2 over a global function field of positive characteristic. Langlands conjecture for function fields roughly states that there exists a bijection between cuspidal automorphic representations of GL_n and certain representations of a Galois group. Drinfeld used these modules in his proofs of these conjectures. Continued research enabled Drinfeld to generalize Drinfeld modules to shtukas, which allowed him to fully prove Langlands conjecture for GL_2. In 1990, Drinfeld was awarded the Fields Medal for his work.

1.1 Brief Overview of Drinfeld Modules

In order to understand Drinfeld modules, we need to set-up some notation. Here, we will give a general set-up, which we will specialize later. Let X be a smooth, projective geometrically connected curve over the finite field $\mathbb{F}_r$. Let $P_\infty \in X$ be a fixed closed rational point over $\mathbb{F}_r$. Set k to be the function field of X and $\mathbb{A} \subset k$ to be the ring of functions which are regular outside P_∞. Let v_∞ be the valuation associated to the point P_∞ and let $K = k_\infty$ be the completion with respect to v_∞. Let $\overline{K}$ be a fixed algebraic closure of K and $\mathbf{C}_\infty$ be the completion of $\overline{K}$. This comes from the canonical extension of v_∞ to $\overline{K}$. Define τ to be the r$^{\text{th}}$ power mapping, i.e. $\tau^i(x) := x^{r^i}$. Let M be a complete extension of $K \subseteq \mathbf{C}_\infty$. Then $M\{\tau\}$ is the composition ring of Frobenius polynomials in τ.

1.1.1 Properties of $M\{\tau\}$

The following is a concise overview of properties of $M\{\tau\}$. For a more thorough explanation, the reader should refer to Goss [5]. It can be shown that $\tau^i(x)$ is an additive polynomial for all i and hence all polynomials spanned by τ^i are additive. Using properties of additive polynomials, we have that $M\{\tau\}$ forms a ring under composition. Since $M \neq \mathbb{F}_r$, it follows that $M\{\tau\}$ is not commutative, however

$$\tau\alpha = \alpha^r\tau \quad \forall\ \alpha \in M$$

Since M is a field of characteristic r, it can be shown that the set of absolutely additive polynomials over M is $M\{\tau\}$.

Some notation that will be useful is

1. If $P(x)$ is additive, then $P(\tau)$ will denote its representation in $M\{\tau\}$. Similarly, if $P(x)$ is $\mathbb{F}_r$-linear, then $P(\tau)$ is its representation in $M\{\tau\}$. It is important to note that $P(\tau)$ is not obtained from $P(x)$ by substituting τ in for x.

2. The multiplication, $P(\tau) \cdot Q(\tau)$, will refer to multiplication in $M\{\tau\}$.

3. $P(\tau)$ is monic if and only if $P(x)$ is monic.

4. Let $P(\tau) = \sum_{i=0}^{t} \alpha_i \tau^i$ with $\alpha_t \neq 0$. Set $t = \deg(P(\tau))$. Notice that

$$r^t = \deg(P(x))$$

The following theorem shows the relationship between $M[x]$ and $M\{\tau\}$.

Theorem 1. *Let $f(x) \in M[x]$. Then there exists $g(\tau) \in M\{\tau\}$ such that $f(x)$ divides $g(x)$.*

It is important to notice that the set of all $g(\tau)$ satisfying the condition of the theorem forms a left ideal in $M\{\tau\}$.

Next, we will briefly discuss the left and right division algorithms for $M\{\tau\}$ along with some other properties. Let $\{f(\tau), g(\tau)\} \subset M\{\tau\}$. Notice that $f(\tau) \cdot g(\tau) = 0$ in $M\{\tau\}$ implies that $f(\tau)$ or $g(\tau)$ must be 0. Therefore multiplication in $M\{\tau\}$ has both left and right cancellation properties.

Definition 1.

1. $f(\tau)$ is right divisible by $g(\tau)$ if there exists $h(\tau) \in M\{\tau\}$ such that

$$f(\tau) = h(\tau) \cdot g(\tau)$$

2. $f(\tau)$ is left divisible by $g(\tau)$ if there exists $m(\tau) \in M\{\tau\}$ such that

$$f(\tau) = g(\tau) \cdot m(\tau)$$

We can see that if $f(\tau)$ is right divisible by $g(\tau)$ then $g(x)$ divides $f(x)$.

The following proposition is the right division algorithm in $M\{\tau\}$.

Proposition 2. *Let* $\{f(\tau), g(\tau)\} \subset M\{\tau\}$ *with* $g(\tau) \neq 0$. *Then there exists* $\{h(\tau), r(\tau)\} \subset M\{\tau\}$ *with* $\deg(r(\tau)) < \deg(g(\tau))$ *such that*

$$f(\tau) = h(\tau) \cdot g(\tau) + r(\tau)$$

Moreover, $h(\tau)$ *and* $r(\tau)$ *are uniquely determined.*

Now that we have a right division algorithm, the following corollary gives us an important property about left ideals in $M\{\tau\}$.

Corollary 3. *Every left ideal of* $M\{\tau\}$ *is principal.*

To state the left division algorithm, we need the following definition.

Definition 2. M is perfect if and only if $\tau M = M$.

Since τ has trivial kernel, a counting argument can be used to show that all finite fields are perfect. Furthermore, every algebraically closed field is perfect. It can be shown that every finite extension of a perfect field is separable. Now we can define the left division algorithm on $M\{\tau\}$ with an additional assumption on M.

Proposition 4. *Let* M *be perfect and let* $\{f(\tau), g(\tau)\} \subset M\{\tau\}$ *with* $g(\tau) \neq 0$. *Then there exists* $\{h(\tau), r(\tau)\} \subset M\{\tau\}$ *with* $\deg(r(\tau)) < \deg(g(\tau))$ *such that*

$$f(\tau) = g(\tau) \cdot h(\tau) + r(\tau)$$

Furthermore, $h(\tau)$ *and* $r(\tau)$ *are uniquely determined.*

The left division algorithm leads to the following corollary about right ideals.

Corollary 5. *If M is perfect, then every right ideal of $M\{\tau\}$ is principal.*

Using the Euclidean Algorithm we can compute the right greatest common divisor of $f(\tau)$ and $g(\tau)$. It is defined as the monic generator of the left ideal generated by $f(\tau)$ and $g(\tau)$. We will denote it as $(f(\tau), g(\tau))$. This leads us to the final lemma we will discuss about $M\{\tau\}$.

Lemma 6. *Let $h(\tau) = (f(\tau), g(\tau))$. Then $h(x)$ is the greatest common divisor of $f(x)$ and $g(x)$.*

1.1.2 Background Definitions and Theorems

To state the general definition of a Drinfeld module, we will present the following definitions and theorem. For further details, the reader should refer to Goss [5].

Definition 3. An $\mathbb{A}$-submodule $L \subset \mathbf{C}_\infty$ (with the usual multiplication of $\mathbb{A}$) is called an M-lattice (or lattice) if and only if

1. L is finitely generated as an $\mathbb{A}$-module
2. L is discrete in the topology of $\mathbf{C}_\infty$
3. Let $M^{\text{sep}} \subseteq \mathbf{C}_\infty$ be the separable closure of M. Then L is contained in M^{sep} and be stable under $\text{Gal}(M^{\text{sep}}/M)$

The rank of L is its rank as a finitely generated torsion-free submodule of $\mathbf{C}_\infty$. Define $d := \text{rank}_{\mathbb{A}}(L)$.

Definition 4. Let L be an M-lattice. Then set

$$e_L(x) = x \prod_{\substack{\alpha \in L \\ 0 \neq \alpha}} (1 - x/\alpha)$$

Drinfeld proved the following result, which is fundamental to the theory behind Drinfeld modules.

Theorem 7. *Let* $0 \neq a \in \mathbb{A}$. *Then*

$$e_L(ax) = ae_L(x) \prod_{0 \neq \alpha \in a^{-1}L/L} (1 - e_L(x)/e_L(\alpha))$$

We shall not go through the proof here, however, it leads us to the following definition.

Definition 5. Let $0 \neq a \in \mathbb{A}$. Then define

$$\phi_a := ax \prod_{0 \neq \alpha \in a^{-1}L/L} (1 - x/e_L(\alpha))$$

From the proof of Theorem 7, we can conclude that $\phi_a \in M\{\tau\}$. With some work, it can be shown that $\deg(\phi_a(\tau)) = d \deg(a)$. For $a \in \mathbb{A}$, the mapping $a \mapsto \phi_a$ is $\mathbb{F}_r$-linear. Also, if $a \in \mathbb{F}_r \subset \mathbb{A}$ then $\phi_a = a\tau^0$. Finally,

$$\phi_{ab}(\tau) = \phi_a(\tau)\phi_b(\tau) = \phi_b(\tau)\phi_a(\tau) = \phi_{ba}(\tau).$$

This last property is not obvious since multiplication in $M\{\tau\}$ is not commutative.

1.1.3 Definition of a Drinfeld Module

Now we are ready to define a Drinfeld module.

Definition 6. The injection which maps $\mathbb{A}$ into $M\{\tau\}$ by $a \mapsto \phi_a$, associated to L is called the Drinfeld module associated to L. Its rank is $d = \text{rank}_{\mathbb{A}}(L)$.

We can actually give a more general definition of a Drinfeld module. For this, we will use the following definitions.

Definition 7. An $\mathbb{A}$ field $\mathcal{F}$ is a field, $\mathcal{F}$, equipped with a fixed morphism $\iota : \mathbb{A} \to \mathcal{F}$. Define the characteristic of $\mathcal{F}$, $\wp$, to be the kernel of ι which is a prime ideal. We say $\mathcal{F}$ has generic characteristic if and only if $\wp = (0)$; otherwise we say that $\wp$ is finite and $\mathcal{F}$ has finite characteristic.

