CYCLICITY OF ELLIPTIC CURVES OVER FUNCTION FIELDS

by

KORAY KARABİNA

Submitted to the Graduate School of Engineering and Natural Sciences

in partial fulfillment of

the requirements for the degree of

Master of Science

Sabancı University

Spring 2005

CYCLICITY OF ELLIPTIC CURVES OVER FUNCTION FIELDS

APPROVED BY

Assist. Prof. Ebru BEKYEL .....
(Thesis Supervisor)

Assist. Prof. Cem GÜNERİ .....

Assist. Prof. Erkay SAVAŞ .....

DATE OF APPROVAL: June 13th, 2005

Aileme..

Acknowledgments

I would like to express my sincere regards to my supervisor Assist. Prof. Ebru Bekyel for her assistance and motivation throughout this thesis.

Also I would like to thank Assist. Prof. Cem Güneri for his support in my study.

Cyclicity of Elliptic Curves over Function Fields

Koray Karabina

Abstract

Let K be a global function field over a finite field F containing q elements. Let E be an elliptic curve defined over K. For a prime P in K we can reduce the elliptic curve mod P and get an elliptic curve over a finite extension of F. The group of points on the reduced elliptic curve is either a cyclic group or it is a product of two cyclic groups. We determine the Dirichlet density of the primes in K such that the reduced curve has a cyclic group structure.

Keywords: Function Fields, Zeta Functions, Elliptic Curves, Dirichlet Density.

Fonksiyon Cisimleri Üzerinde Tanımlı Eliptik Eğrilerin Döngüselliği
Koray Karabina

Özet

K, q elemanlı sonlu cisim F üzerindeki bir fonksiyon cismi olsun. E, K cismi üzerinde tanımlı bir eliptik eğri olsun. E eliptik eğrisinin denklemi K içindeki bir asal için indirgendiğinde elde edilen yeni eliptik eğri sonlu bir cisim üzerinde tanımlıdır. İndirgenen eliptik eğri üzerindeki noktaların oluşturduğu grup ya döngüseldir ya da iki döngüsel grubun çarpımıdır. Bu çalışmada, K cismi içindeki, indirgenmiş eliptik eğri grup yapısını döngüsel yapan asalların Dirichlet yoğunluğu hesaplanmaktadır.

Anahtar kelimeler: Fonksiyon Cisimleri, Zeta Fonksiyonu, Eliptik Eğriler, Dirichlet Yoğunluğu.

Contents

Acknowledgments **v**

Abstract **vi**

Özet **vii**

1 Algebraic Function Fields **1**

1.1 Function Fields 1

1.2 Divisors 6

1.3 Prime Decompositions in Function Field Extensions 10

2 Global Function Fields and the Zeta Function **17**

2.1 Global Function Fields 17

2.2 The Zeta Function of a Global Function Field 19

3 Elliptic Curves **26**

3.1 Curves 26

3.2 Elliptic Function Fields and Elliptic Curves 28

3.3 Reduction of Elliptic Curves 32

4 Dirichlet Density and Cyclicity of Elliptic Curves **36**

CHAPTER 1

Algebraic Function Fields

1.1 Function Fields

In this section, we will investigate function fields and their basic properties. For a general field F consider the extension $F(x)$ where x is a transcendental element over F. This extension consists of elements in the form $f(x)/g(x)$ where $f(x),\ 0 \neq g(x) \in F[x]$ and it is called the *rational function field*. In general, a finite algebraic extension, K, of a rational function field, $F(x)$, is called an *algebraic function field*. We will denote it by K/F. Function fields are very important algebraic structures because geometric objects are closely related to them. As we will see, it is possible to provide a one to one correspondences between geometry and algebra through function fields. Since the rational function field is easy to deal with, we will give examples and prove theorems for the rational function field while just stating the analogous material for more general function fields. The section follows [6] and [8] very closely.

Let $p(x)$ be an irreducible polynomial in $F[x]$ and define

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x],\ \text{g.c.d}(f(x), g(x)) = 1,\ p(x) \nmid g(x) \right\}$$

Clearly, $F \subsetneqq \mathcal{O}_{p(x)} \subsetneqq F(x)$ and $\mathcal{O}_{p(x)}$ is a ring. Note that, for any $0 \neq z \in F(x)$, either $z \in \mathcal{O}_{p(x)}$ or $z^{-1} \in \mathcal{O}_{p(x)}$, that is, the quotient field of $\mathcal{O}_{p(x)}$ gives the rational

function field $F(x)$. Now, define a subset of this ring as

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_{p(x)} \mid \ p(x) \mid f(x) \right\}$$

We see that $P_{p(x)} = \mathcal{O}_{p(x)} \setminus \mathcal{O}^*_{p(x)}$ where $\mathcal{O}^*_{p(x)}$ is the set of units in $\mathcal{O}_{p(x)}$ and we will show that $P_{p(x)}$ is in fact an ideal of $\mathcal{O}_{p(x)}$. Let $z = f(x)/g(x) \in \mathcal{O}_{p(x)}$ and $z_1 = f_1(x)/g_1(x),\ z_2 = f_2(x)/g_2(x) \in P_{p(x)}$. Then $zz_1 \notin \mathcal{O}^*_{p(x)}$ since $z_1 \notin \mathcal{O}^*_{p(x)}$, that is, $zz_1 \in P$. As we remark above z_1/z_2 or z_2/z_1 is in $\mathcal{O}_{p(x)}$. Assume $z_1/z_2 \in \mathcal{O}_{p(x)}$. Then, $z_1 + z_2 = z_2(\frac{z_1}{z_2} + 1) \in P$ since $z_2 \in P$ and $(\frac{z_1}{z_2} + 1) \in \mathcal{O}_{p(x)}$. Hence, P is an ideal of $\mathcal{O}_{p(x)}$ and it is the unique maximal ideal since $P = \mathcal{O}_{p(x)} \setminus \mathcal{O}^*_{p(x)}$. Let $\mathcal{O} = \mathcal{O}_{p(x)}$ and $P = P_{p(x)}$. We showed above that P is the unique maximal ideal of $\mathcal{O}$. In fact, it is a principal ideal and generated by $p(x)$ and so $P = p(x)\mathcal{O}$. Since $p(x)$ is a generator for P and if $z \in F(x) \setminus \{0\}$ either z or z^{-1} is in $\mathcal{O}$, we can write $z = p(x)^n(f(x)/g(x))$ for some $n \in \mathbb{Z}$ with $(f(x)/g(x)) \in \mathcal{O}$, $p(x) \nmid f(x)$. In this representation, we associate a function to P, $v_P : F(x) \to \mathbb{Z} \cup \{\infty\}$, as follows: $v_P(z) = n$ for $z \neq 0$ and $v_P(0) = \infty$. Clearly, $v = v_P$ satisfies the discrete valuation properties. Namely,

i. $v(f) = \infty \Leftrightarrow f = 0$, for any $f \in F(x)$.

ii. $v(fg) = v(f) + v(g)$ for any $f,\ g \in F(x)$.

iii. $v(f + g) \geq \min\{v(f), v(g)\}$ for any $f,\ g \in F(x)$.

iv. There exists an element $f \in F(x)$ with $v(f) = 1$.

v. $v(a) = 0$ for any $0 \neq a \in F$.

Being defined by a discrete valuation on $F(x)$, $\mathcal{O}$ is called a *discrete valuation* ring of $F(x)$.

We have similar situation for general function fields.

