University of Zurich
Institute of Mathematics

Master Thesis

Eisenstein Polynomials over Holomorphy Rings

Author:
Edoardo Dotti

Supervisor:
Joachim Rosenthal
Co-supervisor:
Giacomo Micheli

FS 2015

Contents

Introduction

In the last decade, it has been of interest the computation of the natural densities of both monic Eisenstein polynomials and non-monic Eisenstein polynomials with coefficients over $\mathbb{Z}$ and of degree at most d. For this we first recall that a subset $A \subseteq \mathbb{Z}^n$ is said to have density δ if

$$\delta = \lim_{B\to\infty} \frac{|A \cap [-B, B[^n|}{(2B)^n}.$$

As was first proved by Dubickas in [3], the natural density of monic Eisenstein polynomials over $\mathbb{Z}$ of fixed degree d is

$$1 - \prod_{p \text{ prime}} \left(1 - \frac{p-1}{p^{d+1}}\right). \tag{1}$$

Heyman and Shparlinski extended the results of Dubickas to non-monic Eisenstein polynomials computing also the error term of the densities [4, Theorem 1, Theorem 2], obtaining for the density of the non-monic case

$$1 - \prod_{p \text{ prime}} \left(1 - \frac{(p-1)^2}{p^{d+2}}\right). \tag{2}$$

The main aspect of this thesis is the establishing of the function field analogue of these results, when the coefficients of the polynomials are taken in an integrally closed subring of a function field of a curve (i.e. a holomorphy ring) over a finite field.

In the first chapter of this thesis we develop all the theory about algebraic function fields that we need in order to understand the setting that we are dealing with and to explicitly compute the densities. All the theory concerning algebraic function fields is taken from [7].
In the second chapter we explicitly compute the densities of Eisenstein polynomials and monic Eisenstein polynomials. These computations come directly from the paper written with Giacomo Micheli, see [2].
In the last chapter, as completion, we develop the theory a little more, talking about algebraic extensions of function fields and totally ramified places in order to conclude by giving a function field analogue of the work of Keith Conrad in [1], finding a link between Eisenstein polynomials over function fields and totally ramified places.

Chapter 1

Basic Theory of Algebraic Function Fields

1.1 Algebraic Function Fields

In this chapter we give the definitions and state the results that will be needed for the rest of the thesis.

We start by giving the definition of an algebraic function field.

Definition 1.1.1. Let K denotes a field. An extension field $F \supseteq K$ is said to be an *algebraic function field* of one variable over K if F is a finite algebraic extension of $K(z)$, for some $z \in F$ trascendental over K.

From now on we just say function field for brevity.
We also define $\tilde{K} := \{z \in F \mid z \text{ is algebraic over } K\}$, which is a subfield of F, called the *field of constants*. F is a function field also for $\tilde{K}$. Moreover we have $K \subseteq \tilde{K} \subsetneq F$, and if $K = \tilde{K}$ we say that K is the *full constant field* of F.

Definition 1.1.2. A ring $\mathcal{O}$ is said to be a *valuation ring* of the function field F if

i) $K \subsetneq \mathcal{O} \subsetneq F$,

ii) for every $z \in F$ we have that $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

A valuation ring $\mathcal{O}$ is a local ring having unique maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^\times$, where $\mathcal{O}^\times$ denotes the set of units of $\mathcal{O}$. P is called a *place* of the function field F and we define the set of all places of F by $\mathbb{P}_F := \{P \mid P \text{ is a place of } F\}$.
The maximal ideal P is also principal, and following from this fact, every element $t \in P$ such that $P = t\mathcal{O}$ is called *prime element* for P. More precisely, $\mathcal{O}$ is a principal ideal domain. Moreover, when $P = t\mathcal{O}$, we have that every $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$ and some $u \in \mathcal{O}^\times$.

We also have that a valuation ring $\mathcal{O}$ is uniquely determined by its maximal ideal P, hence we can set $\mathcal{O}_P := \mathcal{O}$ to be the valuation ring of the place P.
Finally notice that the field of constant $\tilde{K}$ is contained in every valuation ring $\mathcal{O} \subseteq F$.

We now give the definition of discrete valuation, which gives us another useful way to describe places and valuation rings.

Definition 1.1.3. Let F be a function field. A function $v : F \to \mathbb{Z} \cup \{\infty\}$ is called a *discrete valuation* of F if it satisfies the following proprieties:

i) $v(x) = \infty \Leftrightarrow x = 0$,

ii) $v(x \cdot y) = v(x) + v(y)$ for all $x, y \in F$,

iii) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in F$,

iv) there exists an element $z \in F$ such that $v(z) = 1$,

v) $v(x) = 0$ for all $0 \neq x \in K$.

Notice also that a discrete valuation of F fulfils the strict triangle inequality, that is to say: $v(x + y) = \min\{v(x), v(y)\}$ for all $x, y \in F$ with $v(x) \neq v(y)$.

Definition 1.1.4. Let F be a function field. Let $P \in \mathbb{P}_F$ be a place of F. We can associate to P the well defined map $v_P : F \to \mathbb{Z} \cup \{\infty\}$ defined in this way: let t be a prime element for P. For an element $0 \neq z \in F$ consider the unique representation $z = t^n u$. Now define $v_P(z) := n$ and $v_P(0) := \infty$.

The map v_P is a discrete valuation and we also have

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\},$$
$$\mathcal{O}_P^\times = \{z \in F \mid v_P(z) = 0\},$$
$$P = \{z \in F \mid v_P(z) > 0\}.$$

Moreover an element $z \in F$ is a prime element for a place P if and only if $v_P(z) = 1$.

Definition 1.1.5. Let $P \in \mathbb{P}_F$ be a place of a function field F.

i) $F_P := \mathcal{O}_P / P$ is called the *residue class field* of P.

ii) $\deg(P) := [F_P : K]$ is called the *degree* of P. A place of degree one is also called a rational place of F.

Notice that the degree of a place is always finite. More precisely for a place P of F and $0 \neq z \in P$ we have that $\deg(P) \leq [F : K(z)] < \infty$. As a corollary of such a statement one can show that the field $\tilde{K}$ of constant of F is a finite field extension of K.

Of course, since we are dealing with places of function fields, it is natural to ask whether they actually exist or not.

Theorem 1.1.6. *Let F be a function field and R a subring of F such that $K \subseteq R \subseteq F$. Assume that $\{0\} \neq I \subsetneq R$ is a proper ideal of R. It follows that there is a place $P \in \mathbb{P}_F$ with $I \subseteq P$ and $R \subseteq \mathcal{O}_P$.*

Proof. For the proof we refer to [7, Theorem 1.1.19]. □

Next we give the definition of zeros and poles, which will play an important role for defining the Riemann-Roch Space.

Definition 1.1.7. Let F be a function field. Let $P \in \mathbb{P}_F$ be a place of F and let $z \in F$. We say that P is a zero of z if $v_P(z) > 0$, conversely if $v_P(z) < 0$ we say that P is a pole of z. Moreover, if $v_P(z) = m > 0$ we say that P is a zero of z of order m, and if $v_P(z) = -m < 0$ we say that P is a pole of z of order m.

Following this definition, as a corollary of the Theorem 1.1.6, we obtain that for a function field F, an element $z \in F$ trascendental over K has at least one zero and one pole. In particular we have that the set of places $\mathbb{P}_F$ is different from the empty set.

More precisely, every function field has infinitely many places. Moreover, every non-zero element $z \in F$ has finitely many zeros and poles. This is a consequence of the independence of valuations, in particular of the *Weak Approximation Theorem* [7, Theorem 1.3.1].

1.2 Divisors

As we have seen before, the field of constants $\tilde{K}$ of a function field is an extension field of K, and also that F can be regarded as a function field over $\tilde{K}$. Hence from now on we can make the following assumption:

Let F be a function field of one variable having full constant field K.

Definition 1.2.1. A *divisor* of a function field F is an element of $\mathrm{Div}(F)$, where $\mathrm{Div}(F)$ denotes the free abelian group generated by the places of F. In other words

$$\mathrm{Div}(F) := \left\{ \sum_{P \in \mathbb{P}_F} n_P P \mid n_P \in \mathbb{Z} \text{ and } n_P = 0 \text{ for all but finitely many places} \right\}.$$

For a convenient writing we can define also the *support* of D as $\mathrm{supp}(D) := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$, and so, considering a finite set $S \subseteq \mathbb{P}_F$ with $S \supseteq \mathrm{supp}(D)$, we can write a divisor as

$$D = \sum_{P \in S} n_P P.$$

Concerning the structure of the group we have that the neutral element of $\mathrm{Div}(F)$ is the divisor $0 := \sum_{P \in \mathbb{P}_F} n_P P$, with all $n_P = 0$. Moreover the sum is made coefficientwise, that is to say: let $D = \sum_{P \in \mathbb{P}_F} n_P P$ and $D' = \sum_{P \in \mathbb{P}_F} n'_P P$, then $D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P$.