Over $\mathcal{F}$ we have the ring $\mathcal{F}\{\tau\}$. Let

$$f(\tau) = \sum_{i=0}^{v} a_i \tau^i \in \mathcal{F}\{\tau\}$$

Set

$$Df := a_0 = f'(\tau)$$

Then the mapping from $\mathcal{F}\{\tau\}$ to $\mathcal{F}$ defined by $f \mapsto Df$ is a morphism of $\mathbb{F}_r$-algebras.

So another definition of a Drinfeld module is given by the following.

Definition 8. Let $\phi : \mathbb{A} \to \mathcal{F}\{\tau\}$ be a homomorphism of $\mathbb{F}_r$-algebras. Then ϕ is a Drinfeld module over $\mathcal{F}$ if and only if

1. $D \circ \phi = \iota$
2. For some $a \in \mathbb{A}$, $\phi_a \neq \iota(a)\tau^0$

1.2 The Carlitz Module

Prior to Drinfeld's discovery, Leonard Carlitz discovered the Carlitz module in 1938. He used the Carlitz module to give an explicit construction of the class field theory of $\mathbb{F}_r(t)$. The Carlitz module is a dimension one rank one Drinfeld module. Here, we let $\mathbb{A} = \mathbb{F}_r[t]$ and $L = \mathbb{A}$, which implies that $k = \mathbb{F}_r(t)$. For $d \geq 0$, define

$$\mathbb{A}(d) = \{\alpha \in \mathbb{A} : \deg(\alpha) < d\}$$

So $\mathbb{A}(d)$ is a d-dimensional $\mathbb{F}_r$-vector space of polynomials of degree less than d. And

$$\mathbb{A} = \bigcup \mathbb{A}(d)$$

Set $e_0(x) = x$ and for $d > 0$,

$$e_d(x) = \prod_{\alpha \in \mathbb{A}(d)} (x - \alpha)$$

$$= \sum_{i=0}^{d} (-1)^{d-i} x^{r^i} \frac{D_d}{D_i L_{d-i}^{r^i}}$$

where

$$[i] = t^{r^i} - t$$

$$D_i = [i][i-1]^r \dots [1]^{r^{i-1}}$$

$$L_i = [i][i-1] \dots [1]$$

It can be shown that $e_d(\tau) \in \mathbb{A}\{\tau\}$ and

$$[i] = \prod_{\substack{f \text{ monic polynomial} \\ \deg(f) | i}} f$$

$$D_i = [i] D_{i-1}^r = \prod_{\substack{g \text{ monic} \\ \deg(g) = i}} g$$

$$L_i = \text{lcm of all polynomials of degree } i$$

Now dividing our formula for $e_d(x)$ by

$$\prod_{0 \neq \alpha \in \mathbb{A}(d)} \alpha$$

then taking the limit as d approaches infinity, we obtain the Carlitz exponential:

$$e_C(x) = \sum_{j=0}^{\infty} \frac{x^{r^j}}{D_j}$$

For $x \in \mathbf{C}_\infty$ and $a \in \mathbb{A}$ with $a = \sum_{j=0}^{v} a_j t^j$ where $a_j \in \mathbb{F}_r$ and $a_v \neq 0$ we have that

$$e_C(ax) = ae_C(x) + \sum_{j=1}^{v} C_a^{(j)} e_C(x)^{r^j}$$

where $\{C_a^{(j)}\} \subset \mathbb{A}$ and $C_a^{(v)} = a_v$.

Now set

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{v} C_a^{(j)} \tau^j$$

So

$$e_C(ax) = C_a(e_C(x))$$

The mapping $C : \mathbb{A} \to k\{\tau\}$ defined by $a \mapsto C_a$ which is an injection of $\mathbb{F}_r$-algebras is called the Carlitz Module.

Later on, we will generalize this construction to a quadratic extension of $\mathbb{F}_r(t)$. In Chapter 3, we will explicitly define the corresponding valuation to our quadratic extension; while in Chapter 4, we construct $e_d(x)$ and give a formula which recursively defines it.

Chapter 2

Set-up

Let $\mathbb{F}_r$ be the finite field with $r = p^m$ elements. In this example, we will be examining the function field $\mathbb{F}_r(t)$ and its quadratic extension. Let $f(t)$ be a square-free polynomial in $\mathbb{F}_r[t]$, then $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$ is a quadratic extension of $\mathbb{F}_r(t)$. This is a special case of the set-up which was given for a general Drinfeld module.

2.1 Background on the Point at Infinity

We will give a brief discussion about points of certain function fields. The reader should refer to Rosen [7] for a more in depth discussion. Let $\mathbb{F}_r$ be a finite field. A function field in one variable over $\mathbb{F}_r$ is a field k containing $\mathbb{F}_r$ and at least one element t, transcendental over $\mathbb{F}_r$, such that $k/\mathbb{F}_r(t)$ is a finite algebraic extension. A field with this property has transcendental degree one over $\mathbb{F}_r$. It can be shown that the algebraic closure of $\mathbb{F}_r$ in k is finite over $\mathbb{F}_r$.

There is a natural one-to-one correspondence between function fields over $\mathbb{F}_r$ and smooth projective curves over $\mathbb{F}_r$. Under such correspondence, a closed point of the curve corresponds to a place of the function field. A place of k is, by definition, a discrete valuation ring of k. The valuation ring associated to a place has quotient field equal to k.

In the case that $k = \mathbb{F}_r(t)$, the corresponding curve is $\mathbb{P}^1_{\mathbb{F}_r}$. And $\mathbb{P}^1_{\mathbb{F}_r}$ is covered by two subvarities $\mathbb{P}^1_{\mathbb{F}_r} - \{P_0\}$ and $\mathbb{P}^1_{\mathbb{F}_r} - \{P_\infty\}$. They are both affine lines $\mathbb{A}^1 \cong \mathrm{Spec}\,(\mathbb{F}_r[T])$ and $\mathbb{A}^1 \cong \mathrm{Spec}\,(\mathbb{F}_r[t])$ respectively. Here $T = 1/t$ and the point P_0 corresponds to the distinct valuation $v_0(t) = 1$. And the point P_∞ corresponds to the distinct valuation $v_\infty(t) = v_\infty(1/T) = -1$. Every other non-zero place of $\mathbb{F}_r(t)$ is given by a unique monic irreducible $\mathbf{p}$ in $\mathbb{F}_r[t]$.

In our case that $F = k = \mathbb{F}_(t)\left(\sqrt{f(t)}\right)$, the corresponding curve, denoted by X, is a double cover of $\mathbb{P}^1_{\mathbb{F}_r}$. The curve X is also covered by two affine subvarieties, which are double covers of $\mathbb{P}^1_{\mathbb{F}_r} - \{P_0\}$ and $\mathbb{P}^1_{\mathbb{F}_r} - \{P_\infty\}$ respectively.

Now we investigate the behavior of the inverse image of P_∞ in X. Let $\mathcal{O}'_F$ denote the integral closure of $\mathbb{F}_r[T]$ in $F = \mathbb{F}_r(t) = \mathbb{F}_r(T)$. Also, let $\mathfrak{m}_\infty$ denote the prime of $\mathbb{F}_r[T]$ corresponding to P_∞. Then P_∞, is ramified in X if and only if $\mathfrak{m}_\infty\mathcal{O}'_F = \mathfrak{m}^2$ for some non-zero prime ideal $\mathfrak{m}$ in $\mathcal{O}'_F$. Otherwise, P_∞ is unramified, in which case, either P_∞ splits completely or P_∞ is inert in X. If P_∞ splits, then $\mathfrak{m}_\infty\mathcal{O}'_F = \mathfrak{m}_1\mathfrak{m}_2$ where $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are distinct prime ideals in $\mathcal{O}'_F$. On the contrary, if P_∞ is inert, then $\mathfrak{m}_\infty\mathcal{O}'_F$ remains a prime ideal in $\mathcal{O}'_F$.

2.2 Integral Closure

We will begin by constructing the integral closure for the quadratic extension of our function field. Recall that the ring of functions which are regular outside P_∞ is $\mathbb{A} = \mathbb{F}_r[t]$.

Proposition 8. $\mathbb{F}_r[t] + \mathbb{F}_r[t]\left[\sqrt{f(t)}\right]$ *is the integral closure of* $\mathbb{F}_r[t]$ *in* $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$.

Proof. Let $\mathcal{O}_F$ be the integral closure of $\mathbb{F}_r[t]$ in $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$. Consider

$$a \in \mathbb{F}_r[t] + \mathbb{F}_r[t]\left[\sqrt{f(t)}\right].$$

(Observe that we are actually referring to the direct sum, but for simplicity of notation, we will denote this by plus.) So

$$a = \sum_{i=0}^{k_1} \alpha_i t^i + \sqrt{f(t)} \sum_{j=0}^{k_2} \beta_j t^j$$

Then a is a zero of the polynomial

$$\left(x - \sum_{i=0}^{k_1} \alpha_i t^i + \sqrt{f(t)} \sum_{j=0}^{k_2} \beta_j t^j \right) \left(x - \sum_{i=0}^{k_1} \alpha_i t^i - \sqrt{f(t)} \sum_{j=0}^{k_2} \beta_j t^j \right)$$

$$= \left(x - \sum_{i=0}^{k_1} \alpha_i t^i \right)^2 - f(t) \left(\sum_{j=0}^{k_2} \beta_j t^j \right)^2$$

So a is a zero of a monic polynomial in $\mathbb{F}_r[t][x]$. Hence $\mathbb{F}_r[t] + \mathbb{F}_r[t]\left[\sqrt{f(t)}\right] \subseteq \mathcal{O}_F$.