Definition 1.1.1. *A valuation ring of the function field K/F is a ring $\mathcal{O} \subseteq K$ with the following properties:*

i. *$F \subsetneq \mathcal{O} \subsetneq K$, and*

ii. *For any $0 \neq z \in K$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

Proposition 1.1.2. *([8], Proposition I.1.5, p.2) Let $\mathcal{O}$ be a valuation ring of the function field K/F. Then*

i. *$\mathcal{O}$ is a local ring, i.e. $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^*$, where $\mathcal{O}^* = \{z \in \mathcal{O} \mid$ there is a $w \in \mathcal{O}$ with $zw=1\}$ is the group of units in $\mathcal{O}$.*

ii. *For, $0 \neq x \in K$, $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$.*

iii. *For the field of constants of K/F, $\bar{F} = \{z \in K \mid z$ is algebraic over $F\}$, we have $\bar{F} \subseteq \mathcal{O}$ and $\bar{F} \cap P = \{0\}$.*

Remark 1.1.3. *Let $\mathcal{O}$ be a valuation ring of K/F and P its maximal ideal. Then by Proposition 1.1.2 we have $\mathcal{O} = \{z \in K \mid z^{-1} \notin P\}$. Therefore, we can write $\mathcal{O}_P = \mathcal{O}$ to specify the valuation ring with its unique maximal ideal P.*

Theorem 1.1.4. *([8], Theorem I.1.6, p.3) Let $\mathcal{O}$ be a valuation ring of the function field K/F and P be its unique maximal ideal. Then,*

i. *P is a principal ideal.*

ii. *If $P = t\mathcal{O}$ then any $0 \neq z \in K$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$.*

iii. *$\mathcal{O}$ is a principal ideal domain. More precisely, if $P = t\mathcal{O}$ and $\{0\} \neq I \subseteq \mathcal{O}$ is an ideal, then $I = t^n\mathcal{O}$ for some $n \in \mathbb{N}$.*

Definition 1.1.5. *A prime P of the function field K/F is the maximal ideal of some valuation ring $\mathcal{O}$ of K/F.*

We note that any function field has infinitely many primes.

For each element in the set $\mathbb{P}_K = \{P \mid P$ is a prime of $K/F\}$, we define a function $v_P : K \to \mathbb{Z} \cup \{\infty\}$ such that if $P = t\mathcal{O}$ and for $0 \neq z \in K$, $z = t^n u$ as in the Theorem 1.1.4 we have $v_P(z) = n$ and $v_P(0) = \infty$. We shall note that this function is well defined, that is $v_P(z)$ does not depend on the choice of t. For

$P = t\mathcal{O} = t'\mathcal{O}$ we have $t = t'w$ for some $w \in \mathcal{O}_P^*$ so $z = t^n u = (t'w)^n u = t'^n w^n u$ with $w^n u \in \mathcal{O}_P^*$. Hence, for any choice of t, we have the same function.

By using Theorem 1.1.4, it can be verified that the valuation ring $\mathcal{O}_P$ for the function field K/F is a discrete valuation ring with the discrete valuation v_P of K/F.

Let $z \in K$ and P be a prime of K. We say that P is a *zero* of z of *order* n if $v_P(z) = n > 0$ and P is a *pole* of z of *order* n if $v_P(z) = n < 0$.

Remark 1.1.6. *Suppose $\bar{F}$ is the algebraic closure of F in K then $[\bar{F} : F] = [\bar{F}(x) : F(x)] \leq [K(x) : F(x)] < \infty$, that is, from now on we can assume without loss of generality that for a function field K/F, F is algebraically closed in K. In this case, F is called the constant field of K.*

Lemma 1.1.7. *If $y \in K \backslash F$ then y is transcendental over F and $[K : F(y)] < \infty$.*

Proof. Since F is the constant field of K, y is clearly transcendental over F. For the second part, note that y is algebraic over $F(x)$ so there exists $g(X, Y) \in F[X, Y]$ with $g(x, y) = 0$. Also, X is not a redundant variable in the polynomial g because otherwise we would have y is algebraic over F which is a contradiction. Thus, x is algebraic over $F(y)$ and finally, $[K : F(y)] = [K : F(x, y)][F(x, y) : F(y)] < \infty$, as required. □

For the function field K over its constant field F, let $\mathcal{O}_P$ be a valuation ring with its maximal ideal P. Then, we get the residue class field of P, $F_P = \mathcal{O}_P/P$. Now, Propsition 1.1.2 (iii) yields us a canonical embedding of the field F into the field F_P and we define the *degree* of P as $\deg P = [F_P : F]$.

Proposition 1.1.8. *deg $P = [F_P : F] < \infty$.*

Proof. It is enough to prove that for any $y \in P$, $[F_P : F] \leq [K : F(y)]$ because right hand side of the inequality is finite by Lemma 1.1.7. We will prove this inequality by showing that choosing a linearly independent set for F_P over F leads a linearly independent set for K over $F(y)$. Now, choose $u_1, \ldots, u_m$ such that $\bar{u}_1 = u_1 (\text{mod } P), \ldots, \bar{u}_m (\text{mod } P)$ are linearly independent over F and suppose that

$u_1, \cdots, u_m$ are not linearly independent over $F(y)$. Then, there exists $f_i(y) \in F(y)$ for $i = 1, \ldots, m$ not all zero and $f_1(y)u_1 + \cdots + f_m(y)u_m = 0$. We can also assume, after cancellation, not all $f_i(y)$ are divisible by y. Finally, reducing the equation mod P gives us that $\bar{u}_1, \ldots, \bar{u}_m$ are not linearly independent over F, which is a contradiction and the proposition is proved. □

Example 1.1.9. *Let $F(x)$ be the rational function field with a valuation ring $\mathcal{O} = \mathcal{O}_{p(x)}$ and with a prime $P = P_{p(x)}$. Consider the mapping*

$$\begin{aligned} \phi : F[x] &\rightarrow F(x)_P \\ f(x) &\mapsto f(x) \ mod \ P \end{aligned}$$

First, we will show that ϕ is onto. For $z = f(x)/g(x) \in \mathcal{O}$, let $\bar{z} = z \ mod \ P \in F(x)_P$. Since $z \in \mathcal{O}$, $p(x) \nmid g(x)$ and so there exists $a(x), b(x) \in F[x]$ such that $a(x)p(x) + b(x)g(x) = 1$, or $a(x)p(x)f(x) + b(x)g(x)f(x) = f(x)$. Now,

$$z = \frac{f(x)}{g(x)} = \frac{a(x)p(x)f(x) + b(x)g(x)f(x)}{g(x)} = p(x)\frac{a(x)f(x)}{g(x)} + b(x)f(x)$$

Hence, $b(x)f(x) \in F[x]$ is a pre-image of $\bar{z}$ and the map is onto. Clearly, the kernel of ϕ is the ideal $(p(x))$ and so we have an isomorphism $F[x]/\,(p(x)) \cong F(x)_P$. Using this isomorphism we get

$$deg \ P = [F(x)_P : F] = [F[x]/\,(p(x)) : F] = deg \ p(x)$$

Now, define a subset for $F(x)$

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], \ deg \ f(x) \leq deg \ g(x) \right\}$$

It is easy to show that $\mathcal{O}_\infty$ is a valuation ring with maximal ideal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], \ deg \ f(x) < deg \ g(x) \right\}$$

called the infinite prime. Let $z = f(x)/g(x) \in P_\infty$. Then

$$z = \frac{1}{x}\frac{xf(x)}{g(x)}, \qquad with \ \tfrac{xf(x)}{g(x)} \in \mathcal{O}_\infty$$

which shows $P_\infty = (1/x)\mathcal{O}_\infty$.