Consider now a place $Q \in \mathbb{P}_F$ and a divisor $D = \sum_{P \in \mathbb{P}_F} n_P P$. We define $v_Q(D) := n_Q$. We can now rewrite a divisor and the definition of support in the following way:

$$\mathrm{supp}(D) = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\} \text{ and } D = \sum_{P \in \mathrm{supp}(D)} v_P(D) P.$$

We now define a *partial ordering* in the group of divisors, which will be important later, in Chapter 2. For this, we first say that a divisor $D \in \mathrm{Div}(F)$ is positive (denoted by $D \geq 0$) if $v_P(D) \geq 0$ for all $P \in \mathbb{P}_F$. Now the partial ordering on $\mathrm{Div}(F)$ can be defined as follow

$$D \leq D' \overset{\text{def}}{\iff} D' - D \geq 0.$$

This is equivalent to say that $D \leq D'$ if and only if $v_P(D) \leq v_P(D')$ for all $P \in \mathbb{P}_F$. We can also define the degree of a divisor through $\deg(D) := \sum_{P \in \mathbb{P}_F} v_P(D) \deg(P)$. Notice that the map $\deg : \mathrm{Div}(F) \to \mathbb{Z}$ is a ring homomorphism.

We now come to the next definitions.

Definition 1.2.2. Let F be a function field. Consider an element $x \in F,\ x \neq 0$. Let Z be the set of zeros of x in $\mathbb{P}_F$ and N be the set of poles of x. We define

$$(x)_0 := \sum_{P \in Z} v_P(x) P, \text{ called the zero divisor of x,}$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x)) P, \text{ called the pole divisor of x,}$$

$$(x) := (x)_0 - (x)_\infty, \text{ the principal divisor of x.}$$

This definition makes sense since we have seen that every non-zero element $x \in F$ has finitely many zeros and poles.
Notice also that both $(x)_0$ and $(x)_\infty$ are positive and that $(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P$.

The set of principal divisors forms a subgroup, more precisely we define

Definition 1.2.3.

i) $\mathrm{Princ}(F) := \{(x) \mid x \in F,\ x \neq 0\}$, the group of principal divisors,

ii) $\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F)$ is called the divisor class group of F.

Let $D \in \mathrm{Div}(F)$, then the divisor class of D, written $[D]$, is the corresponding element in $\mathrm{Cl}(F)$. We can find an equivalence relation between two divisors D and D' in $\mathrm{Div}(F)$, which is: D is equivalent to D' if and only if $[D] = [D']$, meaning that $D = D' + (x)$, for some $0 \neq x \in F$.

1.3 The Riemann-Roch Space

Consider a function field F over K.

Definition 1.3.1. Let $D \in \mathrm{Div}(F)$. The *Riemann-Roch space* associated to D is defined as

$$\mathcal{L}(D) := \{x \in F \mid (x) + D \geq 0\} \cup \{0\}.$$

We can interpret this space as follows:
let $D = \sum_{i=1}^{s} n_i P_i - \sum_{j=1}^{t} m_j Q_j$, with n_i and m_j both larger than zero for all i and j. Then $\mathcal{L}(D)$ consists of all elements $x \in F$ for which hold

- x has zeros of order larger or equal than m_j at Q_j, for $j = 1, \ldots, t$,
- x may have poles only at the places $P_1, \ldots, P_s$, with the order of the pole at P_i bounded by n_i, $i = 1, \ldots, s$.

The Riemann-Roch space $\mathcal{L}(D)$ for a divisor $D \in \mathrm{Div}(F)$ is a K-vector space. We denote its dimension by $\ell(D) := \dim_K(\mathcal{L}(D))$ and call it *the dimension of the divisor D*. For any $D \in \mathrm{Div}(F)$ we have that $\ell(D) < \infty$. More precisely, for a divisor $D \in \mathrm{Div}(F)$ with $D \geq 0$ we get that $\ell(D) \leq \deg(D) + 1$. In addition for any two divisors D and D' with $D \leq D'$ we have that $\mathcal{L}(D) \subseteq \mathcal{L}(D')$ and also

$$\dim_K(\mathcal{L}(D')/\mathcal{L}(D)) = \ell(D') - \ell(D) \leq \deg(D') - \deg(D).$$

We have also that $\mathcal{L}(D) \neq \{0\}$ if and only if there exists a divisor $D' \geq 0$ equivalent to D. Moreover if D and D' are two equivalent divisors, it follows that $\mathcal{L}(D)$ and $\mathcal{L}(D')$ are isomorphic as K-vector spaces.
Furthermore is useful to notice that $\mathcal{L}(0) = K$ and that if $D < 0$, then $\mathcal{L}(D) = \{0\}$.

Remark 1.3.2. Observe that over a finite field with q elements $\mathbb{F}_q$ we have that $\mathcal{L}(D)$ is finite. More precisely

$$\mid \mathcal{L}(D) \mid = q^{\ell(D)}.$$

We state now an important theorem about principal divisors, which essentially tells us that any element $0 \neq x \in F$ has many zeros as poles when those ore counted properly.

Theorem 1.3.3. *All principal divisors have degree zero. More precisely*

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)].$$

Proof. For the proof of this theorem, we refer to [7, Theorem 1.4.11]. □

Now we turn our attention to $\ell(D)$ for $D \in \mathrm{Div}(F)$. The question is which integer values can this dimension have. As we have seen before for a positive divisor $D \in \mathrm{Div}(F)$ we have that $\ell(D) \leq \deg(D) + 1$. But actually we can give a better bound independent of the divisor D which rely only on the function field. In fact there exists a constant ε such that for any divisor $D \in \mathrm{Div}(F)$

$$\deg(D) - \ell(D) \leq \varepsilon.$$

This bound allows us to define an invariant of the function field. This definition will lead us to the Riemann's Theorem, which will be used often in Chapter 2.

Definition 1.3.4. Let F be a function field. The non-negative integer

$$g := \max\{\deg(D) - \ell(D) + 1 \mid D \in \mathrm{Div}(F)\}$$

denotes the genus of F.

Theorem 1.3.5. ***(Riemann's Theorem)***
Let F be a function field of genus g. Then

i) $\ell(D) \geq \deg(D) + 1 - g$, *for all* $D \in \mathrm{Div}(F)$,

ii) there exists an integer β such that

$$\ell(D) = \deg(D) + 1 - g$$

whenever $\deg(D) \geq \beta$, *where β depends only on the function field F.*

We conclude this section by taking a quick look at the *Riemann-Roch Theorem*. The proof and the theory needed in order to obtain this result can be found throughout section 1.5 of [7].

Theorem 1.3.6. ***(Riemann-Roch Theorem)***
Let F be a function field of genus g. Then for any divisor $D \in \mathrm{Div}(F)$ we have

$$\ell(D) = \deg(D) + 1 - g + \ell(W - D),$$

where W denotes a canonical divisor of F.

As a consequence of this theorem, we can now be more precise in choosing the constant β of the Riemann's Theorem. Indeed we now have that

$$\ell(D) = \deg(D) + 1 - g$$

for any divisor $D \in \mathrm{Div}(F)$ with $\deg(D) \geq 2g - 1$.

1.4 Holomorphy Rings

As in the previous sections, let F denotes a function field. Here we treat subrings of function fields, in particular we deal with holomorphy rings. With this we complete the base setting which is needed for the later chapters.

Definition 1.4.1. A set R with $K \subseteq R \subseteq F$ is a subring of F if R is a ring and R is not a field.

As an example one can consider the valuation ring $R = \mathcal{O}_P$ for some place $P \in \mathbb{P}_F$.

Definition 1.4.2. An holomorpy ring is a ring $R \subseteq F$ of the form $R = \mathcal{O}_S$ where

$$\mathcal{O}_S := \{z \in F \mid v_P(z) \geq 0 \text{ for all } P \in S\}$$

for some $S \subsetneq \mathbb{P}_F$, S not the empty set.

Every holomorphy ring is a subring of F. Of course every valuation ring $\mathcal{O}_P$ is a holomorphy ring, just take $S = \{P\}$ and get $\mathcal{O}_P = \mathcal{O}_S$. Moreover for any $P \in \mathbb{P}_F$ and $\emptyset \neq S \subsetneq \mathbb{P}_F$ we have that $\mathcal{O}_S \subseteq \mathcal{O}_P$ if and only if $P \in S$. Also $\mathcal{O}_S = \mathcal{O}_T$ if and only if $S = T$.

As an example one should consider the rational function field $K(x)$ and the holomorphy ring $K[x]$. Namely

$$K[x] = \bigcap_{P \neq P_\infty} \mathcal{O}_P,$$

where P_∞ denotes the only pole of x in $K(x)$.

Now we want to know some proprieties of the holomorpy rings. For this we start with some definitions.