Now suppose that $g \in \mathcal{O}_F$. Then $g^2 + a_1 g + a_0 = 0$ for some $a_0, a_1 \in \mathbb{F}_r[t]$. We know that $g = p + q\sqrt{f(t)}$ with $p, q \in \mathbb{F}_r[t]$. Note that if $q = 0$, then clearly $g \in \mathbb{F}_r[t] + \mathbb{F}_r[t][\sqrt{f(t)}]$. So, assuming $q \neq 0$,

$$\left(p + q\sqrt{f(t)}\right)^2 + a_1 \left(p + q\sqrt{f(t)}\right) + a_0 = 0$$

Multiplying this out we can see that this implies

$$\sqrt{f(t)}\,(2pq + a_1 q) = 0$$

or

$$2p = -a_1$$

Since 2 is invertible, it follows that $p = -2^{-1}a_1 \in \mathbb{F}_r[t]$.

Also,

$$\begin{aligned} 0 &= p^2 + q^2 f(t) + a_1 p + a_0 \\ &= (a_1)^2 \left((2^{-1})^2 - 2^{-1}\right) + a_0 + q^2 f(t) \end{aligned}$$

or

$$q^2 f(t) = -(a_1)^2 \left((2^{-1})^2 - 2^{-1}\right) - a_0$$

Recall that $f(t)$ is square-free, so we can conclude that $q \in \mathbb{F}_r[t]$. It follows that $\mathcal{O}_F \subseteq \mathbb{F}_r[t] + \mathbb{F}_r[t]\left[\sqrt{f(t)}\right]$. Thus the proposition is proved. □

2.3 Quadratic Extensions of $\mathbb{F}_r(t)$

Now that we have constructed the integral closure in $\mathbb{F}_r[t]$ of $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$, we want to examine the behavior of P_∞ in the function field $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$. Hence, we have the following result.

Theorem 9. *Let* $\mathbf{d} = \deg(f(t))$ *and let* $T = 1/t$. *Then*

1. P_∞ *is ramified if and only if* $\mathbf{d}$ *is odd.*
2. P_∞ *is inert if and only if* $\mathbf{d}$ *is even and* $T^{\mathbf{d}} f(1/T)$ *is not a square mod* (T).
3. P_∞ *splits if and only if* $\mathbf{d}$ *is even and* $T^{\mathbf{d}} f(1/T)$ *is a square mod* (T).

2.3.1 Examples

Before we prove Theorem 9, let's look at some specific examples.

Example 1. Let $f(t) = t+1$, and $T = 1/t$. Then $\mathbb{F}_r(t)\left(\sqrt{t+1}\right)$ becomes $\mathbb{F}_r(T)\left(\sqrt{1/T+1}\right)$.

Notice that

$$\begin{aligned}\sqrt{1/T+1} &= \sqrt{(T+1)/T} \\ &= \sqrt{(T^2+T)/T^2} \\ &= (1/T)\sqrt{T^2+T}\end{aligned}$$

So $\mathbb{F}_r(T)\left(\sqrt{1/T+1}\right) = \mathbb{F}_r(T)\left(\sqrt{T^2+T}\right)$.

Using a similar argument to the one given in Proposition 8, it can be verified that

$$\mathcal{O}'_F = \mathbb{F}_r[T] + \mathbb{F}_r[T]\left[\sqrt{T(T+1)}\right]$$

Let $\mathfrak{m} = \left(T, \sqrt{T^2+T}\right) \subset \mathcal{O}'_F$. We claim that $\mathfrak{m}$ is a maximal ideal. It is enough to show that $\mathcal{O}'_F/\mathfrak{m} \cong \mathbb{F}_r$. Define $\varphi : \mathcal{O}'_F \to \mathbb{F}_r$ by

$$\varphi : \alpha + \beta\sqrt{T(T+1)} \mapsto \alpha_0$$

where $\alpha, \beta \in \mathbb{F}_r[T]$ and α_0 is the constant term of α.

It is easy to see that our map is well-defined. Next we will show that φ is a homomorphism. Let $\alpha, \beta, \gamma, \delta \in \mathbb{F}_r[T]$. Then

$$\begin{aligned}\varphi\left(\left(\alpha+\beta\sqrt{T^2+T}\right)+\left(\gamma+\delta\sqrt{T^2+T}\right)\right) &= \varphi\left((\alpha+\gamma)+(\beta+\delta)\sqrt{T^2+T}\right) \\ &= \alpha_0+\gamma_0 \\ &= \varphi\left(\alpha+\beta\sqrt{T^2+T}\right)+\varphi\left(\gamma+\delta\sqrt{T^2+T}\right)\end{aligned}$$

Next notice that since $\varphi\left(\sqrt{T^2+T}\right)=0$, it follows that $\varphi\left(T^2+T\right)=0$. So,

$$\varphi\left(\left(\alpha+\beta\sqrt{T^2+T}\right)\left(\gamma+\delta\sqrt{T^2+T}\right)\right) = \varphi\left(\alpha\gamma+(\beta\delta)\left(T^2+T\right)+(\alpha\delta+\beta\gamma)\sqrt{T^2+T}\right)$$

$$= \alpha_0\gamma_0$$

$$= \varphi\left(\alpha+\beta\sqrt{T^2+T}\right)\varphi\left(\gamma+\delta\sqrt{T^2+T}\right)$$

So φ is a homomorphism.

We claim that $\mathfrak{m}=\ker\varphi$. Clearly $\mathfrak{m}\subseteq\ker\varphi$. Let $s\in\ker\varphi$. Then

$$s=\sum_{i=0}^{k_1} a_iT^i+\sqrt{T^2+T}\sum_{j=0}^{k_2} b_jT^j.$$

Since $\varphi(s)=0$ we can conclude that $a_0=0$. Therefore

$$s=T\sum_{i=1}^{k_1} a_iT^{i-1}+\sqrt{T^2+T}\sum_{j=0}^{k_2} b_jT^j\in\mathfrak{m}$$

Thus $\mathfrak{m}=\ker\varphi$. So $\mathcal{O}'_F/\mathfrak{m}\cong\mathbb{F}_r$ and it follows that $\mathfrak{m}$ is a maximal ideal, and hence a prime ideal.

Now, let's look at $\mathfrak{m}^2$. We can calculate that

$$\mathfrak{m}^2=\left(T^2,T\sqrt{T^2+T},T^2+T\right).$$

Since $T=T^2+T+(-1)T^2$ that implies $T\mathcal{O}'_F\subseteq\mathfrak{m}^2$. So it follows that the ramification index of T with respect to $\mathfrak{m}$ is at least 2.

We claim that $T\mathcal{O}'_F = \mathfrak{m}^2$. It is enough to show that the generators of $\mathfrak{m}$ are contained in $T\mathcal{O}'_F$. Clearly $T^2, T^2+T \in T\mathcal{O}'_F$. And since $\sqrt{T^2+T} \in \mathcal{O}'_F$, it follows that $T\sqrt{T^2+T} \in T\mathcal{O}'_F$. So $\mathfrak{m}^2 \subseteq T\mathcal{O}'_F$, $T\mathcal{O}'_F = \mathfrak{m}^2$ and therefore $T\mathcal{O}'_F$ is ramified in $\mathcal{O}'_F$.

Example 2. Let $f(t) = t - t^2$, $T = 1/t$ and $r \equiv 3\ (4)$. Then $\mathbb{F}_r(t)\left(\sqrt{t-t^2}\right)$ becomes $\mathbb{F}_r\left(T\right)\left(\sqrt{(1/T)(1-1/T)}\right)$. Notice that

$$\begin{aligned}\sqrt{(1/T)(1-1/T)} &= \sqrt{(1/T^2)(T-1)} \\ &= (1/T)\sqrt{T-1}\end{aligned}$$

Hence $\mathbb{F}_r(t)\left(\sqrt{t-t^2}\right)$ becomes $\mathbb{F}_r\left(T\right)\left(\sqrt{T-1}\right)$.

Again, using a similar argument to Proposition 8, it can be shown that

$$\mathcal{O}'_F = \mathbb{F}_r\left[T\right] + \mathbb{F}_r\left[T\right]\left[\sqrt{T-1}\right].$$

Define $\varphi : \mathcal{O}'_F \to \mathbb{F}_r[y]/\left(y^2+1\right)$ by

$$\varphi : \alpha + \beta\sqrt{T-1} \mapsto \alpha_0 + \beta_0 y + \left(y^2+1\right)$$

where $\alpha, \beta \in \mathbb{F}_r[T]$, α_0 is the constant term in α and β_0 is the constant term in β. Observe that y^2+1 is an irreducible polynomial in $\mathbb{F}_r[y]$.

We can see that φ is well-defined. Next we will show that φ is a homomorphism.

Let $\alpha, \beta, \gamma, \delta \in \mathbb{F}_r[T]$. Then

$$\varphi\left(\left(\alpha + \beta\sqrt{T-1}\right) + \left(\gamma + \delta\sqrt{T-1}\right)\right)$$

$$= \varphi\left((\alpha + \gamma) + (\beta + \delta)\sqrt{T-1}\right)$$

$$= \alpha_0 + \gamma_0 + (\beta_0 + \delta_0)\, y + (y^2 + 1)$$

$$= (\alpha_0 + \beta_0 y + (y^2 + 1)) + (\gamma_0 + \delta_0 y + (y^2 + 1))$$

$$= \varphi\left(\alpha + \beta\sqrt{T-1}\right) + \varphi\left(\gamma + \delta\sqrt{T-1}\right)$$

Next notice that since $\varphi\left(\sqrt{T-1}\right) = y$, it follows that $\varphi(T-1) = y^2$. Then

$$\varphi\left(\left(\alpha + \beta\sqrt{T-1}\right)\left(\gamma + \delta\sqrt{T-1}\right)\right)$$

$$= \varphi\left(\alpha\gamma + \beta\delta\,(T-1) + (\gamma\beta + \alpha\delta)\sqrt{T-1}\right)$$

$$= \alpha_0\gamma_0 + \beta_0\delta_0 y^2 + (\gamma_0\beta_0 + \alpha_0\delta_0)\, y + (y^2 + 1)$$

$$= (\alpha_0 + \beta_0 y)(\gamma_0 + \delta_0 y) + (y^2 + 1)$$

$$= \varphi\left(\alpha + \beta\sqrt{T-1}\right)\varphi\left(\gamma + \delta\sqrt{T-1}\right)$$

Thus φ is a homomorphism.