Let $\frac{f(x)}{g(x)} = \frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0}{b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0} \in \mathcal{O}_\infty \subset F(x)$ *with* $m \geq n$ *and* $a_n,\ b_m \neq 0$. *Replacing the variable* x *by* $1/x$ *we get* $\frac{f(1/x)}{g(1/x)} \in F(1/x)$. *Note that* $F(x) = F(1/x)$ *and* $\frac{f(1/x)}{g(1/x)} = x^{m-n}\frac{a_0 x^n + a_1 x^{n-1} + \cdots + a_n}{b_0 x^m + b_1 x^{m-1} + \cdots + b_m}$. *Also* $m - n \geq 0$ *and* $b_m \neq 0$ *so* $f(1/x)/g(1/x) \in \mathcal{O}_{p(x)} \subset F(x)$ *with* $p(x) = x$. *Similar argument for* P_∞ *and* $P_{p(x)}$ *concludes the one to one correspondence between infinite prime* P_∞ *and* $P_{p(x)=x}$. *Hence, the discrete valuation of* $F(x)$ *with respect to* P_∞ *is given by*

$$v_\infty(f(x)/g(x)) = deg\ g(x) - deg\ f(x)$$

and $deg\ P_\infty = 1$.

We have observed the primes of $F(x)$ *which correspond to irreducible polynomials* $p(x)$ *and the prime,* P_∞. *In fact, these are the only primes of* $F(x)$. *([8], Theorem I.2.2, p.10)*

1.2 Divisors

In the previos section, we introduced the primes of a given function field K/F. Now, we will define the divisor group of K generated by primes of K. Each element in this group is associated to a vector space over F. Riemann-Roch theorem will be the main result of the section.

Definition 1.2.1. *The group of divisors of* K, *denoted by* $\mathcal{D}_K$, *is the free abelian group generated by the primes of* K/F.

For a divisor D, in the group $\mathcal{D}_K$ we have a unique representation

$$D = \sum_{P \in \mathbb{P}_K} n_P P,\ n_P \in \mathbb{Z},\ \text{almost all } n_P = 0$$

In this group, two elements are added coefficientwise (coefficients corresponding to the same prime P are added) and the zero element is

$$0 = \sum_{P \in \mathbb{P}_K} n_P P,\ \text{all } n_P = 0$$

The coefficients in the representation are uniquely determined by that divisor so we define for $D = \sum_P n_P P$ and for $P \in \mathbb{P}_K$, $v_P(D) = n_P$. Also,

$$\deg\ D\ = \sum_{P \in \mathbb{P}_K} v_P(D) \deg\ P$$

and by definition,

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ for all } P \in \mathbb{P}_K$$

A divisor D is called *effective* if $D \geq 0$.

Remark 1.2.2. The degree map $\deg\ : D \mapsto \deg\ D$ from $\mathcal{D}_K$ to $\mathbb{Z}$ is a homomorphism and its kernel is the group of *divisors of degree zero*, which is denoted by $\mathcal{D}_K^0$

Definition 1.2.3. *Let $0 \neq z \in K$. The divisor of z, the divisor of zeros of z and the divisor of poles of z are defined respectively as,*

$$\begin{aligned}
(z) &= \sum_P v_P(z) P \\
(z)_0 &= \sum_{\substack{P \\ v_P(z) > 0}} v_P(z) P \\
(z)_\infty &= \sum_{\substack{P \\ v_P(z) < 0}} (-v_P(z)) P
\end{aligned}$$

The above definition makes sense because any $0 \neq z \in K$ has only finitely many zeros and poles. ([8], Corollary I.3.4, p.14).

Now, consider the homomorphism $z \to (z)$ from K^* to $\mathcal{D}_K$. The image of this homomorphism is a subgroup of $\mathcal{D}_K$ and it is called the group of *principal divisors* of K/F and denoted by $\mathcal{P}_K$. The factor group $\mathcal{C}_K = \mathcal{D}_K/\mathcal{P}_K$ is called the *divisor class group*. Two divisors D_1, $D_2 \in \mathcal{D}_K$ are said to be *equivalent*, or *linearly equivalent* if $D_1 = D_2 + (z)$ for some $z \in K^*$. In this case, we write $D_1 \sim D_2$ or $[D_1] = [D_2]$ to indicate that D_1 and D_2 represent the same divisor class.

Remark 1.2.4. *If D_1 and D_2 are two divisors in the same class, then deg D_1 = deg D_2, since the degree of a principal divisor is zero ([8], Theorem I.4.11, p.18). Hence, generalizing the degree map from $\mathcal{C}_K$ to $\mathbb{Z}$ we get a homomorphism with kernel equal to the group of* divisor classes of degree zero*, which is denoted by $\mathcal{C}_K^0$.*

Example 1.2.5. *Let $K = F(x)$ be the rational function field and $z = f(x)/g(x) \in K$. We know that the primes of K are $P_{p(x)}$ and P_∞. Then, writing z as a product of irreducible polynomials over F*

$$z = \frac{f(x)}{g(x)} = \frac{p_1^{n_1}(x)p_2^{n_2}(x)...p_k^{n_k}(x)}{q_1^{m_1}(x)q_2^{m_2}(x)...q_l^{m_l}(x)}$$

we find $v_{P_i}(z) = n_i$, $v_{Q_j}(z) = -m_j$, $v_\infty(z) = (\sum m_j - \sum n_i)$ where P_i and Q_j are the primes corresponding to p_i and q_j, respectively. Note that at any other prime P, $v_P(z) = 0$. Thus,

$$(z) = \sum_{i=1}^{k} n_i P_i - \sum_{j=1}^{l} m_j Q_j + \left(\sum_{j=1}^{l} m_j - \sum_{i=1}^{k} n_i \right) P_\infty$$

and deg $(z) = 0$.

Definition 1.2.6. *For a divisor $D \in \mathcal{D}_K$ we define*

$$\mathscr{L}(D) = \{x \ \in \ K^* \ \mid \ (x) + D \geq 0 \ \} \cup \{0\}.$$

Let $x, y \in \mathscr{L}(D)$ and $D = \sum_i d_i P_i$. Then, $v_{P_i}((x)) \geq -d_i$ and $v_{P_i}((y)) \geq -d_i$ for all i. By the property of the valuation we can write

$$v_{P_i}((x+y)) \geq min\{v_{P_i}((x)),\ v_{P_i}((y))\} \geq -d_i$$

that is $x + y \in \mathscr{L}(D)$. Also, for $0 \neq a \in F$ we have $ax \in \mathscr{L}(D)$ since $v_{P_i}((ax)) = v_{P_i}((x)) \geq -d_i$. Hence, $\mathscr{L}(D)$ is a vector space over F. In fact, it is a finite dimensional vector space and its dimension is denoted by $l(D)$ ([8], Proposition I.4.9, p.18).

Now, we will write the Riemann-Roch Theorem which will be very helpful to classify function fields.

Theorem 1.2.7. *(Riemann-Roch)([6], Theorem 5.4, p.49) Let K be an algebraic function field. Then, there is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $D \in \mathcal{D}_K$ we have*

$$l(D) = deg(D) - g + 1 + l(C - D)$$

The constant g in the above equation is called the *genus* of the function field K.