Definition 1.4.3. Consider a subring $R \subseteq F$.

i) An element $z \in F$ is called integral over R if there exists a monic polynomial

$$f(T) := T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in R[T]$$

such that $f(z) = 0$. This type of equation is called *an integral equation* for z over R.

ii) The *integral closure* of R in F is the set

$$\mathrm{ic}_F(R) := \{z \in F \mid z \text{ is integral over } R\}.$$

iii) R is called integrally closed if $\mathrm{ic}_{\mathrm{Quot}(F)}(R) = R$, where $\mathrm{Quot}(F) \subseteq F$ denotes the quotient field of R. This means that R is called integrally closed if all elements $z \in R$ integral over R already lie in R.

Following this definitions we have that an holomoprhy ring $\mathcal{O}_S$ is integrally closed and its quotient field is F itself. Moreover if we define the set $\mathrm{Sub}(R) = \{P \in \mathbb{P}_F \mid R \subseteq \mathcal{O}_P\}$, we have the following:

- $\emptyset \neq \mathrm{Sub}(R) \subsetneq \mathbb{P}_F$,
- $\mathrm{ic}_F(R) = \mathcal{O}_{\mathrm{Sub}(R)}$. Also $\mathrm{ic}_F(R)$ is an integrally closed subring of F having as quotient field F itself.

We can now deduce that a subring R of F with quotient field F is a holomorphy ring if and only if R is integrally closed.

We conclude this section by stating a useful fact about maximal ideals of holomorphy rings.

Proposition 1.4.4. *There is a one-to-one correspondence between the places in $S \subsetneq \mathbb{P}_F$ and the maximal ideals of the holomorphy ring $\mathcal{O}_S$. This correspondence is given by*

$$P \longrightarrow P \cap \mathcal{O}_S =: P_{\mathcal{O}_S}.$$

Moreover, as a generalization of the fact that any valuation ring is a principal ideal domain, we have that for any non-empty and finite subset of places $S \subsetneq \mathbb{P}_F$ the correspondent holomorphy ring $\mathcal{O}_S$ is a principal ideal domain.

Additionally, for any non-empty proper subset of places $S \subsetneq \mathbb{P}_F$, a holomorphy ring is a Dedekind domain. More precisely, is important to us that any prime ideal in a holomorphy ring is also a maximal ideal.

Concerning this result, here we state two lemmas which we prove using only theory coming from [7]. More advanced proofs can also be found.

Lemma 1.4.5. *Let F be a function field and $\mathcal{O}_S$ a holomorphy ring of F. Let $\mathfrak{p} \subseteq \mathcal{O}_S$ be a prime ideal but not maximal. Then there exists a finite number of places $\{P_1, \dots, P_n\} \subseteq \mathbb{P}_F$ such that $\mathfrak{p}$ is prime but not maximal in $\mathcal{O}_{\widehat{S}}$ with $\widehat{S} = \{P_1, \dots, P_n\}^c \supseteq S$.*

Proof. Suppose by contradiction that any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_S$ is maximal in any $\mathcal{O}_{\widehat{S}}$ with $\widehat{S}^c$ finite. Consider an element $x \in \mathcal{O}_S$. Since any element of a function field has finitely many poles, it follows that $x \in \mathcal{O}_{\widehat{S}}$ for some $\widehat{S}$. Moreover, due to the fact that $\mathfrak{p} \subseteq \mathcal{O}_S$ is maximal in any $\mathcal{O}_{\widehat{S}}$ with $\widehat{S}^c$ finite, we have that $x \cdot y = 1 \mod \mathfrak{p} \cap \mathcal{O}_{\widehat{S}}$ for some y. This also imply that $x \cdot y = 1 \mod \mathfrak{p}$, since $\mathfrak{p} \supset \mathfrak{p} \cap \mathcal{O}_{\widehat{S}}$. We deduce that x is invertible in $\mathcal{O}_S/\mathfrak{p}$. Since x was chosen arbitrarily, we get that $\mathcal{O}_S/\mathfrak{p}$ is a field, giving us the maximality for $\mathfrak{p}$ and contradicting the assumption of the lemma. □

Lemma 1.4.6. *Let F be a function field and $\mathcal{O}_{\widehat{S}}$ a holomorphy ring of F with $\widehat{S}$ having finite complement. Then any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{\widehat{S}}$ is maximal.*

Proof. By exercise 3.2 of [7] we get that there exists an element $x \in F$ such that the extension $F : K(x)$ is separable and x has poles exactly at $\widehat{S}^c$, which means that x actually lies in $\mathcal{O}_{\widehat{S}}$. Consider now the holomorphy ring $K[x]$, we have

$$\mathrm{ic}_F(K[x]) = \bigcap_{P \in \mathbb{P}_F : K[x] \subseteq \mathcal{O}_P} \mathcal{O}_P = \bigcap_{P \in \mathbb{P}_F : x \in \mathcal{O}_P} \mathcal{O}_P = \bigcap_{P \in \widehat{S}} \mathcal{O}_P = \mathcal{O}_{\widehat{S}}.$$

Since $K[x]$ is a principal ideal domain, we can apply part c) of Theorem 3.3.4 of [7], which tells us that there exists a basis $\{u_1, \dots, u_n\}$ for F, where n is the finite degree of the extension, with the following propriety

$$\mathcal{O}_{\widehat{S}} = \sum_{i=1}^{n} K[x] u_i.$$

We now quotient both sides by $\mathfrak{p}$ and obtain that $\mathcal{O}_{\widehat{S}}/\mathfrak{p}$, which is a integral domain since $\mathfrak{p}$ is prime, can be written as a finite dimensional vector space. Hence $\mathcal{O}_{\widehat{S}}/\mathfrak{p}$ is a finite integral domain and thus a field. From this it follows that $\mathfrak{p}$ must be maximal. □

Lemma 1.4.6 shows that the consequence of Lemma 1.4.5 is always not true. Consequently the assumption of Lemma 1.4.5 must be false and so we obtain that in a holomorphy ring of a function field every prime ideal is also maximal.

Chapter 2

Density of Eisenstein Polynomials

In this chapter we are interested in computing the densities of monic and non-monic Eisenstein polynomials of a fix degree d with coefficient lying in a holomorphy ring of a function field over a finite field. To do this we apply a strategy similar to the one used in [6]. The formulas we obtain for the densities are analogous to the ones over the integers described in the introduction. All the computations come directly from the paper [2], written jointly with Giacomo Micheli.
We start with the definition of Eisenstein polynomial.

Definition 2.0.7. Let R be an integral domain. A polynomial $f(X) = \sum_{i=0}^{n} a_i x^i \in R[X]$ is said to be Eisenstein if there exists a prime ideal $\mathfrak{p} \subseteq R$ for which

- $a_i \in \mathfrak{p}$ for all $i \in \{0, \dots, n-1\}$,
- $a_0 \notin \mathfrak{p}^2$,
- $a_n \notin \mathfrak{p}$.

Notice that it makes sense to talk about Eisenstein polynomials over holomorphy rings since those are integral domains, as we have seen in Chapter 1.

Let q be a prime power and $\mathbb{F}_q$ be the finite field of order q. Let F be an algebraic function field having full constant field $\mathbb{F}_q$. Let $\mathbb{P}_F$ be the set of places of F and denote with S a proper non-empty subset of $\mathbb{P}_F$. To S we associate the holomorphy ring $H = \bigcap_{P \in S} \mathcal{O}_P$. Furthermore let us define the set $\mathcal{D} := \{D \in \mathrm{Div}(F) \mid D \geq 0 \text{ and } \mathrm{supp}(D) \subseteq \mathbb{P}_F \setminus S\}$. It follows that

$$H = \bigcup_{D \in \mathcal{D}} \mathcal{L}(D),$$

where $\mathcal{L}(D)$ denotes the Riemann-Roch space for the divisor D. Furthermore, we recall that a holomorphy ring is also a Dedekind domain, hence the prime ideals of H correspond to the maximal ideals of H, which are of the form $P \cap H =: P_H$ and are in one-to-one correspondence with the places in $S \subsetneq \mathbb{P}_F$. In order not to heavier the notation, we will denote P_H again by P.

We now need an appropriate definition of density for our setting and for this we state a definition analogous to the natural density of the integer setting.

Definition 2.0.8. Let $A \subseteq H^m$, we define the *upper* and *lower density* of A as

$$\overline{\mathbb{D}}(A) = \limsup_{D \in \mathcal{D}} \frac{|A \cap \mathcal{L}(D)^m|}{|\ \mathcal{L}(D)^m\ |},$$

$$\underline{\mathbb{D}}(A) = \liminf_{D \in \mathcal{D}} \frac{|A \cap \mathcal{L}(D)^m|}{|\ \mathcal{L}(D)^m\ |}.$$

This limit is defined using the Moore-Smith convergence ad described in [5, Chapter 2]. As we have seen in Chapter 1 we have a partial ordering for the set of divisors, hence $(\mathcal{D}, \leq)$ is a directed set. Thus the map going from $\mathcal{D}$ to the topological space $\mathbb{R}$ defined as

$$D \longrightarrow \frac{|A \cap \mathcal{L}(D)^m|}{|\ \mathcal{L}(D)^m\ |}$$

is a net. Therefore the definition makes sense, since $\mathbb{R}$ is a Hausdorff space. Furthermore, if $\overline{\mathbb{D}}(A) = \underline{\mathbb{D}}(A)$, we denote this value $\mathbb{D}(A)$ and call it the *density* of A.