Next we will show that $\ker\varphi = T\mathcal{O}'_F$. Recall, that $\varphi(T-1) = y^2$. So $\varphi(T) = y^2 + 1$.

Hence $T\mathcal{O}'_F \subseteq \ker\varphi$. Now let $s \in \ker\varphi$. So

$$s = \sum_{i=0}^{k_1} a_i T^i + \sqrt{T-1}\sum_{j=0}^{k_2} b_j T^j.$$

Since $\varphi(s) = y^2 + 1$, this implies that $a_0 = b_0 = 0$. So

$$s = T\left(\sum_{i=1}^{k_1} a_i T^{i-1} + \sqrt{T-1}\sum_{j=1}^{k_2} b_j T^{j-1}\right) \in T\mathcal{O}'_F$$

Hence $T\mathcal{O}'_F = \ker\varphi$. Therefore we can conclude that $\mathcal{O}'_F/T\mathcal{O}'_F \cong \mathbb{F}_r[y]/\left(y^2+1\right)$. Since $\mathbb{F}_r[y]/\left(y^2+1\right)$ is a field, it follows that $\mathcal{O}'_F/T\mathcal{O}'_F$ is a field and thus $T\mathcal{O}'_F$ is maximal. We conclude that $T\mathcal{O}'_F$ is prime and so $T\mathcal{O}'_F$ is inert in $\mathcal{O}'_F$.

Example 3. Let $f(t) = t^2 + t$ and $T = 1/t$. Then $\mathbb{F}_r(t)\left(\sqrt{t^2+t}\right) = \mathbb{F}_r\left(T\right)\left(\sqrt{(1/T)(1+1/T)}\right)$. Notice that

$$\begin{aligned}\sqrt{(1/T)(1+1/T)} &= \sqrt{(1/T^2)(T+1)} \\ &= (1/T)\sqrt{T+1}\end{aligned}$$

Hence $\mathbb{F}_r(t)\left(\sqrt{t^2+t}\right)$ becomes $\mathbb{F}_r\left(T\right)\left(\sqrt{T+1}\right)$.

We can show, using a similar argument to Proposition 8, that

$$\mathcal{O}'_F = \mathbb{F}_r\left[T\right] + \mathbb{F}_r\left[T\right]\left[\sqrt{T+1}\right].$$

Let $\mathfrak{m}_1 = \left(T, \sqrt{T+1}+1\right)$ and $\mathfrak{m}_2 = \left(T, \sqrt{T+1}-1\right)$. Define $\varphi_1 : \mathcal{O}'_F \to \mathbb{F}_r$ by

$$\varphi_1 : \alpha + \beta\sqrt{T+1} \mapsto \alpha_0 + \beta_0$$

where $\alpha, \beta \in \mathbb{F}_r[T]$ and α_0 and β_0 are the constant terms of α and β respectively.

Clearly φ_1 is well-defined. First, we will check that φ_1 is a homomorphism. Let

$\alpha, \beta, \gamma, \sigma \in \mathbb{F}_r[T]$. Then

$$\varphi_1\left(\left(\alpha + \beta\sqrt{T+1}\right) + \left(\gamma + \sigma\sqrt{T+1}\right)\right)$$

$$= \varphi_1\left((\alpha + \gamma) + (\beta + \sigma)\sqrt{T+1}\right)$$

$$= \alpha_0 + \gamma_0 + (\beta_0 + \sigma_0)$$

$$= \alpha_0 + \beta_0 + \gamma_0 + \sigma_0$$

$$= \varphi_1\left(\alpha + \beta\sqrt{T+1}\right) + \varphi_1\left(\gamma + \sigma\sqrt{T+1}\right)$$

And

$$\varphi_1\left(\left(\alpha + \beta\sqrt{T+1}\right)\left(\gamma + \sigma\sqrt{T+1}\right)\right)$$

$$= \varphi_1\left((\alpha\gamma) + (\beta\sigma)(T+1) + (\gamma\beta + \alpha\sigma)\sqrt{T+1}\right)$$

$$= \alpha_0\gamma_0 + \beta_0\sigma_0 + (\gamma_0\beta_0 + \alpha_0\sigma_0)$$

$$= (\alpha_0 + \beta_0)(\gamma_0 + \sigma_0)$$

$$= \varphi_1\left(\alpha + \beta\sqrt{T+1}\right)\varphi_1\left(\gamma + \sigma\sqrt{T+1}\right)$$

Hence φ_1 is a homomorphism.

We claim that $\ker\varphi_1 = \mathfrak{m}_1$. We know that $\varphi_1(T) = 0$ and since

$$\varphi_1\left(\sqrt{T+1} - 1\right) = 1 - 1 = 0,$$

it follows that $\mathfrak{m}_1 \subseteq \ker \varphi_1$. Now, let $s \in \ker \varphi_1$. So

$$s = \sum_{i=0}^{k_1} a_i T^i + \sqrt{T+1} \sum_{j=0}^{k_2} b_j T^j.$$

Since $\varphi_1(s) = 0$, it follows that $a_0 = b_0 = 0$. So

$$s = T \left(\sum_{i=1}^{k_1} a_i T^{i-1} + \sqrt{T+1} \sum_{j=1}^{k_2} b_j T^{j-1} \right) \in \mathfrak{m}_1$$

So $\mathfrak{m}_1 = \ker \varphi_1$. Therefore $\mathcal{O}'_F/\mathfrak{m}_1 \cong \mathbb{F}_r$, so $\mathcal{O}'_F/\mathfrak{m}_1$ is a field. Hence $\mathfrak{m}_1$ is a maximal and thus a prime ideal.

Similarly, we can define $\varphi_2 : \mathcal{O}'_F \to \mathbb{F}_r$ by

$$\varphi_2 : \alpha + \beta\sqrt{T+1} \mapsto \alpha_0 - \beta_0$$

where $\alpha, \beta \in \mathbb{F}_r[T]$ and α_0, β_0 are the constant terms of α and β respectively.

Clearly φ_2 is well-defined. First we will check that φ_2 is a homomorphism. Let

$\alpha, \beta, \gamma, \sigma \in \mathbb{F}_r[T]$. Then

$$\varphi_2\left(\left(\alpha+\beta\sqrt{T+1}\right)+\left(\gamma+\sigma\sqrt{T+1}\right)\right)$$

$$=\varphi_2\left((\alpha+\gamma)+(\beta+\sigma)\sqrt{T+1}\right)$$

$$=\alpha_0+\gamma_0-(\beta_0+\sigma_0)$$

$$=\alpha_0-\beta_0+\gamma_0-\sigma_0$$

$$=\varphi_2\left(\alpha+\beta\sqrt{T+1)}\right)+\varphi_2\left(\gamma+\sigma\sqrt{T+1}\right)$$

And

$$\varphi_2\left(\left(\alpha+\beta\sqrt{T+1}\right)\left(\gamma+\sigma\sqrt{T+1}\right)\right)$$

$$=\varphi_2\left((\alpha\gamma)+(\beta\sigma)(T+1)+(\gamma\beta+\alpha\sigma)\sqrt{T+1}\right)$$

$$=\alpha_0\gamma_0+\beta_0\sigma_0-(\gamma_0\beta_0+\alpha_0\sigma_0)$$

$$=(\alpha_0-\beta_0)(\gamma_0-\sigma_0)$$

$$=\varphi_2\left(\alpha+\beta\sqrt{T+1}\right)\varphi_2\left(\gamma+\sigma\sqrt{T+1}\right)$$

Hence φ_2 is a homomorphism.

We claim that $\ker\varphi_2=\mathfrak{m}_2$. We know that $\varphi_2(T)=0$ and since

$$\varphi_2\left(\sqrt{T+1}+1\right)=-1+1=0,$$

t follows that $\mathfrak{m}_2 \subseteq \ker \varphi_2$. Now, let $s \in \ker \varphi_2$. So

$$s = \sum_{i=0}^{k_1} a_i T^i + \sqrt{T+1} \sum_{j=0}^{k_2} b_j T^j.$$

Since $\varphi_2(s) = 0$, it follows that $a_0 = b_0 = 0$. So

$$s = T \left(\sum_{i=1}^{k_1} a_i T^{i-1} + \sqrt{T+1} \sum_{j=1}^{k_2} b_j T^{j-1} \right) \in \mathfrak{m}_2$$

So $\mathfrak{m}_2 = \ker \varphi_2$. Therefore $\mathcal{O}'_F / \mathfrak{m}_2 \cong \mathbb{F}_r$, so $\mathcal{O}'_F / \mathfrak{m}_2$ is a field. Hence $\mathfrak{m}_2$ is a maximal and thus a prime ideal.