Suppose $\mathscr{L}(D) \neq \{0\}$. Then, there exists $x \in K^*$ such that $(x) \geq -D$ implying $0 = \deg((x)) \geq \deg(-D) = -deg(D)$. Hence, we proved

$$\text{if } \deg(D) < 0 \text{ then } \mathscr{L}(D) = \{0\} \text{ and } l(D) = 0$$

If D_1 and D_2 are linearly equivalent divisors then there exists $x \in K$ such that $D_1 = D_2 + (x)$. Let $x_2 \in D_2$ and define $x_1 = x_2/x$. Then, $(x_1) = (x_2) - (x) \geq -(D_2 + (x)) = -D_1$ proving that $x_1 \in D_1$. Similarly, for $x_1 \in D_1$ we get $x_2 = x_1 x \in D_2$. Hence, the map

$$\begin{aligned} \mathscr{L}(D_1) &\rightarrow \mathscr{L}(D_2) \\ x_1 &\mapsto x x_1 \end{aligned}$$

is surjective. Clearly, this is a homomorphism with kernel 0 and proves for linearly equivalent divisors D_1 and D_2

$$\mathscr{L}(D_1) \simeq \mathscr{L}(D_2) \text{ and } l(D_1) = l(D_2).$$

In the Riemann-Roch equation, putting $D = 0$ we get $l(0) - l(C) = \deg 0 - g + 1$, that is

$$l(C) = g.$$

and putting $D = C$ we get

$$\deg(C) = 2g - 2.$$

Finally, if $\deg D > 2g - 2$, then $\deg(C - D) < 0$, that is $l(C - D) = 0$ and

$$l(D) = \deg D - g + 1.$$

Example 1.2.8. *Let $F(x)$ be the rational function field with prime P_∞ of degree 1. Suppose $z = f(x)/g(x) \in \mathscr{L}(nP_\infty)$, that is, $v_{P_\infty}((z)) \geq -n$ and $v_P((z)) \geq 0$ for any prime $P \neq P_\infty$. If*

$$z = \frac{f(x)}{g(x)} = \frac{p_1^{n_1}(x)p_2^{n_2}(x)...p_k^{n_k}(x)}{q_1^{m_1}(x)q_2^{m_2}(x)...q_l^{m_l}(x)}$$

for irreducible polynomials p_i and q_j over F, we must have $\sum_j m_j = 0$, each n_i is non-negative and $\sum_i n_i \leq n$ (cf. Example 1.2.5). Hence, z is a polynomial over F of degree $\leq n$. Conversely, if z is a polynomial of degree $\leq n$, it is clear that $z \in \mathscr{L}(nP_\infty)$. Thus, $\mathscr{L}(nP_\infty)$ is generated by $\{1, x, \cdots, x^n\}$ and $l(nP_\infty) = n + 1$.

Example 1.2.9. *Let $F(x)$ be a rational function field of genus g with a prime divisor P_∞ of degree 1. Choosing $n \in \mathbb{Z}^+$ big enough we guarantee that $deg(nP_\infty) = n > 2g - 2$. Then, $l(nP_\infty) = n - g + 1$ and by Example 1.2.8 $l(nP_\infty) = n + 1$. Hence, the genus of a rational function field is $g = 0$. Now, suppose K is a function field of genus 0 with a prime divisor P of degree 1. Then, deg $P = 1 > 2g - 2 = -2$ and so $l(P) = deg(P) - g + 1 = 2$, that is, there exists a non-constant $x \in K$ such that $(x) + P \geq 0$. Note that $deg((x) + P) = 1$ which implies $(x) + P = Q$ for some prime Q of degree 1, or $(x) = Q - P$. By ([6], Proposition 5.1, p.47), we conclude $[K : F(x)] =$deg $(x)_0 = 1$ and $K = F(x)$.*

1.3 Prime Decompositions in Function Field Extensions

In this section, we assume that K is a function field over its constant field F which is perfect and L is a finite, extension of K with constant field E. Let P be a prime in K and $\mathcal{O}_P$ the associated discrete valuation ring. Similarly, let $\mathfrak{P}$ be a prime in L with discrete valuation ring $\mathcal{O}_\mathfrak{P}$. We say $\mathfrak{P}$ *lies above* P if $\mathcal{O}_P = \mathcal{O}_\mathfrak{P} \cap K$ and $P = \mathfrak{P} \cap K$. In this case, we get $P\mathcal{O}_\mathfrak{P} = \mathfrak{P}^e$ and the integer $e = e(\mathfrak{P}/P) \geq 1$ is called the *ramification index*. Also, we define $f = [\mathcal{O}_P/P : \mathcal{O}_\mathfrak{P}/\mathfrak{P}]$ and $f = f(\mathfrak{P}/P)$ is called the *relative degree*. If the extension L/K is Galois then its Galois group

will be denoted by $G = \mathrm{Gal}(L/K)$. Now, let $\{\mathfrak{P}_1, ..., \mathfrak{P}_g\}$ is the set of all primes in L lying above P such that each $\mathfrak{P}_i$ has the ramification index e_i and the relative degree f_i. Then, we have

Proposition 1.3.1. *([6], p.79) Assume L/K is a finite, separable extension of fields. Then, $\sum_{i=1}^{g} e_i f_i = [L : K]$.*

$\mathfrak{P}$ is *unramified* over P if $e(\mathfrak{P}/P) = 1$. Otherwise, $\mathfrak{P}$ is *ramified* over P. A prime P in K *splits completely* in L if there are $n = [L : K]$ primes in L lying above P. Using the above proposition we conclude P splits completely in L if and only if $e_i = f_i = 1$ for $i = 1, ..., n$. Our aim is to caharacterize the splitting behaviour of primes in K over the Galois extensions $[L : K]$.

Proposition 1.3.2. *Let K be a function field over its constant field F. Let L be a finite Galois extension of K with Galois group G and constant field E.*

- ***i.*** *The restriction map, which is obtained by restriction of automorphisms of G to E, $G \to Gal(E/F)$ is onto and the extension E/F is Galois.*
- ***ii.*** *If N is the kernel of this map then the fixed field of N is KE, the maximal constant field extension of K contained in L.*

Proof. Let $\sigma \in G$ and $\alpha \in E$. Because α is algebraic over F and σ fixes K we get that $\sigma\alpha$ is also algebraic over F, that is $\sigma\alpha \in E$. Hence, the restriction of an automorhism σ to E gives an automorphism in $Aut(E/F)$, say $res(\sigma)$. Now, the fixed field of the set $\{res(\sigma) \ : \sigma \in G\}$ is $E \cap K = F$ and which proves part (i).
Let N' be the fixed field of N. N fixes KE by definition so we have $|N| = [L : N'] \leq [L : KE]$. On the other hand, $G/N \cong \mathrm{Gal}(E/F)$ that is $[L : K] = |G| = |N|\,|\mathrm{Gal}(E/F)| = |N|\,[E : F]$. Finally, using $[E : F] = [KE : K]$([6], Proposition 8.1, p.102) we get $|N| = [L : KE]$, that is $N' = KE$. □

Next we look at the action of the Galois group on the primes of L lying above P.