Finally notice that throughout this chapter, when Y is a set and m is a positive integer, we will denote by Y^m the cartesian product of m-copies of Y. To avoid confusion, the square of an ideal Q will then be denoted by $\widehat{Q} = Q \cdot Q$. Furthermore notice that in the whole chapter we consider polynomials of degree $d > 1$.

2.1 Monic Eisenstein Polynomials

In this section we focus on computing the density of monic Eisenstein polynomials.

We begin by introducing the notation which will be used. First we fix an enumeration of the places of S, that is $\{Q_1, Q_2, \dots, Q_i, \dots\}$. Now, with a small abuse of notation we identify H^d with the set of all monic polynomials of degree d having entries over H, meaning that if $(h_0, \dots, h_{d-1}) \in H^d$, then h_i denotes the coefficient of the monomial of degree i. Furthermore, we denote by $\mathcal{E} \subset H^d$ the set of monic Eisenstein polynomials of degree d and by $\mathcal{N}$ its complement in H^d. Moreover we denote by $\mathcal{E}_i$ the set of monic polynomials which are Eisenstein with respect to Q_i, that is to say:

$$\mathcal{E}_i = \{(h_0, \dots, h_{d-1}) \in H^d : \quad h_l \in Q_i \text{ for all } l \in \{0, \dots d-1\} \text{ and } h_0 \notin \widehat{Q}_i\}.$$

Finally we denote by $\mathcal{N}_i$ the complement of $\mathcal{E}_i$.

In order to compute the density we approximate the complement of $\mathcal{E}$ with $\overline{\mathcal{N}_t} := \bigcap_{i=1}^{t} \mathcal{N}_i$. First we give an explicit computation of the density of $\overline{\mathcal{N}_t}$, second we state a lemma telling us under which conditions the density of $\overline{\mathcal{N}_t}$ converges to the density of $\mathcal{N}$. To conclude, we verify that such conditions are fulfilled and then the density of $\mathcal{E}$ will just be the complement of the density of $\mathcal{N}$.

Proposition 2.1.1. *The density of $\overline{\mathcal{N}_t}$ is*

$$\mathbb{D}(\overline{\mathcal{N}_t}) = \prod_{i=1}^{t} \left(1 - \frac{q^{\deg(Q_i)} - 1}{q^{(d+1)\deg(Q_i)}}\right).$$

Proof. Consider the map

$$\tilde{\phi} : H^d \to \left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^d,$$

which is defined componentwise by the reduction modulo the ideal $(\widehat{Q}_1 \cdots \widehat{Q}_t)$. Observe also that $\left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^d \simeq \prod_{i=1}^{t} \left(H/\widehat{Q}_i\right)^d$ by the Chinese Remainder Theorem. Consider now a divisor $D \in \mathcal{D}$. In order to compute the density of $\overline{\mathcal{N}_t}$ it is enough to count how many elements there are in $\overline{\mathcal{N}_t} \cap \mathcal{L}(D)^d$, when the degree of D is large.

We start by showing that $\mathcal{L}(D)^d$ maps surjectively onto $\left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^d$ when the degree of D is large enough.

For this consider the $\mathbb{F}_q$ linear map $\phi : \mathcal{L}(D) \to \left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)$. We have $\ker(\phi) = \mathcal{L}(D) \cap (\widehat{Q}_1 \cdots \widehat{Q}_t)$, which represents the elements of $\mathcal{L}(D)$ having at least a double root at each Q_i. Hence $\ker(\phi) = \mathcal{L}(D - 2\sum_{i=1}^{t} Q_i)$.
By Riemann's Theorem, if the degree of D is large enough, the dimension of the kernel as an $\mathbb{F}_q$ vector space is

$$\ell\left(D - 2\sum_{i=1}^{t} Q_i\right) = \deg\left(D - 2\sum_{i=1}^{t} Q_i\right) + 1 - g$$

$$= \deg(D) - 2\sum_{i=1}^{t} \deg(Q_i) + 1 - g, \tag{2.1}$$

where g denotes the genus of the function field.
By the same theorem $\ell(D) = \deg(D) + 1 - g$. Hence we obtain

$$\dim_{\mathbb{F}_q}\left(\mathcal{L}(D)/\ker(\phi)\right) = \ell(D) - \ell\left(D - 2\sum_{i=1}^{t} Q_i\right) = 2\sum_{i=1}^{t} \deg(Q_i).$$

On the other hand, by the Chinese Remainder Theorem

$$\dim_{\mathbb{F}_q}\left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right) \overset{CRT}{=} \dim_{\mathbb{F}_q}\left(H/\widehat{Q}_1 \times \cdots \times H/\widehat{Q}_t\right) = 2\sum_{i=1}^{t} \deg(Q_i).$$

Therefore when the degree of D is large enough ϕ is surjective, thus $\tilde{\phi}$ is surjective.

Let $\psi_i : \left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^d \longrightarrow \left(H/\widehat{Q}_i\right)^d$. We have the following situation:

$$\mathcal{L}(D)^d \overset{\tilde{\phi}}{\twoheadrightarrow} \left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^d \overset{\psi}{\to} \prod_{i=1}^{t} \left(H/\widehat{Q}_i\right)^d,$$

where $\psi = (\psi_1, \ldots, \psi_t)$. Notice that the check for $f \in H^d$ not to be Eisenstein with respect to Q_i can be performed by looking at the reduction modulo $\widehat{Q}_i$. Therefore $f \in \overline{\mathcal{N}_t} \cap \mathcal{L}(D)^d$ if and only if $\psi_i \circ \tilde{\phi}(f) \notin \left((Q_i/\widehat{Q}_i) \setminus \{0\}\right) \times \left(Q_i/\widehat{Q}_i\right)^{d-1} =: E_i$ for all $i \in \{1, \ldots, t\}$.

It follows that $\overline{\mathcal{N}_t} \cap \mathcal{L}(D)^d = \tilde{\phi}^{-1}\left(\psi^{-1}\left(\prod_{i=1}^{t}\left((H/\widehat{Q}_i)^d \setminus E_i\right)\right)\right) \cap \mathcal{L}(D)^d$. Hence

$$|\,\overline{\mathcal{N}_t} \cap \mathcal{L}(D)^d\,| = |\,\ker(\tilde{\phi})\,| \cdot \prod_{i=1}^{t} |\,\left(H/\widehat{Q}_i\right)^d \setminus E_i\,|$$

$$= q^{d\left(\deg(D) - 2\sum_{i=1}^{t}\deg(Q_i) + 1 - g\right)} \cdot \prod_{i=1}^{t} |\,\left(H/\widehat{Q}_i\right)^d \setminus E_i\,|,$$

where the last equality follows from (2.1). Now it remains to compute

$$|\,\left(H/\widehat{Q}_i\right)^d \setminus E_i\,| = q^{2d\deg(Q_i)} - |\,\left((Q_i/\widehat{Q}_i) \setminus \{0\}\right) \times \left(Q_i/\widehat{Q}_i\right)^{d-1}\,|$$

$$= q^{2d\deg(Q_i)} - \left(q^{\deg(Q_i)} - 1\right) \cdot q^{(d-1)\deg(Q_i)}$$

$$= q^{2d\deg(Q_i)}\left(1 - q^{-d\deg(Q_i)} + q^{-(d+1)\deg(Q_i)}\right).$$

Therefore for D of degree large enough

$$\frac{|\,\overline{\mathcal{N}_t} \cap \mathcal{L}(D)^d\,|}{|\,\mathcal{L}(D)^d\,|} = \frac{q^{d\left(\deg(D) - 2\sum_{i=1}^{t}\deg(Q_i) + 1 - g\right)}}{q^{d(\deg(D) + 1 - g)}} \cdot \prod_{i=1}^{t} q^{2d\deg(Q_i)}\left(1 - q^{-d\deg(Q_i)} + q^{-(d+1)\deg(Q_i)}\right)$$

$$= \prod_{i=1}^{t} \left(1 - q^{-d\deg(Q_i)} + q^{-(d+1)\deg(Q_i)}\right) = \prod_{i=1}^{t} \left(1 - \frac{q^{\deg(Q_i)} - 1}{q^{(d+1)\deg(Q_i)}}\right).$$

Hence

$$\mathbb{D}(\overline{\mathcal{N}_t}) = \lim_{D\in\mathcal{D}} \frac{|\ \overline{\mathcal{N}_t} \cap \mathcal{L}(D)^d\ |}{|\ \mathcal{L}(D)^d\ |} = \prod_{i=1}^{t} \left(1 - \frac{q^{\deg(Q_i)} - 1}{q^{(d+1)\deg(Q_i)}}\right).$$