Finally, we observe that

$$\mathfrak{m}_1 \mathfrak{m}_2 = \left(T^2, T \left(\sqrt{T+1} - 1 \right), T \left(\sqrt{T+1} + 1 \right), T \right)$$

So it is obvious that $\mathfrak{m}_1 \mathfrak{m}_2 \subseteq T\mathcal{O}'_F$. Consider $\left(T \left(\sqrt{T+1} - 1 \right), T \left(\sqrt{T+1} + 1 \right) \right)$, which is contained in $\mathfrak{m}_1 \mathfrak{m}_2$. Then the difference of our two generators must be in this ideal and

$$T \left(\sqrt{T+1} - 1 \right) - T \left(\sqrt{T+1} + 1 \right) = 2T$$

Hence

$$T\mathcal{O}'_F \subseteq \left(T \left(\sqrt{T+1} - 1 \right), T \left(\sqrt{T+1} + 1 \right) \right) \subseteq \mathfrak{m}_1 \mathfrak{m}_2$$

Thus $T\mathcal{O}'_F = \mathfrak{m}_1 \mathfrak{m}_2$. So $T\mathcal{O}'_F$ splits in $\mathcal{O}'_F$.

2.3.2 Proof of Theorem 9

Now let's prove Theorem 9. Here, P_∞ is the ideal generated by $\frac{1}{t}$.

Proof. Let $\mathbf{d} = deg(f(t))$ and let $T = 1/t$. Since we have $f(t)$ is square-free, we can write

$$f(t) = t^\epsilon f_0(t)$$

where $\epsilon \in \{0, 1\}$ and $t \nmid f_0(t)$. Let $F = \mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$. Then

$$\begin{aligned}
\mathbb{F}_r(t)\left(\sqrt{f(t)}\right) &= \mathbb{F}_r\left(T\right)\left(\sqrt{f\left(1/T\right)}\right) \\
&= \mathbb{F}_r\left(T\right)\left(T^{\lceil \mathbf{d}/2 \rceil}\sqrt{f\left(1/T\right)}\right) \\
&= \begin{cases} \mathbb{F}_r\left(T\right)\left(\sqrt{T^{\mathbf{d}} f\left(1/T\right)}\right) & \mathbf{d} \text{ is even} \\ \mathbb{F}_r\left(T\right)\left(\sqrt{T^{\mathbf{d}+1} f\left(1/T\right)}\right) & \mathbf{d} \text{ is odd} \end{cases}
\end{aligned}$$

Let

$$\tilde{f}(T) = \begin{cases} T^{\mathbf{d}} f\left(1/T\right) & \mathbf{d} \text{ is even} \\ T^{\mathbf{d}+1} f\left(1/T\right) & \mathbf{d} \text{ is odd} \end{cases}$$

Let $\tilde{d} = \deg\left(\tilde{f}(T)\right)$. So

$$\tilde{d} = \begin{cases} \mathbf{d} & \epsilon = 0 \\ \mathbf{d} - 1 & \epsilon = 1 \end{cases}$$

So

$$\tilde{f}(T) = \sum_{i=0}^{\tilde{d}} \tilde{f}_i T^i$$

Using a similar argument as in Proposition 8, we can show that

$$\mathcal{O}'_F = \mathbb{F}_r[T] + \mathbb{F}_r[T]\left[\sqrt{\tilde{f}(T)}\right]$$

Thus, $P_\infty = (T)$ in $\mathbb{F}_r[T]$. There are three cases that we need to consider.

Case 1: d is odd

So $\tilde{f}(T) = T\left(T^{\mathbf{d}} f(1/T)\right)$. Let $\mathfrak{m} = \left(T, \sqrt{\tilde{f}\,(T)}\right)$. Define $\varphi : \mathcal{O}'_F \to \mathbb{F}_r$ by

$$\varphi : \alpha + \beta\sqrt{\tilde{f}\,(T)} \mapsto \alpha_0$$

where $\alpha, \beta \in \mathbb{F}_r[T]$ and α_0 is the constant term of α.

Clearly, φ is well-defined. First, we want to show that φ is a homomorphism. Let $\alpha, \beta, \gamma, \delta \in \mathbb{F}_r\,[T]$. Then

$$\varphi\left(\left(\alpha + \beta\sqrt{\tilde{f}(T)}\right) + \left(\gamma + \delta\sqrt{\tilde{f}(T)}\right)\right)$$

$$= \varphi\left((\alpha + \gamma) + (\beta + \delta)\sqrt{\tilde{f}(T)}\right)$$

$$= \alpha_0 + \gamma_0$$

$$= \varphi\left(\alpha + \beta\sqrt{\tilde{f}(T)}\right) + \varphi\left(\gamma + \delta\sqrt{\tilde{f}(T)}\right)$$

Notice that $\varphi\left(\sqrt{\tilde{f}(T)}\right) = 0$, it follows that $\varphi\left(\tilde{f}(T)\right) = 0$. Therefore,

$$\varphi\left(\left(\alpha + \beta\sqrt{\tilde{f}(T)}\right)\left(\gamma + \delta\sqrt{\tilde{f}(T)}\right)\right)$$

$$= \varphi\left(\alpha\gamma + \beta\delta\tilde{f}(T) + (\gamma\beta + \alpha\delta)\sqrt{\tilde{f}(T)}\right)$$

$$= \alpha_0\gamma_0$$

$$= \varphi\left(\alpha + \beta\sqrt{\tilde{f}(T)}\right)\varphi\left(\gamma + \delta\sqrt{\tilde{f}(T)}\right)$$

Thus φ is a homomorphism.

Next we want to show that $\ker\varphi = \mathfrak{m}$. Clearly $\mathfrak{m} \subseteq \ker\varphi$. Now, let $s \in \ker\varphi$. Then

$$s = \sum_{i=0}^{k_1} a_i T^i + \sqrt{\tilde{f}(T)} \sum_{j=0}^{k_2} b_j T^j.$$

So $\varphi(s) = 0$. This implies that $a_0 = 0$ and hence

$$s = T\sum_{i=1}^{k_1} a_i T^{i-1} + \sqrt{\tilde{f}(T)} \sum_{j=0}^{k_2} b_j T^j \in \mathfrak{m}.$$

So $\ker\varphi \subseteq \mathfrak{m}$. Thus $\mathfrak{m} = \ker\varphi$. Using the First Isomorphism Theorem, we can conclude that $\mathcal{O}'_F/\mathfrak{m} \cong \mathbb{F}_r$. So $\mathcal{O}'_F/\mathfrak{m}$ is a field and hence $\mathfrak{m}$ is maximal.

Now, let's look at $\mathfrak{m}^2$. So

$$\mathfrak{m}^2 = \left(T^2, T\sqrt{\tilde{f}(T)}, \tilde{f}(T)\right)$$

Since $T = \tilde{f}(T) - aT^2$ for some $a \in \mathbb{F}_r[T]$, $T\mathcal{O}'_F \subseteq \mathfrak{m}^2$. Recall that $\tilde{f}(T) = T\left(T^{\mathbf{d}} f(1/T)\right)$.

So $\tilde{f}(T)$ is divisible by T and not by T^2. Then $v_\infty\left(\tilde{f}(T)\right) = 1$ and so

$$T\mathcal{O}'_F = \left(T^2, \tilde{f}(T)\right)$$

Since $\sqrt{\tilde{f}(T)} \in \mathcal{O}'_F$, it follows that $T\sqrt{\tilde{f}(T)} \in T\mathcal{O}'_F$. Therefore $\mathfrak{m}^2 = T\mathcal{O}'_F$. Thus $T\mathcal{O}'_F$ is ramified.

Case 2: d is even and $\tilde{f}_0$, the constant term of $\tilde{f}(T)$, is not a square in $\mathbb{F}_r$

Define $\varphi : \mathcal{O}'_F \to \mathbb{F}_r[y]/\left(y^2 - \tilde{f}_0\right)$ by

$$\varphi : \alpha + \beta\sqrt{\tilde{f}\,(T)} \mapsto \alpha_0 + \beta_0 y + \left(y^2 - \tilde{f}_0\right)$$

where $\alpha, \beta \in \mathbb{F}_r[T]$ and α_0, β_0 are the constant terms of α and β respectively. Observe that $y^2 - \tilde{f}_0$ is an irreducible polynomial in $\mathbb{F}_r[y]$. To see this, suppose that

$$\begin{aligned} y^2 - \tilde{f}_0 &= (y+\delta)(y+\gamma) \\ &= y^2 + (\delta+\gamma)y + \delta\gamma \end{aligned}$$

This implies that $\delta+\gamma = 0$ or $\delta = -\gamma$. So $\delta\gamma = -\gamma^2 = -\tilde{f}_0$. This contradicts our assumption that $\tilde{f}_0$ is not a square in $\mathbb{F}_r$. So $\mathbb{F}_r[y]/\left(y^2 - \tilde{f}_0\right)$ is a field.

Again, φ is well-defined. We will show that φ is a homomorphism. Let $\alpha, \beta, \gamma, \delta \in$

$\mathbb{F}_r[T]$. Then

$$\varphi\left(\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)+\left(\gamma+\delta\sqrt{\tilde{f}(T)}\right)\right)$$

$$=\varphi\left((\alpha+\gamma)+(\beta+\delta)\sqrt{\tilde{f}(T)}\right)$$

$$=\alpha_0+\gamma_0+(\beta_0+\delta_0)\,y+\left(y^2-\tilde{f}_0\right)$$

$$=\left(\alpha_0+\beta_0 y+\left(y^2-\tilde{f}_0\right)\right)+\left(\gamma_0+\delta_0 y+\left(y^2-\tilde{f}_0\right)\right)$$

$$=\varphi\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)+\varphi\left(\gamma+\delta\sqrt{\tilde{f}(T)}\right)$$

Next notice that since $\varphi\left(\sqrt{\tilde{f}(T)}\right)=y$, it follows that $\varphi\left(\tilde{f}(T)\right)=y^2$. Then

$$\varphi\left(\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)\left(\gamma+\delta\sqrt{\tilde{f}(T)}\right)\right)$$

$$=\varphi\left(\alpha\gamma+\beta\delta\tilde{f}(T)+(\gamma\beta+\alpha\delta)\sqrt{\tilde{f}(T)}\right)$$

$$=\alpha_0\gamma_0+\beta_0\delta_0 y^2+(\gamma_0\beta_0+\alpha_0\delta_0)\,y+\left(y^2-\tilde{f}_0\right)$$

$$=(\alpha_0+\beta_0 y)(\gamma_0+\delta_0 y)+\left(y^2-\tilde{f}_0\right)$$

$$=\varphi\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)\varphi\left(\gamma+\delta\sqrt{\tilde{f}(T)}\right)$$

Thus φ is a homomorphism.