Proposition 1.3.3. *([6], Proposition 9.2, p.117) Let* $\{\mathfrak{P}_1, ..., \mathfrak{P}_g\}$ *be the set of primes of* L *lying above* P*. The Galois group* G *acts transitively on this set.*

Proposition 1.3.4. *Let* $\sigma \in G$*,* P *be a prime ideal of* K*,* $\mathfrak{P}$ *be a prime ideal in* L *lying above* P *and* $\sigma\mathfrak{P} = \mathfrak{P}'$*. Then,* $\sigma O_{\mathfrak{P}}$ *is a discrete valuation ring with maximal ideal* $\sigma\mathfrak{P}$*, that is* $\sigma O_{\mathfrak{P}} = O_{\mathfrak{P}'}$*.*

Proof. Let $x \in \sigma O_P$, that is $\sigma^{-1}x \in O_P$ implying $(\sigma^{-1}x)^{-1} = \sigma^{-1}x^{-1} \notin P$. It follows that $x^{-1} \notin \sigma P$ and so $x \in O_{\sigma\mathfrak{P}} = O_{\mathfrak{P}'}$.
Conversely, if $x \in O_{\mathfrak{P}'}$ then $x^{-1} \notin \mathfrak{P}' = \sigma\mathfrak{P}$, that is $\sigma^{-1}x^{-1} = (\sigma^{-1}x)^{-1} \notin \mathfrak{P}$ implying $\sigma^{-1}x \in O_{\mathfrak{P}}$, or $x \in \sigma O_{\mathfrak{P}}$. This proves the proposition. □

Proposition 1.3.5. *Let the number of the primes in* L *lying above* P *be* $g(P)$*. We have* $f(\mathfrak{P}_i/P) = f(\mathfrak{P}_j/P) = f(P)$*,* $e(\mathfrak{P}_i/P) = e(\mathfrak{P}_j/P) = e(P)$ *for all* $1 \leq i, j \leq g$ *and* $e(P)f(P)g(P) = n = [L : K]$*.*

Proof. For given $\mathfrak{P}_i$ and $\mathfrak{P}_j$ there is an isomorphism σ such that $\sigma\mathfrak{P}_i = \mathfrak{P}_j$. If $x \in O_{\mathfrak{P}_i}$ then $\sigma x \in \sigma O_{\mathfrak{P}_i} = O_{\mathfrak{P}_j}$. Also, if $y \in O_{\mathfrak{P}_j} = \sigma O_{\mathfrak{P}_i}$ then $\sigma^{-1}y \in O_{\mathfrak{P}_i}$. Therefore, we have an onto homomorphism $O_{\mathfrak{P}_i} \to O_{\mathfrak{P}_j}$ given by $x \mapsto \sigma x$.
Now, consider $O_{\mathfrak{P}_i} \to O_{\mathfrak{P}_j}/\mathfrak{P}_j$, by $x \mapsto \overline{\sigma x}$ which is an onto homomorphism with kernel, say N. Let $x \in N$ then $\overline{\sigma x} = 0$, that is $\sigma x \in \mathfrak{P}_j$. It follows that $x \in \sigma^{-1}\mathfrak{P}_j = \mathfrak{P}_i$ and $N \subset \mathfrak{P}_i$. Conversely, if $x \in \mathfrak{P}_i$ then $\sigma x \in \sigma\mathfrak{P}_i = \mathfrak{P}_j$, implying $\overline{\sigma x} = 0$. Hence, $N = \mathfrak{P}_i$ and we have an isomorphism

$$\begin{array}{ccc} O_{\mathfrak{P}_j}/\mathfrak{P}_j & \to & O_{\mathfrak{P}_j}/\mathfrak{P}_j \\ \overline{x} & \mapsto & \overline{\sigma x} \end{array}$$

Clearly, this is a well defined map and proves that $f(\mathfrak{P}_i/P) = f(\mathfrak{P}_j/P) = f(P)$. Also, if $PO_{\mathfrak{P}_i} = \mathfrak{P}_i^e$ applying σ to both sides we get $PO_{\mathfrak{P}_j} = \mathfrak{P}_j^e$. Finally, using $\sum_{i=1}^{g(P)} e(\mathfrak{P}_i/P)f(\mathfrak{P}_j/P) = n$ concludes $e(P)f(P)g(P) = n = [L : K]$. □

Definition 1.3.6. *Let* $\mathfrak{P}$ *be a prime of* L *lying above a prime* P *of* K*. Then, two subgroups of* G*, the* decomposition group *of* $\mathfrak{P}$ *over* P *and the* inertia group *of* $\mathfrak{P}$

over P are defined respectively as

$$Z(\mathfrak{P}/P) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$
$$I(\mathfrak{P}/P) = \{\tau \in G \mid \tau x \equiv x (mod \mathfrak{P}) \text{ for all } x \in O_{\mathfrak{P}}\}$$

If we consider the group G as acting on the set of primes of L lying above P then the decomposition group of $\mathfrak{P}$ over P is the stabilizer of $\mathfrak{P}$ and by ([2], Theorem 4.3, p.89) we have $[G : Z(\mathfrak{P}/P)] = g(P)$. Now using Proposition 1.3.5 we conclude the following

$$|Z(\mathfrak{P}/P)| = e(\mathfrak{P}/P)f(\mathfrak{P}/P) \tag{1.1}$$

Proposition 1.3.7. *Let $M \subseteq L$ be the fixed field of $Z(\mathfrak{P}/P)$ and $\mathfrak{p}$ the prime M lying below $\mathfrak{P}$. Then $\mathfrak{P}$ is the only prime in L lying above $\mathfrak{p}$. Moreover, $e(\mathfrak{p}/P) = f(\mathfrak{p}/P) = 1$ and $[M : K] = g(P)$.*

Proof. The field extension $[L : M]$ is a Galois extension with the Galois group $Z(\mathfrak{P}/P)$. We know by Proposition 1.3.3 that the set of primes of L lying above $\mathfrak{p}$ are of the form $\sigma\mathfrak{P}$ for $\sigma \in Z(\mathfrak{P}/P)$. However, $\sigma\mathfrak{P} = \mathfrak{P}\ \forall\ \sigma \in Z(\mathfrak{P}/P)$. This proves $\mathfrak{P}$ is the only prime in L lying above $\mathfrak{p}$. For the rest of the lemma

$$\begin{aligned} Z(\mathfrak{P}/\mathfrak{p}) &= Z(\mathfrak{P}/P) \\ \Rightarrow e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) &= e(\mathfrak{P}/P)f(\mathfrak{P}/P) \\ \Rightarrow e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) &= e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/P)f(\mathfrak{P}/\mathfrak{p})f(\mathfrak{p}/P) \\ \Rightarrow e(\mathfrak{p}/P) &= f(\mathfrak{p}/P) = 1 \end{aligned}$$

and finally,

$$\begin{aligned} [L : K] &= [L : M][M : K] \\ \Rightarrow |G| &= |Z(\mathfrak{P}/\mathfrak{p})|\,[M : K] \\ \Rightarrow [M : K] &= g(P). \end{aligned}$$

□

Theorem 1.3.8. *([6], Theorem 9.6, p.118) Let $E_{\mathfrak{P}}$ be the residue class field of $O_{\mathfrak{P}}$ and F_P be the residue class field of O_P. Suppose L/K is a Galois extension with $G = Gal(L/K)$ and that $\mathfrak{P}$ is a prime of L lying over a prime $P$of K. Then the extension $E_{\mathfrak{P}}/F_P$ is also a Galois extension. There is a natural homomorphism from $Z(\mathfrak{P}/P)$ onto $Gal(E_{\mathfrak{P}}/F_P)$ and the kernel of this homomorphism is $I(\mathfrak{P}/P)$. The inertia group is a normal subgroup of the decompositon group and $\#I(\mathfrak{P}/P) = e(P/P)$.*

Corollary 1.3.9. *If $\mathfrak{P}/P$ is unramified, then $Z(\mathfrak{P}/P) \cong Gal(E_{\mathfrak{P}}/F_P)$.*