□

Lemma 2.1.2. *Let $n \in \mathbb{N}$, $A \subseteq H^n$. Let $\{A_t\}_{t\in\mathbb{N}}$ be a family of subsets of H^n such that $A_{t+1} \subseteq A_t$ and $\bigcap_{t\in\mathbb{N}} A_t = A$. Assume also that $\mathbb{D}(A_t)$ exists for all t. If $\lim_{t\to\infty} \overline{\mathbb{D}}(A_t \setminus A) = 0$, then $\mathbb{D}(A) = \lim_{t\to\infty} \mathbb{D}(A_t)$.*

Proof. We start from the equality $|\ A_t \cap \mathcal{L}(D)^n\ | = |\ A \cap \mathcal{L}(D)^n\ | + |\ (A_t \setminus A) \cap \mathcal{L}(D)^n\ |$, from which it follows

$$\begin{aligned}\liminf_{D\in\mathcal{D}} \frac{|\ A \cap \mathcal{L}(D)^n\ |}{|\ \mathcal{L}(D)^n\ |} &= \liminf_{D\in\mathcal{D}} \left(\frac{|\ A_t \cap \mathcal{L}(D)^n\ |}{|\ \mathcal{L}(D)^n\ |} - \frac{|\ (A_t \setminus A) \cap \mathcal{L}(D)^n\ |}{|\ \mathcal{L}(D)^n\ |}\right) \\ &\geq \liminf_{D\in\mathcal{D}} \frac{|\ A_t \cap \mathcal{L}(D)^n\ |}{|\ \mathcal{L}(D)^n\ |} - \limsup_{D\in\mathcal{D}} \frac{|\ (A_t \setminus A) \cap \mathcal{L}(D)^n\ |}{|\ \mathcal{L}(D)^n\ |}.\end{aligned}$$

It follows that $\underline{\mathbb{D}}(A_t) - \overline{\mathbb{D}}(A_t \setminus A) \leq \underline{\mathbb{D}}(A)$. Since $\mathbb{D}(A_t)$ exists for all t we get

$$\mathbb{D}(A_t) - \overline{\mathbb{D}}(A_t \setminus A) \leq \underline{\mathbb{D}}(A).$$

Now notice that $\lim_{t\to\infty} \mathbb{D}(A_t)$ exists since $\mathbb{D}(A_t)$ is decreasing and bounded from below. By taking the limit in t, the last expression then becomes

$$\lim_{t\to\infty} \mathbb{D}(A_t) - \lim_{t\to\infty} \overline{\mathbb{D}}(A_t \setminus A) \leq \underline{\mathbb{D}}(A).$$

Since $\lim_{t\to\infty} \overline{\mathbb{D}}(A_t \setminus A) = 0$ by assumption, it follows that $\lim_{t\to\infty} \mathbb{D}(A_t) \leq \underline{\mathbb{D}}(A)$.

On the other hand $A \subseteq A_t$ which implies $\overline{\mathbb{D}}(A) \leq \mathbb{D}(A_t)$. In particular $\overline{\mathbb{D}}(A) \leq \lim_{t\to\infty} \mathbb{D}(A_t)$. Combining all together we get

$$\lim_{t\to\infty} \mathbb{D}(A_t) \leq \underline{\mathbb{D}}(A) \leq \overline{\mathbb{D}}(A) \leq \lim_{t\to\infty} \mathbb{D}(A_t),$$

therefore the claim follows. □

Theorem 2.1.3. *The density of the set of monic Eisenstein polynomials with coefficients in H is*

$$\mathbb{D}(\mathcal{E}) = 1 - \prod_{Q\in\mathcal{S}} \left(1 - \frac{q^{\deg(Q)} - 1}{q^{(d+1)\deg(Q)}}\right).$$

Proof. We make use of Lemma 2.1.2 for the family $\{\overline{\mathcal{N}_t}\}_{t\in\mathbb{N}}$. Hence we want to show that $\lim_{t\to\infty} \overline{\mathbb{D}}(\overline{\mathcal{N}_t} \setminus \mathcal{N}) = 0$.
First notice that

- $\overline{\mathcal{N}_t} \setminus \mathcal{N} = \bigcup_{r>t} \mathcal{E}_r \subseteq \bigcup_{r>t} Q_r^d$,
- $Q_r \cap \mathcal{L}(D) = \mathcal{L}(D - Q_r) = 0$, if $\deg(D) - \deg(Q_r) < 0$.

Now we get

$$\overline{\mathbb{D}}(\overline{\mathcal{N}_t} \setminus \mathcal{N}) = \limsup_{D\in\mathcal{D}} \frac{|\ (\overline{\mathcal{N}_t} \setminus \mathcal{N}) \cap \mathcal{L}(D)^d\ |}{|\ \mathcal{L}(D)^d\ |} \leq \limsup_{D\in\mathcal{D}} \left| \bigcup_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} Q_r^d \cap \mathcal{L}(D)^d \right| q^{-d\ell(D)}$$

$$= \limsup_{D\in\mathcal{D}} \left| \bigcup_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \mathcal{L}(D-Q_r)^d \right| q^{-d\ell(D)} \leq \limsup_{D\in\mathcal{D}} \sum_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \frac{q^{d\ell(D-Q_r)}}{q^{d\ell(D)}}. \quad (2.2)$$

Observe now that if $\deg(D-Q_r) \geq 0$ we have that $\ell(D-Q_r) \leq \deg(D-Q_r)+1$ and also that $\ell(D) \geq \deg(D)+1-g$ by Riemann's Theorem.
Hence we have that (2.2) is less or equal than

$$\limsup_{D\in\mathcal{D}} \sum_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \frac{q^{d(1+\deg(D)-\deg(Q_r))}}{q^{d(\deg(D)+1-g)}} \leq \sum_{r>t} q^{d(g-\deg(Q_r))} = q^{dg} \sum_{r>t} q^{-d\deg(Q_r)}.$$

We now notice that $\sum_{r>t} q^{-d\deg(Q_r)}$ is the tail of a subseries of the Zeta function, which is absolutely convergent for $d>1$. Letting t going to infinity the tail converges to 0, thus $\lim_{t\to\infty} \overline{\mathbb{D}}(\overline{\mathcal{N}_t} \setminus \mathcal{N}) = 0$. We are now able to apply Lemma 2.1.2 with $n=d$, $A_t = \overline{\mathcal{N}_t}$ and $A = \mathcal{N}$

$$\mathbb{D}(\mathcal{N}) = \lim_{t\to\infty} \mathbb{D}(\overline{\mathcal{N}_t}) = \lim_{t\to\infty} \prod_{i=1}^{t} \left(1 - \frac{q^{\deg(Q_i)}-1}{q^{(d+1)\deg(Q_i)}}\right) = \prod_{Q\in\mathcal{S}} \left(1 - \frac{q^{\deg(Q)}-1}{q^{(d+1)\deg(Q)}}\right).$$

We conclude by taking the complement

$$\mathbb{D}(\mathcal{E}) = 1 - \mathbb{D}(\mathcal{N}) = 1 - \prod_{Q\in\mathcal{S}} \left(1 - \frac{q^{\deg(Q)}-1}{q^{(d+1)\deg(Q)}}\right).$$

□

2.2 Non-Monic Eisenstein Polynomials

In this section we compute the density of non-monic Eisenstein polynomials applying the same strategy of section 2.1. As before we fix an enumeration of the places of S, that is $\{Q_1, Q_2, \ldots, Q_i, \ldots\}$. Analogously to the previous section, we identify the set of all polynomials of degree d having entries over H with H^{d+1}. Let $\mathcal{E}^+ \subseteq H^{d+1}$ be the set of Eisenstein polynomials of degree d and $\mathcal{N}^+$ be its complement in H^{d+1}. We denote by $\mathcal{E}_i^+$ the set of polynomials which are Eisenstein with respect to Q_i:

$$\mathcal{E}_i^+ = \{(h_0, \ldots, h_d) \in H^{d+1} : \quad h_l \in Q_i \text{ for all } l \in \{0, \ldots d-1\},\ h_0 \notin \widehat{Q}_i \text{ and } h_d \notin Q_i\}.$$

We denote by $\mathcal{N}_i^+$ the complement of $\mathcal{E}_i^+$.
Finally let $\overline{\mathcal{N}_t}^+ = \bigcap_{i=1}^t \mathcal{N}_i^+$.

Proposition 2.2.1. *The density of $\overline{\mathcal{N}_t}^+$ is*

$$\mathbb{D}(\overline{\mathcal{N}_t}^+) = \prod_{i=1}^{t} \left(1 - \frac{(q^{\deg(Q_i)}-1)^2}{q^{(d+2)\deg(Q_i)}}\right).$$

Proof. Consider a divisor $D \in \mathcal{D}$. With the same reasoning of the monic case one can show that $\mathcal{L}(D)^{d+1}$ maps surjectively onto $\left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^{d+1}$ when the degree of D is large enough.