Next we will show that $\ker \varphi = T\mathcal{O}'_F$. Recall that $\varphi\left(\tilde{f}(T)\right) = y^2$. So

$$\varphi\left(\sum_{i=1}^{\tilde{d}} \tilde{f}_i T^i\right) = y^2 - \tilde{f}_0.$$

So $\varphi(T) = y^2 - \tilde{f}_0$. Hence $T\mathcal{O}'_F \subseteq \ker \varphi$. Now let $s \in \ker \varphi$. So

$$s = \sum_{i=0}^{k_1} a_i T^i + \sqrt{\tilde{f}(T)} \sum_{j=0}^{k_2} b_j T^j.$$

Since $\varphi(s) = y^2 - \tilde{f}_0$, this implies that $a_0 = b_0 = 0$. So

$$s = T\left(\sum_{i=1}^{k_1} a_i T^{i-1} + \sqrt{\tilde{f}(T)} \sum_{j=1}^{k_2} b_j T^{j-1}\right) \in T\mathcal{O}'_F$$

Hence $T\mathcal{O}'_F = \ker \varphi$. Therefore we can conclude that $\mathcal{O}'_F / T\mathcal{O}'_F \cong \mathbb{F}_r[y]/\left(y^2 - \tilde{f}_0\right)$. Since $\mathbb{F}_r[y]/\left(y^2 - \tilde{f}_0\right)$ is a field, it follows that $\mathcal{O}'_F / T\mathcal{O}'_F$ is a field and hence $T\mathcal{O}'_F$ is maximal. Thus we conclude that $T\mathcal{O}'_F$ is prime and so $T\mathcal{O}'_F$ is inert in $\mathcal{O}'_F$.

Case 3: d is even and $\tilde{f}_0$, the constant term of $\tilde{f}(T)$, is a square in $\mathbb{F}_r$

Since $\tilde{f}_0$ is a square in $\mathbb{F}_r$, $\tilde{f}_0 = \delta^2$ for some $\delta \in \mathbb{F}_r$. Let $\mathfrak{m}_1 = \left(T, \sqrt{\tilde{f}\,(T)} - \delta\right)$ and $\mathfrak{m}_2 = \left(T, \sqrt{\tilde{f}\,(T)} + \delta\right)$. Define $\varphi_1 : \mathcal{O}'_F \to \mathbb{F}_r$ by

$$\varphi_1 : \alpha + \beta\sqrt{\tilde{f}\,(T)} \mapsto \alpha_0 + \beta_0 \delta$$

where $\alpha, \beta \in \mathbb{F}_r[T]$ and α_0, β_0 are the constant terms of α and β respectively.

Clearly φ_1 is well-defined. First we will check that φ_1 is a homomorphism. Let

$\alpha, \beta, \gamma, \sigma \in \mathbb{F}_r[T]$. Then

$$\varphi_1\left(\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)+\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)\right)$$

$$=\varphi_1\left((\alpha+\gamma)+(\beta+\sigma)\sqrt{\tilde{f}(T)}\right)$$

$$=\alpha_0+\gamma_0+(\beta_0+\sigma_0)\,\delta$$

$$=\alpha_0+\beta_0\delta+\gamma_0+\sigma_0\delta$$

$$=\varphi_1\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)+\varphi_1\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)$$

And

$$\varphi_1\left(\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)\right)$$

$$=\varphi_1\left((\alpha\gamma)+(\beta\sigma)\,\tilde{f}\,(T)+(\gamma\beta+\alpha\sigma)\sqrt{\tilde{f}(T)}\right)$$

$$=\alpha_0\gamma_0+\beta_0\sigma_0\delta^2+(\gamma_0\beta_0+\alpha_0\sigma_0)\,\delta$$

$$=(\alpha_0+\beta_0\delta)\,(\gamma_0+\sigma_0\delta)$$

$$=\varphi_1\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)\varphi_1\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)$$

Hence φ_1 is a homomorphism.

We claim that $\ker\varphi_1=\mathfrak{m}_1$. We know that $\varphi_1(T)=0$ and since

$$\varphi_1\left(\sqrt{\tilde{f}\,(T)}-\delta\right)=\delta-\delta=0,$$

it follows that $\mathfrak{m}_1 \subseteq \ker \varphi_1$. Now, let $s \in \ker \varphi_1$. So

$$s = \sum_{i=0}^{k_1} a_i T^i + \sqrt{\tilde{f}(T)} \sum_{j=0}^{k_2} b_j T^j.$$

Since $\varphi_1(s) = 0$, it follows that $a_0 = b_0 = 0$. So

$$s = T \left(\sum_{i=1}^{k_1} a_i T^{i-1} + \sqrt{\tilde{f}(T)} \sum_{j=1}^{k_2} b_j T^{j-1} \right) \in \mathfrak{m}_1$$

So $\mathfrak{m}_1 = \ker \varphi_1$. Therefore $\mathcal{O}'_F/\mathfrak{m}_1 \cong \mathbb{F}_r$, so $\mathcal{O}'_F/\mathfrak{m}_1$ is a field. Hence $\mathfrak{m}_1$ is a maximal and thus a prime ideal.

Similarly, we can define $\varphi_2 : \mathcal{O}'_F \to \mathbb{F}_r$ by

$$\varphi_2 : \alpha + \beta \sqrt{\tilde{f}\,(T)} \mapsto \alpha_0 - \beta_0 \delta$$

where $\alpha, \beta \in \mathbb{F}_r[T]$ and α_0, β_0 are the constant terms of α and β respectively.

Clearly φ_2 is well-defined. First we will check that φ_2 is a homomorphism. Let

$\alpha, \beta, \gamma, \sigma \in \mathbb{F}_r[T]$. Then

$$\varphi_2\left(\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)+\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)\right)$$

$$=\varphi_2\left((\alpha+\gamma)+(\beta+\sigma)\sqrt{\tilde{f}(T)}\right)$$

$$=\alpha_0+\gamma_0-(\beta_0+\sigma_0)\,\delta$$

$$=\alpha_0-\beta_0\delta+\gamma_0-\sigma_0\delta$$

$$=\varphi_2\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)+\varphi_2\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)$$

And

$$\varphi_2\left(\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)\right)$$

$$=\varphi_2\left((\alpha\gamma)+(\beta\sigma)\,\tilde{f}\,(T)+(\gamma\beta+\alpha\sigma)\sqrt{\tilde{f}(T)}\right)$$

$$=\alpha_0\gamma_0+\beta_0\sigma_0\delta^2-(\gamma_0\beta_0+\alpha_0\sigma_0)\,\delta$$

$$=(\alpha_0-\beta_0\delta)\,(\gamma_0-\sigma_0\delta)$$

$$=\varphi_2\left(\alpha+\beta\sqrt{\tilde{f}(T)}\right)\varphi_2\left(\gamma+\sigma\sqrt{\tilde{f}(T)}\right)$$

Hence φ_2 is a homomorphism.

We claim that $\ker\varphi_2=\mathfrak{m}_2$. We know that $\varphi_2(T)=0$ and since

$$\varphi_2\left(\sqrt{\tilde{f}\,(T)}+\delta\right)=-\delta+\delta=0,$$

it follows that $\mathfrak{m}_2 \subseteq \ker \varphi_2$. Now,let $s \in \ker \varphi_2$. So

$$s = \sum_{i=0}^{k_1} a_i T^i + \sqrt{\tilde{f}(T)} \sum_{j=0}^{k_2} b_j T^j.$$

Since $\varphi_2(s) = 0$, it follows that $a_0 = b_0 = 0$. So

$$s = T \left(\sum_{i=1}^{k_1} a_i T^{i-1} + \sqrt{\tilde{f}(T)} \sum_{j=1}^{k_2} b_j T^{j-1} \right) \in \mathfrak{m}_2$$

So $\mathfrak{m}_2 = \ker \varphi_2$. Therefore $\mathcal{O}'_F/\mathfrak{m}_2 \cong \mathbb{F}_r$, so $\mathcal{O}'_F/\mathfrak{m}_2$ is a field. Hence $\mathfrak{m}_2$ is a maximal and thus a prime ideal.

Finally, we observe that

$$\mathfrak{m}_1\mathfrak{m}_2 = \left(T^2, T\left(\sqrt{\tilde{f}\,(T)} - \delta\right), T\left(\sqrt{\tilde{f}\,(T)} + \delta\right), \tilde{f}\,(T) - \delta^2 \right)$$

Notice that $\tilde{f}\,(T) - \delta^2 = \tilde{f}\,(T) - \tilde{f}_0$, so it is divisible by T. Therefore it is obvious that $\mathfrak{m}_1\mathfrak{m}_2 \subseteq T\mathcal{O}'_F$. Consider $\left(T\left(\sqrt{\tilde{f}\,(T)} - \delta\right), T\left(\sqrt{\tilde{f}\,(T)} + \delta\right) \right)$, which is contained in $\mathfrak{m}_1\mathfrak{m}_2$. Then the difference of our two generators must be in this ideal and

$$T\left(\sqrt{\tilde{f}\,(T)} - \delta\right) - T\left(\sqrt{\tilde{f}\,(T)} + \delta\right) = 2\delta T$$

Hence

$$T\mathcal{O}'_F \subseteq \left(T\left(\sqrt{\tilde{f}\,(T)} - \delta\right), T\left(\sqrt{\tilde{f}\,(T)} + \delta\right) \right) \subseteq \mathfrak{m}_1\mathfrak{m}_2$$

Thus $T\mathcal{O}'_F = \mathfrak{m}_1\mathfrak{m}_2$. So $T\mathcal{O}'_F$ splits in $\mathcal{O}'_F$.