Proposition 1.3.10. *Suppose L/K is a Galois extension of function fields and suppose $\mathfrak{P}$ is a prime of L lying above a prime P of K. Let $\sigma \in Gal(L/K)$. Then, $Z(\sigma\mathfrak{P}/P) = \sigma Z(\mathfrak{P}/P)\sigma^{-1}$ and $I(\sigma\mathfrak{P}/P) = \sigma I(\mathfrak{P}/P)\sigma^{-1}$.*

Proof. We have, $\tau \in Z(\sigma\mathfrak{P}/P) \Leftrightarrow \tau\sigma\mathfrak{P} = \sigma\mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\sigma\mathfrak{P} = \mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\sigma \in Z(\mathfrak{P}/P) \Leftrightarrow \tau \in \sigma Z(\mathfrak{P}/P)\sigma^{-1}$, as required. □

Recalling the Proposition 1.3.3, we conclude the following corollary

Corollary 1.3.11. *All the decomposition groups of primes above P in L are conjugate and similiarly for the inertia groups.*

Proposition 1.3.12. *Let L/K be a Galois extension of function fields and M an arbitrary intermediate field. Let $\mathfrak{P}$ be a prime of L and $\mathfrak{p}$ and P the primes of M and K respectively which lie below $\mathfrak{P}$. Set $H = Gal(L/M)$. Then,*

i. *$Z(\mathfrak{P}/\mathfrak{p}) = H \cap Z(\mathfrak{P}/P)$ and $I(\mathfrak{P}/\mathfrak{p}) = H \cap I(\mathfrak{P}/P)$.*

Now, assume H is a normal subgroup and let $res : Gal(L/K) \to Gal(M/K)$ be the restriction map. Then,

ii. *$res(Z(\mathfrak{P}/P)) = Z(\mathfrak{p}/\mathfrak{P})$ and $res(I(\mathfrak{P}/P)) = I(\mathfrak{p}/\mathfrak{P})$.*

Proof. i. Let $\sigma \in Z(\mathfrak{P}/\mathfrak{p})$. Then, by definition $\sigma \in H$. Also, $\sigma \in Z(\mathfrak{P}/P)$ since $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$ and σ fixes $\mathfrak{P}$. Converse inclusion is clear.
(ii) Consider the map $res : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ and let $\sigma \in Z(\mathfrak{P}/P)$. Then

$\tau = res(\sigma) \in \mathrm{Gal}(M/K)$ and so $\tau\mathfrak{p} = \mathfrak{p}$, that is $\tau \in Z(\mathfrak{p}/P)$. Thus, by restricting the map res onto $Z(\mathfrak{P}/P)$ we get $res|_Z : Z(\mathfrak{P}/P) \to Z(\mathfrak{p}/P)$ with kernel $Z(\mathfrak{P}/P) \cap H = Z(\mathfrak{P}/\mathfrak{p})$. This gives,

$$\begin{aligned} \#res|_Z(Z(\mathfrak{P}/P)) &= e(\mathfrak{P}/P)f(\mathfrak{P}/P)/e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) \\ &= e(\mathfrak{p}/P)f(\mathfrak{p}/P) \\ &= \#Z(\mathfrak{p}/P) \end{aligned}$$

and proves ii. □

Lemma 1.3.13. *Let L/K be a Galois extension of function fields and $\mathfrak{P}$ a prime of L lying above a prime P of K. Then, P splits completely in L if and only if $Z(\mathfrak{P}/P) = (e)$.*

Proof. Suppose P splits completely in L By definition, there are $n = [L : K]$ primes above it in L and using Proposition 1.3.5 we get $e(\mathfrak{P}/P) = f(\mathfrak{P}/P) = 1$ for all primes $\mathfrak{P}$ of L lying above P. Now, using Equation (1.1) we conclude $Z(\mathfrak{P}/P) = (e)$ for all such $\mathfrak{P}$. Conversely, assume that $Z(\mathfrak{P}/P) = (e)$ for a prime $\mathfrak{P}$ of L lying above P. Then, by Equation (1.1) $e(\mathfrak{P}/P) = f(\mathfrak{P}/P) = 1$. In fact, by Proposition 1.3.5, this is true for all primes of L lying above P and so there are $[L : K]$ primes of L lying above P. □

Theorem 1.3.14. *Let M_1 and M_2 be two Galois extensions of a function field K and let $L = M_1M_2$ be the compositium. A prime P of K spilits completely in L if and only if it splits copletely in M_1 and M_2. A prime P of K is unramified in L if and only if it is unramified in M_1 and M_2.*

Proof. Let $\mathfrak{P}$ be a prime of L lying above P and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ the primes of M_1 and M_2, respectively, lying below $\mathfrak{P}$. Suppose P splits completely in L, then Lemma 1.3.13 tells us that $Z(\mathfrak{P}/P) = (e)$. Now, using Propositon 1.3.12 (ii) we get $Z(\mathfrak{p}_1/P) = Z(\mathfrak{p}_2/P) = (e)$. Again by Lemma 1.3.13, P splits completely in M_1 and M_2.

Conversely, suppose P splits completely in M_1 and M_2. Then, $Z(\mathfrak{p}_1/P) = Z(\mathfrak{p}_2/P) =$

(e). For any $\sigma \in Z(\mathfrak{P}/P)$, the restriction of σ to M_1 and M_2 is identity by Proposition 1.3.12. It follows that σ is identity because $L = M_1M_2$, that is $Z(\mathfrak{P}/P) = (e)$ or equivalently P splits completely in L.

Unramified case can be proven similiarly.

□

CHAPTER 2

Global Function Fields and the Zeta Function

2.1 Global Function Fields

A function field over a finite constant field is called a *global function field*. From now on, we will assume that K is a global function field over its constant field $\mathbb{F}$ with q elements. In this section, we will invstigate the zeta function of K and conclude with the Riemann Hypothesis for global function fields.

Lemma 2.1.1. *For any integer $n \geq 0$ the number of effective divisors of degree n is finite.*

Proof. We know that except for one prime, each prime of the rational function field $\mathbb{F}(x)$ corresponds to a monic irreducible polynomial in $\mathbb{F}(x)$. This shows that there are only finitely many primes of $\mathbb{F}(x)$ of a fixed degree. On the other hand, for any prime P in $\mathbb{F}(x)$ there are only finitely many primes of $\mathfrak{P}$ of K that lie above P and we always have deg $\mathfrak{P} \geq$ deg P. Hence, there are only finitely many primes of K of any fixed degree. Now, let $D = \sum_P v_P(D)P$ be an effective divisor of degree n. Then, for each prime P in the summand we must have deg $P \leq n$ and also $v_P(D) \leq n$. Finally, using the above arguments, this combination gives finitely many effective divisors of degree n. □

Lemma 2.1.2. *The number of divisor classes of degree zero is finite.*

Proof. Let D be a divisor of degree 1 and for a divisor, A of degree zero, consider the vector space $\mathscr{L}(gD+A)$. By Theorem 1.2.7, $l(gD+A) = \deg(gD+A) - g + 1 = 1$ and so there exists a nonzero $f \in \mathscr{L}(gD+A)$. Now, setting $B = (f) + gD + A$ we get $A \sim B - gD$ where B is an effective divisor of degree g. This equivalence relation shows that the number of divisor classes of degree zero is bounded above by the number of effective divisors of degree g, say b_g. We have already proved the finiteness of b_g in the above lemma, this completes the proof. □

The number of divisor classes of degree zero is called the *class number* of K and it is denoted by h_K.