Let $\psi_i : \left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^{d+1} \longrightarrow \left(H/\widehat{Q}_i\right)^{d+1}$ as before. The situation is now the following:

$$\mathcal{L}(D)^{d+1} \overset{\tilde{\phi}}{\twoheadrightarrow} \left(H/(\widehat{Q}_1 \cdots \widehat{Q}_t)\right)^{d+1} \overset{\psi}{\to} \prod_{i=1}^{t} \left(H/\widehat{Q}_i\right)^{d+1},$$

where $\psi = (\psi_1, \ldots, \psi_t)$.
Analogously to the case of monic polynomials we note that we can verify that $f \in H$ is not Eisenstein with respect to Q_i by looking at the reduction modulo $\widehat{Q}_i$. Hence $f \in \overline{\mathcal{N}_t}^{+} \cap \mathcal{L}(D)^{d+1}$ if and only if $\psi_i \circ \tilde{\phi}(f) \notin \left((Q_i/\widehat{Q}_i) \setminus \{0\}\right) \times \left(Q_i/\widehat{Q}_i\right)^{d-1} \times \left((H/\widehat{Q}_i) \setminus (Q_i/\widehat{Q}_i)\right) =: E_i^{+}$ for all $i \in \{1, \ldots, t\}$.
Hence we get

$$| \overline{\mathcal{N}_t}^{+} \cap \mathcal{L}(D)^{d+1} | = | \ker(\tilde{\phi}) | \cdot \prod_{i=1}^{t} | \left(H/\widehat{Q}_i\right)^{d+1} \setminus E_i^{+} |$$

$$= q^{(d+1)\left(\deg(D) - 2\sum_{i=1}^{t} \deg(Q_i) + 1 - g\right)} \cdot \prod_{i=1}^{t} | \left(H/\widehat{Q}_i\right)^{d+1} \setminus E_i^{+} |,$$

where

$$\begin{aligned}
| \left(H/\widehat{Q}_i\right)^{d+1} \setminus E_i^{+} | &= q^{2(d+1)\deg(Q_i)} - | \left((Q_i/\widehat{Q}_i) \setminus \{0\}\right) \times \left(Q_i/\widehat{Q}_i\right)^{d-1} \times \left((H/\widehat{Q}_i) \setminus (Q_i/\widehat{Q}_i)\right) | \\
&= q^{2(d+1)\deg(Q_i)} - \left(\left(q^{\deg(Q_i)} - 1\right) q^{(d-1)\deg(Q_i)} \left(q^{2\deg(Q_i)} - q^{\deg(Q_i)}\right)\right) \\
&= q^{2(d+1)\deg(Q_i)} \left(1 - \frac{q^{2\deg(Q_i)} - 2q^{\deg(Q_i)} + 1}{q^{(d+2)\deg(Q_i)}}\right) \\
&= q^{2(d+1)\deg(Q_i)} \left(1 - \frac{\left(q^{\deg(Q_i)} - 1\right)^2}{q^{(d+2)\deg(Q_i)}}\right).
\end{aligned}$$

Therefore for D of degree large enough

$$\begin{aligned}
\frac{| \overline{\mathcal{N}_t}^{+} \cap \mathcal{L}(D)^{d+1} |}{| \mathcal{L}(D)^{d+1} |} &= \frac{q^{(d+1)\left(\deg(D) - 2\sum_{i=1}^{t} \deg(Q_i) + 1 - g\right)}}{q^{(d+1)(\deg(D) + 1 - g)}} \cdot \prod_{i=1}^{t} q^{2(d+1)\deg(Q_i)} \left(1 - \frac{\left(q^{\deg(Q_i)} - 1\right)^2}{q^{(d+2)\deg(Q_i)}}\right) \\
&= \prod_{i=1}^{t} \left(1 - \frac{\left(q^{\deg(Q_i)} - 1\right)^2}{q^{(d+2)\deg(Q_i)}}\right).
\end{aligned}$$

Hence

$$\mathbb{D}(\overline{\mathcal{N}_t}^{+}) = \lim_{D \in \mathcal{D}} \frac{| \overline{\mathcal{N}_t}^{+} \cap \mathcal{L}(D)^{d+1} |}{| \mathcal{L}(D)^{d+1} |} = \prod_{i=1}^{t} \left(1 - \frac{\left(q^{\deg(Q_i)} - 1\right)^2}{q^{(d+2)\deg(Q_i)}}\right).$$

□

Theorem 2.2.2. *The density of the set of Eisenstein polynomials with coefficients in H is*

$$\mathbb{D}(\mathcal{E}^{+}) = 1 - \prod_{Q \in \mathcal{S}} \left(1 - \frac{(q^{\deg(Q)} - 1)^2}{q^{(d+2)\deg(Q)}}\right).$$

Proof. Again by Lemma 2.1.2 we have to show that $\lim_{t\to\infty} \overline{\mathbb{D}}(\overline{\mathcal{N}_t}^+ \setminus \mathcal{N}^+) = 0$. Observe that $\mathcal{E}_r^+ \cap \mathcal{L}(D)^{d+1} \subseteq Q_r^d \times \mathcal{L}(D)$. We get

$$\begin{aligned}
\overline{\mathbb{D}}(\overline{\mathcal{N}_t}^+ \setminus \mathcal{N}^+) &= \limsup_{D\in\mathcal{D}} \frac{|\ (\overline{\mathcal{N}_t}^+ \setminus \mathcal{N}^+) \cap \mathcal{L}(D)^{d+1}\ |}{|\ \mathcal{L}(D)^{d+1}\ |} \\
&\leq \limsup_{D\in\mathcal{D}} \left| \bigcup_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \mathcal{E}_r^+ \cap \mathcal{L}(D)^{d+1} \right| q^{-(d+1)\ell(D)} \\
&\leq \limsup_{D\in\mathcal{D}} \left| \bigcup_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \Big(Q_r^d \times \mathcal{L}(D)\Big) \cap \mathcal{L}(D)^{d+1} \right| q^{-(d+1)\ell(D)} \\
&\leq \limsup_{D\in\mathcal{D}} \sum_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \frac{|\ \big(Q_r^d \times \mathcal{L}(D)\big) \cap \mathcal{L}(D)^{d+1}\ |}{q^{(d+1)\ell(D)}} \\
&= \limsup_{D\in\mathcal{D}} \sum_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \frac{|\ Q_r \cap \mathcal{L}(D)\ |^d |\ \mathcal{L}(D)\ |}{q^{(d+1)\ell(D)}} \\
&= \limsup_{D\in\mathcal{D}} \sum_{\substack{r>t \\ \deg(Q_r)\leq\deg(D)}} \frac{|\ Q_r \cap \mathcal{L}(D)\ |^d}{q^{d\ell(D)}}
\end{aligned}$$

which is equation (2.2). Hence for t going to infinity we obtain $\overline{\mathbb{D}}(\overline{\mathcal{N}_t}^+ \setminus \mathcal{N}^+) = 0$.

We now apply Lemma 2.1.2 with $n = d+1$, $A_t = \overline{\mathcal{N}_t}^+$ and $A = \mathcal{N}^+$ obtaining

$$\mathbb{D}(\mathcal{N}^+) = \lim_{t\to\infty} \mathbb{D}(\overline{\mathcal{N}_t}^+) = \lim_{t\to\infty} \prod_{i=1}^{t} \left(1 - \frac{\left(q^{\deg(Q_i)} - 1\right)^2}{q^{(d+2)\deg(Q_i)}}\right) = \prod_{Q\in\mathcal{S}} \left(1 - \frac{\left(q^{\deg(Q)} - 1\right)^2}{q^{(d+2)\deg(Q)}}\right).$$

We now take the complement

$$\mathbb{D}(\mathcal{E}^+) = 1 - \mathbb{D}(\mathcal{N}^+) = 1 - \prod_{Q\in\mathcal{S}} \left(1 - \frac{\left(q^{\deg(Q)} - 1\right)^2}{q^{(d+2)\deg(Q)}}\right).$$

□

Chapter 3

Eisenstein Polynomials and Totally Ramified Places

Since in the previous chapters we have discussed function fields and Eisenstein polynomials, we would like to develop the theory a little further in order to obtain a result which connects the two things in some way. This will be the function field analogue of the work of Keith Conrad in [1], which is about number fields. For this we start talking about algebraic extensions of function fields.

3.1 Algebraic Extensions of Function Fields

Definition 3.1.1.

i) Let F be a function field over K. An *algebraic extension* of F is an algebraic function field E over K' such that $E \supseteq F$ is an algebraic field extension and also $K' \supseteq K$.

ii) The extension E of F is called finite if $[E : F] < \infty$.

iii) If the extension E of F satisfies $E = FK'$, then E is called a constant field extension.

For the rest of the chapter let E over K' denotes an algebraic extension of the function field F over K, with $K \subseteq K'$.

As a consequence of the definitions, we can see that if E is an algebraic extension of F, then K' is algebraic over K and $K = F \cap K'$. Moreover we have that E is a finite extension of F if and only if $[K' : K] < \infty$. Also note that $F' := FK'$ over K' is a constant field extension of F and E is a finite extension of F'.

With the notion of extensions of function fields is natural to discuss the intersection between the base field and its extension. For this we investigate the relations between the places of the two fields.