□

Chapter 3

Valuations

In this chapter, we will explicitly define the valuation that corresponds to P_∞ in X when P_∞ of $\mathbb{P}^1_\infty$ is inert in X.

Let $f(t)$ be a square-free irreducible polynomial in $\mathbb{F}_r[t]$ with degree $\mathbf{d}$. Let $T = \frac{1}{t}$. Define

$$v_\infty : \mathbb{F}_r(t) \rightarrow \mathbb{R} \cup \{\infty\} \quad \text{where} \quad v_\infty(T) = 1$$

We need to extend this to $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$. We will only consider the inert case.

Recall that in the inert case, $f(t)$ has even degree and $\tilde{f}(T) = T^{\mathbf{d}} f(1/T)$ is not a square mod (T). So

$$\tilde{f}(T) = \sum_{i=0}^{\tilde{d}} \tilde{f}_i T^i \quad \text{where } \tilde{f}_0 \text{ is not a square in } \mathbb{F}_r$$

Let $a, b \in \mathbb{F}_r$. Then

$$\begin{aligned}\left(a + b\sqrt{\tilde{f}(T)}\right)\left(a - b\sqrt{\tilde{f}(T)}\right) &= a^2 - b^2 \tilde{f}(T) \\ &= a^2 - b^2 \tilde{f}_0 - b^2 \sum_{i=1}^{\tilde{d}} \tilde{f}_i T^i\end{aligned}$$

We know that

$$v_\infty\left(a^2-b^2\tilde{f}\left(T\right)\right)\geq\min\left\{v_\infty(a^2),v_\infty(b^2\tilde{f}_0),v_\infty\left(b^2\sum_{i=1}^{\tilde{d}}\tilde{f}_iT^i\right)\right\}$$

with equality if $a^2\neq b^2\tilde{f}_0$. However, since $\tilde{f}_0$ is not a square in $\mathbb{F}_r$, $a^2\neq b^2\tilde{f}_0$, thus

$$v_\infty\left(a^2-b^2\tilde{f}\left(T\right)\right)=\min\left\{v_\infty(a^2),v_\infty(b^2\tilde{f}_0),v_\infty\left(b^2\sum_{i=1}^{\tilde{d}}\tilde{f}_iT^i\right)\right\}=0$$

Therefore we can conclude that

$$v_\infty\left(a\pm b\sqrt{\tilde{f}\left(T\right)}\right)=0$$

So we define the valuation in the extension $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$ as

$$v_\infty\left(\sqrt{f(t)}\right)=-\frac{\mathbf{d}}{2}$$

Lemma 10. *Let $\alpha\in\mathbb{F}_r[t][\sqrt{f(t)}]$ where*

$$\alpha=\sum_{i=0}^{k_1}a_it^i+\sum_{j=0}^{k_2}b_jt^j\sqrt{f(t)}$$

Then, in the inert case, assuming some a_i and b_j are not zero,

$$v_\infty\left(\alpha\right)=-\max\left\{k_1,k_2+\frac{\mathbf{d}}{2}\right\}$$

Proof. We have two cases to consider.

Case 1: Assume $k_1 \neq k_2 + \frac{\mathbf{d}}{2}$. Then

$$v_\infty\left(\sum_{i=0}^{k_1} a_i t^i\right) = -k_1$$

and

$$v_\infty\left(\sum_{j=0}^{k_2} b_j t^j \sqrt{f(t)}\right) = -\left(k_2 + \frac{\mathbf{d}}{2}\right)$$

Hence,

$$v_\infty\left(\sum_{i=0}^{k_1} a_i t^i\right) \neq v_\infty\left(\sum_{j=0}^{k_2} b_j t^j \sqrt{f(t)}\right)$$

So,

$$v_\infty(\alpha) = -\max\left\{k_1, k_2 + \frac{\mathbf{d}}{2}\right\}$$

Case 2: Assume $k_1 = k_2 + \frac{\mathbf{d}}{2}$. Then

$$\begin{aligned}\alpha &= \sum_{i=0}^{k_1} a_i t^i + \sum_{j=0}^{k_1-\mathbf{d}/2} b_j t^j \sqrt{f(t)} \\ &= \sum_{i=0}^{k_1} a_i t^i + \sum_{j=0}^{k_1-\mathbf{d}/2} b_j t^{j+\mathbf{d}/2} \sqrt{\tilde{f}(T)}\end{aligned}$$

Define $\{\overline{b_l}\}_{l=0}^{k_1}$ where

$$\overline{b_l} = \begin{cases} 0, & 0 \leq l < \mathbf{d}/2 \\ b_{l-\mathbf{d}/2}, & \mathbf{d}/2 \leq l \leq k_1 \end{cases}$$

Then

$$\alpha = \sum_{i=0}^{k_1}\left(a_i + \overline{b_i}\sqrt{\tilde{f}(T)}\right) t^i$$

But since $v_\infty\left(a_i+\overline{b_i}\sqrt{\tilde{f}\,(T)}\right)=0$ for all i, it follows that

$$v_\infty(\alpha)=-k_1=-k_2-\frac{\mathbf{d}}{2}.$$

□

Chapter 4

Construction of $e(x)$

In this chapter we will construct $e_d(x)$ for our specialized case in a similar way as in the Carlitz module. We will give a formula which allows us to recursively define $e_d(x)$.

Let $f(t)$ be a square-free irreducible polynomial in $\mathbb{F}_r[t]$ with even degree where $\tilde{f}(T) = (T)^{\deg(f(t))} f(1/T)$ is not a square mod (T). Then

$$\sqrt{f(t)} = t^{\frac{\deg(f(t))}{2}} \sqrt{\tilde{f}(T)}$$

Let $d > 0$. Define

$$L(d) = \left\{ \alpha \in \mathbb{F}_r[t]\left[\sqrt{f(t)}\right] : -d < v_\infty(\alpha) \le 0 \right\}$$

Then $\mathbb{F}_r[t]\left[\sqrt{f(t)}\right] = \bigcup_d L(d) \cup \{0\}$. Define

$$e_0(x) = x$$

and for $d > 0$,

$$e_d(x) = x \prod_{\alpha \in L(d)} (x - \alpha)$$

So $\deg(e_d(x)) = |L(d)| + 1$.

4.1 Degree of $e_d(x)$

Proposition 11. *Let* $\mathcal{D} = 2d - \frac{\deg(f(t))}{2}$*. Then*

$$\deg\left(e_d(x)\right) = \begin{cases} r^d & d \leq \frac{\deg(f(t))}{2} \\ r^{\mathcal{D}} & d > \frac{\deg(f(t))}{2} \end{cases}$$

Proof. Suppose that $d \leq \frac{\deg(f(t))}{2}$. We know that

$$v_\infty\left(\sqrt{f(t)}\right) = -\frac{\deg(f(t))}{2} \leq -d$$

So $\sqrt{f(t)} \notin L(d)$. Then for all $\alpha \in L(d)$,

$$\alpha = \sum_{i=0}^{d-1} a_i t^i$$

Therefore, since we are working over $\mathbb{F}_r$, $|L(d)| = r^d - 1$. So, in this case,

$$\deg(e_d(x)) = |L(d)| + 1 = r^d.$$

Now suppose that $d > \frac{\deg(f(t))}{2}$. Then

$$v_\infty\left(\sqrt{f(t)}\right) = -\frac{\deg(f(t))}{2} > -d$$

Let $\alpha \in L(d)$. Then α can have one of the following forms

$$\alpha_1 = \sum_{i=0}^{k_1} a_i t^i$$

$$\alpha_2 = \sum_{i=0}^{k_2} b_i t^i \sqrt{f(t)}$$

$$\alpha_3 = \sum_{i=0}^{k_1} a_i t^i + \sum_{j=0}^{k_2} b_j t^j \sqrt{f(t)}$$

If $\alpha = \alpha_1$, then $v_\infty(\alpha) = -k_1$.

If $\alpha = \alpha_2$, then $v_\infty(\alpha) = -k_2 + \frac{\deg(f(t))}{2}$.

Finally, if $\alpha = \alpha_3$, then by Lemma 10, we know that

$$v_\infty(\alpha) = -\max\left\{k_1, k_2 + \frac{\deg(f(t))}{2}\right\}$$

So $k_1 < d$ and $k_2 + \frac{\deg(f(t))}{2} < d$. Hence

$$|L(d)| = r^d \left(r^{d-\frac{\deg(f(t))}{2}}\right) - 1 = r^{2d-\frac{\deg(f(t))}{2}} - 1$$

Thus, in this case, $\deg(e_d(x)) = r^{\mathcal{D}}$ where $\mathcal{D} = 2d - \frac{\deg(f(t))}{2}$. □

4.2 Recursively Defining $e_d(x)$

The following lemma is important in the construction of our final proposition.

Lemma 12. *$e_d(x)$ is an additive polynomial.*

Proof. We know that the zeros of $e_d(x)$ are all the elements of $L(d) \cup \{0\}$. Also, $e_d(x) \in \mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$. Let $w \in \mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$. If $w \in L(d) \cup \{0\}$, then $e_d(x + w) = e_d(x)$. So assume $y \in \mathbb{F}_r(t)\left(\sqrt{f(t)}\right) \setminus (L(d) \cup \{0\})$. Define

$$H(x) = e_d(x+y) - e_d(x) - e_d(y)$$

So $\deg(H(x)) < \deg(e_d(x))$ since the leading terms cancel in $H(x)$. Also, for $w \in L(d) \cup \{0\}$,

$$\begin{aligned} H(w) &= e_d(w+y) - e_d(w) - e_d(y) \\ &= e_d(y) - e_d(y) \\ &= 0 \end{aligned}$$

Therefore, since $|L(d)| + 1 = \deg(e_d) > \deg(H)$, it follows that $H(x) \equiv 0$.