Lemma 2.1.3. *For a divisor A, the class of A, $[A]$, contains effective divisors if and only if $l(A) > 0$.*

Proof. Suppose $B \in [A]$ is an effective divisor. Then, there exists $f \in K^*$ such that $(f) + A = B \geq 0$, that is $f \in \mathscr{L}(A)$ and $l(A) > 0$. Conversely, supose $l(A) > 0$. Then, there exists a nonzero f in $\mathscr{L}(A)$, that is $(f) + A \geq 0$. Hence, $B = (f) + A$ is an effective divisor in $[A]$, as required. □

Lemma 2.1.4. *For any divisor A, the number of effective divisors in $[A]$ is $\frac{q^{l(A)}-1}{q-1}$.*

Proof. By Lemma 2.1.3 we can assume $l(A) > 0$. Consider the mapping

$$\begin{array}{ccccc} \phi & : & \mathscr{L}(A) - \{0\} & \rightarrow & \{D \in [A] \mid D \geq 0\} \\ & & (x) & \mapsto & (x) + A \end{array}$$

For any $D \in [A]$ with $D \geq 0$ we have $D = A + (x) \geq 0$ and so $x \in \mathscr{L}(A)$. This shows the map is surjective. If $\phi(x) = \phi(y)$ then $(x) - (y) = 0$ and that means x and y differ by a nonzero constant. Equivalently, $q-1$ different elements are mapped to one element under ϕ. Hence, the cardinality of the image is $\frac{q^{l(A)}-1}{q-1}$. □

Lemma 2.1.5. *([6], p.50) For any integer $n \geq 0$, there are exactly h_K divisor classes of degree n.*

2.2 The Zeta Function of a Global Function Field

In this section K is assumed to be a global function field with genus g over its constant field $\mathbb{F}$ with q elements and $h = h_K$ is the class number of the field K.

Definition 2.2.1. *The zeta function of K is defined as*

$$\zeta_K(s) = \sum_{D \geq 0} ND^{-s}$$

where s is a complex variable and the sum is taken over all positive divisors in D_K and for $D \in D_K$, $ND = q^{deg(D)}$.

We will see in Theorem 2.2.4 that $\zeta_K(s)$ is convergent for $\Re(s) > 1$.

Lemma 2.2.2. *Suppose $n \geq 0$ and let $\{[D_1], [D_2], \cdots, [D_h]\}$ be the divisor classes of degree n. Define*

$$b_n = \#\{D \ \geq \ 0 \ \mid \ deg(D) \ = \ n \ \}$$

If $n > 2g - 2$ then,

$$b_n = h\frac{q^{n-g+1} - 1}{q - 1}$$

Proof. First of all let $n \geq 0$ then by Lemma 2.1.4 and Lemma 2.1.5 we get

$$b_n = \sum_{i=1}^{h} \frac{q^{l(D_i)} - 1}{q - 1}$$

Now, assume also that $n > 2g - 2$. Then we get from the results following Theorem 1.2.7, $l(D_i) = \deg(D_i) - g + 1 = n - g + 1$ for all $i = 1, \cdots, h$ and the result follows. □

We can rewrite the zeta function as

$$\zeta_K(s) = \sum_{D \geq 0} q^{-sdeg(D)} = \sum_{n=1}^{\infty} b_n q^{-ns}$$

and making the change of variable $t = q^{-s}$ leads to the following equivalent definition of the zeta function.

Definition 2.2.3.

$$\zeta_K(s) = Z_K(t) = \sum_{n=0}^{\infty} b_n t^n$$

Theorem 2.2.4. *Let $K/\mathbb{F}$ be global function field with genus g. Then, $Z_K(t)$ is convergent for $|t| < 1/q$ and one has*

i. *If $g = 0$ then $Z_K(t) = \frac{1}{q-1}(\frac{q}{1-qt} - \frac{1}{1-t})$*

ii. *If $g \geq 1$ then $Z_K(t) = F(t) + G(t)$*

where

$$\begin{aligned} F(t) &= \frac{1}{q-1} \sum_{\substack{[D] \\ 0 \leq deg(D) \leq 2g-2}} q^{l([D])} t^{deg[D]} \\ G(t) &= \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2t}\frac{1}{1-qt} - \frac{1}{1-t}\right) \end{aligned}$$

Proof. i. First, we will prove that if $g = 0$ then every divisor of degree zero is a principal divisor, that is, $h = 1$. Let $D \in D_K$ and $\deg(D) = 0$. Then, $l(D) \geq \deg(D) + 1 - g = 1$ and so there exists $0 \neq x \in \mathscr{L}(D)$, i.e, $(x) \geq -D$. Also, note that $\deg((x)) = \deg(D) = 0$. Hence, we must have $(x) = -D$, proving our claim. Now, using Lemma 2.2.2 with $h = 1$ and $g = 0$ we can write

$$\begin{aligned} Z_K(t) &= \sum_{n=0}^{\infty} b_n t^n = \sum \frac{1}{q-1}(q^{n+1} - 1)t^n \\ &= \frac{1}{q-1}\left(q\sum_{n=0}^{\infty} q^n t^n - \sum_{n=0}^{\infty} t^n\right) \\ &= \frac{1}{q-1}\left(\frac{q}{1-qt} - \frac{1}{1-t}\right) \quad \text{for } |qt| < 1. \end{aligned}$$

ii. Suppose $g \geq 1$. Then,

$$
\begin{aligned}
Z_K(t) &= \sum_{n=0}^{\infty} b_n t^n = \sum_{\substack{[D] \\ deg[D] \geq 0}} \frac{q^{l([D])} - 1}{(q-1)} t^{deg[D]} \\
&= \frac{1}{q-1} \sum_{\substack{[D] \\ 0 \leq deg[D] \leq 2g-2}} q^{l([D])} t^{deg[D]} + \\
&\quad \frac{1}{q-1} \sum_{\substack{[D] \\ deg[D] > 2g-2}} q^{l([D])} t^{deg[D]} - \frac{1}{q-1} \sum_{\substack{[D] \\ deg[D] \geq 0}} t^{deg[D]}
\end{aligned}
$$

□

In the above equation, calling the first term $F(t)$ and calling the sum of the last two terms $G(t)$ we prove the theorem since

$$
\begin{aligned}
(q-1)G(t) &= \sum_{n=2g-1}^{\infty} hq^{n+1-g} - \sum_{n=0}^{\infty} ht^n \\
&= h\left(q^{1-g}(qt)^{2g-2} \sum_{n=0}^{\infty} (qt)^n\right) - h\frac{1}{1-t}
\end{aligned}
$$

and the above equation, therefore $F(t) + G(t)$, is convergent for $|qt| < 1$.

Theorem 2.2.5. *The zeta function of a function field K over $\mathbb{F}$ has Euler product*

$$
Z_K(t) = \prod_{P \in \mathbb{P}_K} \left(1 - t^{degP}\right)^{-1} \qquad for\ |t| < q^{-1}
$$

Proof. Since

$$
\sum_{P \in \mathbb{P}_K} t^{degP} < \sum_{D \geq 0} t^{degD} = Z_K(t) < \infty \qquad for\ |t| < q^{-1}
$$

we get that $\prod_{P \in \mathbb{P}_K} \left(1 - t^{degP}\right)^{-1}$ is absolutely convergent for $|t| < q^{-1}$.