Definition 3.1.2. Let E be an extension of F. Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_E$ be places of F and of E respectively. If $P \subseteq P'$ then P' is said to lie over P. Equivalent one can say that P lies under P' or that P' is an extension of P. The notation is $P' \mid P$.

Such extensions of places exists as shown in [7, Proposition 3.1.7]. More precisely, for each place $P \in \mathbb{P}_F$ there is at least one, but finitely many extensions $P' \in \mathbb{P}_E$. On the opposite, for each $P' \in \mathbb{P}_E$ there is exactly one $P \in \mathbb{P}_F$ for which $P' \mid P$ and this will turn out to be $P = P' \cap F$.

Next we state a proposition which tells us which are equivalent conditions for the fulfilment of the Definition 3.1.2.

Proposition 3.1.3. *Let E be an algebraic extension of F. Consider a place $P \in \mathbb{P}_F$ and a place $P' \in \mathbb{P}_E$ and let $\mathcal{O}_P \subseteq F$ and $\mathcal{O}_{P'} \subseteq E$ be the corresponding valuation rings with respect to the discrete valuations v_P and $v_{P'}$. Then the following are equivalent:*

1. *$P' \mid P$,*
2. *$\mathcal{O}_P \subseteq \mathcal{O}_{P'}$,*
3. *there exists $e \in \mathbb{N}$, $e \geq 1$ such that for all $x \in F$ $v_{P'}(x) = e \cdot v_P(x)$.*

Furthermore notice that if $P' \mid P$, it follows that

$$P = P' \cap F \text{ and } \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

Proof. See [7, Proposition 3.1.4]. □

This proposition justify the next definitions.

Definition 3.1.4. Let E be an algebraic extension of F and consider the place $P \in \mathbb{P}_F$ lying under $P' \in \mathbb{P}_E$.

i) The natural number $e(P' \mid P) := e$ for which

$$v_{P'}(x) = e \cdot v_P(x)$$

is called the ramification index.

ii) We say that $P' \mid P$ is unramified if $e(P' \mid P) = 1$ and that $P' \mid P$ is ramified $e(P' \mid P) > 1$.

iii) $[E_{P'} : F_P] =: f(P' \mid P)$, where $F_P = \mathcal{O}_P/P$, is called the relative degree of P' over P. Notice that $f(P' \mid P)$ can also be infinite.

Moreover for the relative degree we have that $f(P \mid P') < \infty$ if and only if $[E : F] < \infty$. Furthermore for the ramification index and the relative degree there is a multiplicative propriety, that is to say: let E' over K'' be an algebraic extension of E with P'' lying over P', then

$$e(P'' \mid P) = e(P'' \mid P') \cdot e(P' \mid P),$$

$$f(P'' \mid P) = f(P'' \mid P') \cdot f(P' \mid P).$$

We now state a very important theorem.

Theorem 3.1.5. *Let E be an extension of F, $[E : F] < \infty$. Let $P \in \mathbb{P}_F$ and let $P_1, \ldots, P_n$ all the places in $\mathbb{P}_E$ lying over P. Then*

$$\sum_{i=1}^{n} e_i \cdot f_i = [E : F],$$

where e_i denotes the ramification index $e(P_i \mid P)$ and f_i denotes the relative degree $f(P_i \mid P)$.

Proof. [7, Theorem 3.1.11]. □

As a direct corollary of this theorem one can see that $|\{P' \in \mathbb{P}_E : P' \mid P\}| \leq [E:F]$ and moreover for a place P' such that $P' \mid P$ we have that $e(P' \mid P) \leq [E:F]$ and $f(P' \mid P) \leq [E:F]$.

These new results authorize us to state the next definitions.

Definition 3.1.6. Let E be an extension of F of degree n and consider a place $P \in \mathbb{P}_F$. Then

i) if there are exactly n places $P' \in \mathbb{P}_E$ lying over P, then we say that P splits completely in E,

ii) if there exist a place $P' \in \mathbb{P}_E$ with $e(P' \mid P) = n$, then we say that P is totally ramified in E.

We conclude this section by giving two statements which will be useful in Section 3.2.

Proposition 3.1.7. *Let F be a function field and let R be a holomoprhy ring of F. Let E be a finite extension of F and consider $x \in E$. Denote with $f_x(T) \in F[T]$ the minimal polynomial of x in F. Then*

$$x \text{ is integral over } R \Leftrightarrow f_x(T) \in R[T].$$

Lemma 3.1.8. *Let F be a function field and E a finite separable extension of F. Consider $P \in \mathbb{P}_F$. Then the integral closure of $\mathcal{O}_P$ in E is*

$$\mathrm{ic}_E(\mathcal{O}_P) = \bigcap_{P'|P} \mathcal{O}_{P'}.$$

The proofs can be found in [7, Proposition 3.3.1] and [7, Corollary 3.3.5] respectively.

3.2 Eisenstein Polynomials and Totally Ramified Places

In this section we establish a connection between totally ramified places of a function field and Eisenstein polynomials in a similar way to the work of K. Conrad in [1]. The two results are converse of each other. First we show that whenever we have a simple extension of a function field F, i.e. $E = F(\alpha)$, with α being a root a polynomial which is Eisenstein at a place $Q \in \mathbb{P}_F$, then Q is totally ramified in E. Second we show that whenever we deal with a finite separable extension E of a function field F with a place $Q \in \mathbb{P}_F$ totally ramified in E, then E can be written as $E = F(\alpha)$, where α is a prime element of Q and its minimal polynomial is Eisenstein at Q. The first result will be a direct corollary of Theorem 3.2.1, whereof a more general version can be found in [7, Proposition 3.1.15]. The second result will need a more thoughtful approach, for which I would like to thank Giacomo Micheli.

Theorem 3.2.1. *Let F be a function field and E an extension of F of the form $E = F(\alpha)$, where α is a root of the polynomial $f_\alpha(T) = a_n T^n + \cdots + a_1 T + a_0 \in F[T]$. Let $Q \in \mathbb{P}_F$ be a place of F such that*

i) $v_Q(a_0) = 1$,

ii) $v_Q(a_i) > 0$ *for all* $i \in \{1, \ldots, n-1\}$,

iii) $v_Q(a_n) = 0$.

Then Q is totally ramified in E.

Proof. Consider a place P lying over Q and denote by $e := e(P \mid Q)$ its ramification index, i.e $v_P(x) = e \cdot v_Q(x)$ for all $x \in F$.
We want to show that $e = n$, where $n = [F(\alpha) : F]$. By Theorem 3.1.5 we already know that $e \leq n$, so if we can show that $e \geq n$, we are done.
Notice that the three conditions in the assumption imply also that $v_P(a_i) > 0$ for all $i \in \{1, \dots, n-1\}$ and $v_P(a_n) = 0$.
Since α is a root of $f_\alpha(T)$ we get the equation

$$-a_n\alpha^n = a_0 + \cdots + a_{n-1}\alpha^{n-1}. \tag{3.1}$$

By taking the valuation at P of the left and right side of (3.1) and applying the triangle inequality for valuations, one can see that $v_P(\alpha) > 0$. Now for $i \in \{1, \dots, n-1\}$ we obtain

$$v_P(a_i\alpha^i) = v_P(a_i) + v_P(\alpha^i) = e \cdot v_Q(a_i) + i \cdot v_P(\alpha) > e \cdot v_Q(a_i) \geq e \cdot v_Q(a_0) = v_P(a_0).$$

We can now apply the strict triangle inequality while we take the valuation of (3.1) at P obtaining

$$n \cdot v_P(\alpha) = v_P(-a_n\alpha^n) = v_P(a_0 + \cdots + a_{n-1}\alpha^{n-1}) = v_P(a_0) = e \cdot v_Q(a_0).$$

Hence, since by assumption $v_Q(a_0) = 1$, we get that $n \cdot v_P(\alpha) = e$, implying that n divides e, which tells us that $n \leq e$, completing the proof. □

Corollary 3.2.2. *Let F be a function field and $H \subseteq F$ a holomorphy ring of F. Let E be an extension of F of the form $E = F(\alpha)$, where α is a root of a polynomial $f_\alpha(T) \in H[T]$ with f_α Eisenstein at a place $Q \in \mathbb{P}_F$. Then Q is totally ramified in E.*

Proof. For the proof is enough to show that the valuations of the coefficients of f_α satisfy the proprieties of Theorem 3.2.1, and then the proof will follow by the same theorem.
Since f_α is Eisenstein at Q it means that $a_0 \in Q \setminus Q^2$, $a_i \in Q$ for all $i \in \{1, \dots, n-1\}$ and $a_n \notin Q$.
This directly imply that $v_Q(a_0) = 1$, $v_Q(a_i) > 0$ for all $i \in \{1, \dots, n-1\}$ and, since all the coefficients of f_α are in H, $v_Q(a_n) = 0$. Thus all the assumptions of Theorem 3.2.1 are fulfilled and the claim follows. □

We now would like to establish some sort of converse result. Notice that, differently from the result of Conrad, in order to obtain this converse relation between totally ramified places and Eisenstein polynomials, we have to assume the extension of F to be separable. This is not needed in the work of Conrad since extensions of number fields are always separable extensions.