Now let z be an arbitrary indeterminate and define

$$H_1(z) = e_d(x+z) - e_d(x) - e_d(z)$$

So $H_1(z) \in \mathbb{F}_r(t)\left(\sqrt{f(t)}\right)[x,z]$. Then, for all $\alpha \in \mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$, we conclude that $H_1(\alpha) = 0$. Since $\mathbb{F}_r(t)\left(\sqrt{f(t)}\right)$ is infinite, $H_1(z) \equiv 0$. Hence $e_d(x)$ is additive. $\square$

Finally, we will define the following notation before stating our recursive formula for $e_d(x)$. Let $\delta := \sqrt{\tilde{f}(T)}$. Define

$$D_d := e_d\left(t^d\right) \quad \text{and} \quad D'_d := e_d\left(t^d\delta\right)$$

Since $e_d(x)$ is an additive polynomial, we are able to generate all polynomials of valuation d. Note if $d \leq \frac{\deg(f(x))}{2}$, then we are in the case of the Carlitz module described in Chapter 1. Therefore all properties of $e_d(x)$, which hold for Carlitz, will hold here. So, we will focus on the case $d > \frac{\deg(f(x))}{2}$. We have the following proposition on how to recursively define $e_d(x)$.

Proposition 13. *If* $d > \frac{\deg(f(t))}{2}$*, then*

$$e_d(x) = e_{d-1}^{r^2}(x) + B_{d-1} \cdot e_{d-1}^{r}(x) + C_{d-1} \cdot e_{d-1}(x)$$

where

$$B_{d-1} := \frac{-\left(D_{d-1}^{r^2-1} - \left(D'_{d-1}\right)^{r^2-1}\right)}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}}$$

and

$$C_{d-1} := \frac{D_{d-1}^{r^2-1}\left(D'_{d-1}\right)^{r-1} - D_{d-1}^{r-1}\left(D'_{d-1}\right)^{r^2-1}}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}}$$

Proof. Let $\beta = \frac{\deg(f(t))}{2}$ and assume $d > \beta$. We want to show that

$$e_d(x) = e_{d-1}^{r^2}(x) + B \cdot e_{d-1}^{r}(x) + C \cdot e_{d-1}(x)$$

It is enough to show that both the left and right hand side are monic, have the same degree and the same set of roots. We know by construction that $e_d(x)$ and $e_{d-1}(x)$ are monic. Also, since $d > \beta$, we have that $\deg(e_d(x)) = r^{2d-\beta}$. If $d = \beta + 1$, then $\deg(e_{d-1}(x)) = r^{d-1}$. And so

$$\begin{aligned}
\deg\left((e_{d-1}(x))^{r^2}\right) &= r^{d-1}r^2 \\
&= r^{d+1} \\
&= r^{\beta+2} \\
&= r^{2(\beta+1)-\beta} \\
&= r^{2d-\beta}
\end{aligned}$$

If $d > \beta + 1$, then $\deg(e_{d-1}(x)) = r^{2(d-1)-\beta}$ and hence

$$\begin{aligned}
\deg\left((e_{d-1}(x))^{r^2}\right) &= r^{2d-2-\beta}r^2 \\
&= r^{2d-\beta}
\end{aligned}$$

Also,

$$\deg\left(e_{d-1}^r(x)\right) = r^d,$$

and for $d > \beta$,

$$r^{2d\beta} > r^d > r^{d-1}$$

Therefore both the left and the right hand side are monic and have the same degree. It remains to show that they have the same zeros (i.e. $L(d) \cup \{0\}$). Clearly, 0 is a root of both, so let $\alpha \in L(d)$. If $\alpha \in L(d-1)$, $e_{d-1}(\alpha) = 0$, so clearly it is a root of the right hand side of our equation. Now assume $\alpha \in L(d) \setminus L(d-1)$. Then $\alpha = \zeta h$ where $v_\infty(h) = -(d-1)$ and $\zeta \in \mathbb{F}_r^*$. So $\zeta^r = \zeta$. And

$$h = \sum_{i=0}^{d-1} a_i t^i + \sum_{j=0}^{d-1-\beta} b_j t^{j+\beta} \sqrt{\tilde{f}(T)}$$

Observe that

$$e_{d-1}(h) = a_{d-1} e_{d-1}(t^{d-1}) + b_{d-1} e_{d-1}(t^{d-1}\delta).$$

Therefore it suffices to show that the right hand side is zero for $h = t^{d-1}$ and $h = t^{d-1}\delta$. So

$$(e_{d-1}(\zeta h))^{r^2} + B_{d-1} \cdot (e_{d-1}(\zeta h))^r + C_{d-1} \cdot e_{d-1}(\zeta h)$$

$$= \zeta^{r^2} \left(D_{d-1} + D'_{d-1}\right)^{r^2} + B_{d-1} \cdot \zeta^r \left(D_{d-1} + D'_{d-1}\right)^r + C_{d-1} \cdot \zeta \left(D_{d-1} + D'_{d-1}\right)$$

$$= \zeta \left(D_{d-1}\right)^{r^2} + \left(\frac{-\left(D_{d-1}^{r^2-1} - \left(D'_{d-1}\right)^{r^2-1}\right)}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}}\right) \zeta \left(D_{d-1}\right)^r + \left(\frac{D_{d-1}^{r^2-1}\left(D'_{d-1}\right)^{r-1} - D_{d-1}^{r-1}\left(D'_{d-1}\right)^{r^2-1}}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}}\right) \zeta \left(D_{d-1}\right)$$

$$+\zeta \left(D'_{d-1}\right)^{r^2} + \left(\frac{-\left(D_{d-1}^{r^2-1} - \left(D'_{d-1}\right)^{r^2-1}\right)}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}}\right) \zeta \left(D'_{d-1}\right)^r + \left(\frac{D_{d-1}^{r^2-1}\left(D'_{d-1}\right)^{r-1} - D_{d-1}^{r-1}\left(D'_{d-1}\right)^{r^2-1}}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}}\right) \zeta \left(D'_{d-1}\right)$$

$$= \zeta \left(\left(D_{d-1}\right)^{r^2} + \frac{-\left(D_{d-1}\right)^{r^2+r-1} - \left(D_{d-1}\right)^r \left(D'_{d-1}\right)^{r^2-1}}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}} + \frac{D_{d-1}^{r^2}\left(D'_{d-1}\right)^{r-1} - D_{d-1}^{r}\left(D'_{d-1}\right)^{r^2-1}}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}} \right)$$

$$+\zeta \left(\left(D'_{d-1}\right)^{r^2} + \frac{-\left(D_{d-1}^{r^2-1}\left(D'_{d-1}\right)^{r} - \left(D'_{d-1}\right)^{r^2+r-1}\right)}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}} + \frac{D_{d-1}^{r^2-1}\left(D'_{d-1}\right)^{r} - D_{d-1}^{r-1}\left(D'_{d-1}\right)^{r^2}}{D_{d-1}^{r-1} - \left(D'_{d-1}\right)^{r-1}} \right)$$

$$= \zeta(0) + \zeta(0)$$
$$= 0$$

So they have the same zeros. Thus the equation holds. □

Chapter 5

Future Work

First, we have shown that we can recursively compute the exponential function, $e_d(x)$, in terms of $e_{d-1}(x)$, D_{d-1} and D'_{d-1} when $d > \frac{\deg(f(t))}{2}$. This formula is nice, however, we were unable to find a way to express the coefficient of each term of $e_d(x)$ similar to how was described in Chapter 1.

Second, it is important for the reader to keep in mind that the Drinfeld module we constructed is only one of the possible rank one dimension two Drinfeld modules. In our paper, we chose to use the standard lattice. However, there are many other ways to choose a lattice. The number of non-isomorphic Drinfeld modules equals the class number of the ring we are working over.

This leads us to alternate directions for further research. One direction would be to construct a rank two dimension one Drinfeld module. In this case, we might take $\mathbb{A} = \mathbb{F}_r[t]$ and $L = \mathbb{F}_r[t]\left[\sqrt{f(t)}\right]$, where $f(t)$ is chosen appropriately. Another approach would be to construct a rank two dimension two Drinfeld module. In this case we may take $\mathbb{A} = \mathbb{F}_r[t]\left[\sqrt{f(t)}\right]$ and L to be an extension of $\mathbb{A}$ of degree 2, where, again, $f(t)$ is chosen appropriately. We could even explore more complicated examples by choosing an ideal I of $\mathbb{A}$ which is not in the trivial class group and take $L = I$. Moreover, the ideal I we choose could be in the function field of $\mathbb{A}$, which would increase the dimension of our Drinfeld module. These are just a few possibilities for further work.

Bibliography

[1] L. Carlitz. On certain functions connected with polynomials in a galois field. *Duke Math. J.*, 1:137–168, 1935.

[2] M.I. Rosen D. Goss, D.R. Hayes. *The Arithmetic of Function Fields*. Walter de Gruyter, 1992.

[3] D. Goss. von-staudt for $f_q[t]$. *Duke Math. J.*, 45:885–910, 1978.

[4] D. Goss. Modular forms for $f_r[t]$. *J. reine angew. Math.*, 317:16–39, 1980.

[5] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer-Verlag Berlin Heidelberg, 1998.

[6] O. Ore. On a special class of polynomials. *Trans. Amer. Math So.*, 35:559–584, 1933.

[7] M. Rosen. *Number Theory in Function Fields*. Springer-Verlag, 2002.