Lemma 3.2.3. *Let F be a function field and let E be a separable extension of F of the form $E = F(\alpha)$, α algebraic over F. Assume the degree of the extension to be $[E : F] = d < \infty$. Let now $P \in \mathbb{P}_E$ such that $\alpha \in P \setminus P^2$ and let $Q \in \mathbb{P}_F$ the unique place of F lying under P. Assume finally that Q is totally ramified in E. Then the minimal polynomial of α, $f_\alpha(T) \in F[T]$, is Eisenstein at Q.*

Proof. First we claim that the coefficients of the minimal polynomial of α actually lie in the valuation ring $\mathcal{O}_Q$. Indeed, by Proposition 3.1.8 and since Q is totally ramified it follows that

$$\mathrm{ic}_E(\mathcal{O}_Q) = \{z \in E \mid z \text{ is integral over } \mathcal{O}_Q\} = \bigcap_{P' \mid Q} \mathcal{O}_{P'} = \mathcal{O}_P.$$

Since α is an element of $P \setminus P^2$, it is in particular an element of $\mathcal{O}_P$ implying that α is integral over $\mathcal{O}_Q$. Thus we just apply Lemma 3.1.7 and we get that $f_\alpha \in \mathcal{O}_Q[T]$.

Moreover notice that $Q \subseteq P^d$. This is true since $v_Q(x) \geq 1$ for all $x \in Q$, hence for $x \in Q$ we get $v_P(x) = d \cdot v_Q(x) \geq d$.
Assume now that all the firsts $j-1$ coefficients of f_α are in Q but $a_j \notin Q$, for a fixed $j \in \{0, \dots, d-1\}$. Consider now the equation given by $f_\alpha(\alpha)$:

$$\alpha^d + \sum_{i=1}^{d-1} a_i \alpha^i + a_0 = 0.$$

By taking the equation modulo P^d we obtain

$$\sum_{i=j+1}^{d-1} a_i \alpha^i + a_j \alpha^j \equiv 0 \mod P^d$$

and so we get

$$\alpha^j \left(\sum_{i=j+1}^{d-1} a_i \alpha^{i-j} + a_j \right) \equiv 0 \mod P^d. \tag{3.2}$$

We now take the valuation at P of the left side

$$v_P\left(\alpha^j \left(\sum_{i=j+1}^{d-1} a_i \alpha^{i-j} + a_j \right)\right) = j + v_P\left(\sum_{i=j+1}^{d-1} a_i \alpha^{i-j} + a_j \right)$$

$$= j + \min\{v_P\left(\sum_{i=j+1}^{d-1} a_i \alpha^{i-j} \right), v_P(a_j)\}.$$

Observe that since we are assuming that $a_j \notin Q$ and since $a_j \in \mathcal{O}_Q$ we get that $v_P(a_j) = d \cdot v_Q(a_j) = 0$. Thus we obtain

$$\min\{v_P\left(\sum_{i=j+1}^{d-1} a_i \alpha^{i-j} \right), v_P(a_j)\} = 0 \text{ and so } v_P\left(\alpha^j \left(\sum_{i=j+1}^{d-1} a_i \alpha^{i-j} + a_j \right)\right) = j.$$

Combining what we have so far we get

$$d - 1 \geq j = v_P\left(\alpha^j \left(\sum_{i=j+1}^{d-1} a_i \alpha^{i-j} + a_j \right)\right) \geq d,$$

were the last inequality follows from (3.2). Clearly this is a contradiction, and so all the coefficients of f_α have to lie in Q.

It remains to prove that $a_0 \in Q \setminus Q^2$, which is equivalent to prove that $v_Q(a_0) = 1$. Since $a_0 \in Q$ we already have that $v_Q(a_0) \geq 1$. In order to produce a contradiction, assume that $v_Q(a_0) > 1$, which implies $v_P(a_0) = d \cdot v_Q(a_0) \geq 2d$. Consider now once again the equation given by $f_\alpha(\alpha)$: $-\alpha^d = \sum_{i=1}^{d-1} a_i \alpha^i + a_0$.
Taking the valuation of the equation at P and applying the triangle inequality we get

$$d \geq \min_{i=1,\dots,d-1} \{v_P(a_i) + i, v_P(a_0)\} \geq \min_{i=1,\dots,d-1} \{v_P(a_i) + i, 2d\}$$

$$= \min_{i=1,\dots,d-1} \{d \cdot v_Q(a_i) + i, 2d\} \geq \min_{i=1,\dots,d-1} \{d + i, 2d\} = d + 1,$$

which is a contradiction.
Hence $v_Q(a_0) = 1$, i.e. $a_0 \in Q \setminus Q^2$, therefore the claim follows.

□

Theorem 3.2.4. *Let F be a function field and let E be a finite and separable extension of F of degree $[E : F] = n$. Let $Q \in \mathbb{P}_F$ be a place of F and $P \in \mathbb{P}_E$ be a place of E lying above Q, with Q totally ramified in E. Moreover consider $\alpha \in P \setminus P^2$. Then the minimal polynomial $f_\alpha \in F[T]$ of α is a polynomial of degree n and it is Eisenstein at Q.*

Proof. Consider the following chain of extensions

$$E : F(\alpha) : F \tag{3.3}$$

and also consider $P \in \mathbb{P}_E$, $P' \in \mathbb{P}_{F(\alpha)}$ and $Q \in \mathbb{P}_F$ such that $P \mid P'$ and $P' \mid Q$. Notice that Q, being totally ramified in E, is also totally ramified in the intermediate extension $F(\alpha)$. Now $\alpha \in P \setminus P^2$, which means $v_P(\alpha) = 1$, and since we have $v_P(\alpha) = e(P \mid P') \cdot v_{P'}(\alpha)$, we get $v_{P'}(\alpha) = 1$, that is to say $\alpha \in P' \setminus P'^2$.
Due to the assumption that E is finite and separable we have also that the intermediate extension $F(\alpha)$ is finite and separable, therefore we can now apply Lemma 3.2.3. Thus the minimal polynomial f_α is Eisenstein at Q of degree $[F(\alpha) : F] =: d$.
It remains to show that $d = n$. By construction in (3.3) we already have that $d \leq n$, which means that we are left to show that $n \leq d$.
For this consider the equation given by $f_\alpha(\alpha)$:

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

By taking the valuation at P and using the triangle inequality for valuations we get

$$d = v_P(-\alpha^d) = v_P(\sum_{i=0}^{d-1} a_i \alpha^i)$$

$$\geq \min_{i=0,\dots,d-1} \{v_P(a_i) + i \cdot v_P(\alpha)\} = \min_{i=0,\dots,d-1} \{v_P(a_i) + i\}. \tag{3.4}$$

Recall that Q is totally ramified in E, hence $v_P(a_i) = n \cdot v_Q(a_i)$ for all $i \in \{0, \dots, d-1\}$, with $v_Q(a_i) \geq 1$ due to the fact that f_α is Eisenstein at Q. Therefore (3.4) is greater or equal than

$$\min_{i=0,\dots,d-1} \{n + i\} = n,$$

hence $d \geq n$ and so the claim follows. □

Corollary 3.2.5. *Let F be a function field and let E be a finite, separable extension of F of degree $[E : F] = n$. Let $Q \in \mathbb{P}_F$ be a place of F totally ramified in E. Then $E = F(\alpha)$, where α is a root of a polynomial $f_\alpha \in F[T]$ with f_α Eisenstein at Q.*

Proof. Consider the places $P \in \mathbb{P}_E$ lying above Q. Take an element $\alpha \in P \setminus P^2$ and consider its minimal polynomial $f_\alpha \in F[T]$. By Theorem 3.2.4 we have that f_α is Eisenstein at Q and has degree n. Therefore, with n being also the degree of the extension, we can conclude that E is of the from $E = F(\alpha)$, giving us the desired result. □

Acknowledgements

I would like to thank Professor J. Rosenthal for accepting to be my supervisor for this thesis and a special thanks to Giacomo Micheli who has accepted to follow me as co-supervisor throughout all this work, answering my questions, helping me when I was stuck, and teaching me a different way to think when dealing with new problems.

References

[1] Keith Conrad. Totally ramified primes and eisenstein polynomials. `http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/totram.pdf`.

[2] Edoardo Dotti and Giacomo Micheli. Eisenstein polynomials over function fields. *arXiv preprint arXiv:1506.05380*, 2015.

[3] Artūras Dubickas. Polynomials irreducible by eisenstein's criterion. *Applicable Algebra in Engineering, Communication and Computing*, 14(2):127–132, 2003.

[4] Randell Heyman and Igor E Shparlinski. On the number of eisenstein polynomials of bounded height. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):149–156, 2013.

[5] J. L. Kelley. *General topology*. New York: Van Nostrand, 1955.

[6] Giacomo Micheli and Reto Schnyder. On the density of coprime m-tuples over holomorphy rings. *To appear in International Journal of Number Theory*, 2014. URL `arXiv:1411.6876`.

[7] H. Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer, 2009.