Now,

$$\begin{aligned}\prod_{P\in\mathbb{P}_K}\left(1-t^{degP}\right)^{-1} &= \prod_{P\in\mathbb{P}_K}\left(\sum_{n=0}^{\infty}t^{ndegP}\right)\\ &= \prod_{P\in\mathbb{P}_K}\left(\sum_{n=0}^{\infty}t^{deg(nP)}\right)\\ &= \sum_{D\geq 0}t^{degD}\\ &= Z_K(t)\end{aligned}$$

□

Example 2.2.6. *In this example, we will investigate the zeta function of the rational function field $\mathbb{F}(x)$ where $\mathbb{F}$ is a finite field with q elements. Recall that the primes, $P \in \mathbb{F}(x)$ (except for the prime at infinity, P_∞) are in one to one correspondence with the monic irreducible polynomials $p(x) \in \mathbb{F}[x]$. We have deg P = deg $p(x)$ and deg $P_\infty = 1$. Then, we can write*

$$\begin{aligned}\zeta_{\mathbb{F}(x)}(s) &= \prod_{P\in\mathbb{P}_{\mathbb{F}(x)}}(1-q^{-sdegP})^{-1}\\ &= (1-q^{-s})^{-1}\prod_{\substack{p(x)\in\mathbb{F}[x]\\ monic,\ irreducible}}(1-q^{-sdegp(x)})^{-1}\end{aligned}$$

Now, define the norm of a function as $\mid p(x) \mid = q^{deg\ p(x)}$. Using the multiplicativity of this function and the unique decomposition of polynomials into product of irreducible polynomials we get

$$\begin{aligned}\zeta_{\mathbb{F}(x)}(s) &= (1-q^{-s})^{-1}\prod_{\substack{p(x)\in\mathbb{F}[x]\\ monic, irreducible}}(1-\mid p(x)\mid^{-s})^{-1}\\ &= (1-q^{-s})^{-1}\sum_{\substack{f(x)\in\mathbb{F}[x]\\ monic}}\mid f(x)\mid^{-s}\end{aligned}$$

Note that there are exactly q^d monic polynomials of degree d. Hence,

$$\zeta_{\mathbb{F}(x)}(s) = (1-q^{-s})^{-1}(\sum_{d=0}^{\infty} \frac{q^d}{q^{ds}}) = (1-q^{-s})^{-1}(1-q^{1-s})^{-1}$$

Theorem 2.2.7. *Let K be a function field of genus g over its constant field $\mathbb{F}$ with q elements. Let $t = q^{-s}$. Then there is a polynomial $L_K(t) \in \mathbb{Z}[t]$ of degree $2g$ such that*

$$\zeta_K(s) = \frac{L_K(t)}{(1-t)(1-qt)}$$

for all $\Re(s) > 1$. The function $\zeta_K(s)$ has simple poles at $s = 0$ and $s = 1$, $L_K(0) = 1$, $L_K(1) = h$ and $L'_K(0) = a_1 - 1 - q$ where a_1 is the number of primes of degree 1 in K.

Proof. We know that for $n > 2g-2$, $b_n = h\frac{q^{n-g+1}-1}{q-1}$. Then,

$$\begin{aligned}
Z_K(t) &= \sum_{n=0}^{2g-2} b_n t^n + \sum_{n=2g-1}^{\infty} h\frac{q^{n-g+1}-1}{q-1}t^n \\
&= \sum_{n=0}^{2g-2} b_n t^n + \frac{ht^{2g-1}}{q-1}\sum_{n=0}^{\infty} q^g t^n - t^n \\
&= \sum_{n=0}^{2g-2} b_n t^n + \frac{ht^{2g-1}}{q-1}\left(\frac{q^g}{1-qt} - \frac{1}{1-t}\right) \qquad (2.1) \\
&= \sum_{n=0}^{2g-2} b_n t^n + ht^{2g-1}\frac{(1+q+\cdots+q^{g-1}) - qt(1+q+\cdots+q^{g-2})}{(1-qt)(1-t)} \\
&= \frac{L_K(t)}{(1-qt)(1-t)}. \qquad (2.2)
\end{aligned}$$

It follows that $L_K(t) \in \mathbb{Z}[t]$ and $\deg(L_K(t)) \leq 2g$.

Now, we will see that the exact degree of the polynomial $L_K(t)$ is $2g$. For this it suffices to show $t^{1-g}Z_K(t)$ is invariant under the transformation t with $q^{-1}t^{-1}$ because assuming the invariant transformation property we get

$$t^{1-g}Z_K(t) = \frac{t^{1-g}L_K(t)}{(1-t)(1-qt)} = \frac{(q^{-1}t^{-1})^{1-g}L_K(q^{-1}t^{-1})}{(1-t^{-1})(1-q^{-1}t^{-1})} \qquad \Leftrightarrow$$

$$L_K(t) = q^g t^{2g} L_K(q^{-1}t^{-1}) \qquad (2.3)$$

Finally, taking limit as $t \to \infty$ proves that $L_K(t)$ is a polynomial of degree $2g$ with the highest degree term $q^g t^{2g}$.

For the rest of the proof let us write

$$\begin{aligned}
(q-1)Z_K(t) &= \sum_{n=0}^{\infty} b_n t^n \\
&= (q-1)\sum_{n=0}^{\infty} \sum_{deg[D]=n} \frac{q^{l([D])}-1}{q-1} t^n \\
&= \sum_{deg[D]\geq 0} q^{l([D])} t^{deg[D]} - \frac{h}{1-t} \\
&= \sum_{0\leq deg[D]\leq 2g-2} q^{l([D])} t^{deg[D]} - \frac{h}{1-t} + \sum_{deg[D]>2g-2} q^{l([D])} t^{deg[D]} \\
&= \sum_{0\leq deg[D]\leq 2g-2} q^{l([D])} t^{deg[D]} - \frac{h}{1-t} + h\frac{q^g t^{2g-1}}{1-qt}
\end{aligned}$$

For the last equation we used $l([D])$ =deg$([D])-g+1$ in the last summand. We can rewrite the above equation as

$$(q-1)t^{1-g}Z_K(t) = R(t) + S(t)$$

where

$$R(t) = \sum_{0\leq deg[D]\leq 2g-2} q^{l(D)} t^{deg[D]-g+1}, \qquad S(t) = h\left(\frac{q^g t^g}{1-qt} - \frac{t^{1-g}}{1-t}\right)$$

Then, for a divisor class $\mathcal{C}$,

$$\begin{aligned}
R(q^{-1}t^{-1}) &= \sum_{deg[D]\leq 2g-2} q^{l([D])+g-1+deg([D])} t^{g-1-deg([D])} \\
&= \sum_{deg[D]\leq 2g-2} q^{l(\mathcal{C}-[D])} t^{l(\mathcal{C}-[D])-g+1}
\end{aligned}$$

the last equality follows from the fact $l(\mathcal{C}-[D])$ =deg$(C-D)-g+1+l([D]) = g-1-$deg$([D])+l([D])$.

But the map $[D] \to \mathcal{C}-[D]$ is a permuatation of the divisor classes of degree less than $2g-1$. Hence, $R(q^{-1}t^{-1}) = R(t)$. Also, it is easy to show $S(q^{-1}t^{-1}) = S(t)$. These two equality then give us $t^{1-g}Z_K(t)$ is invariant under the tramsformation $t \to q^{-1}t^{-1}$, as we need it above.

For $\zeta_K(s)$ to have simple poles at $s = 0$ and $s = 1$ we need to show $L_K(1)$ and $L_K(q^{-1})$ are nonzero. We have $\lim_{t\to 1}(t-1)Z_K(t) = -h/(q-1)$ and $\lim_{t\to 1}(t-1)Z_K(t) = -L_K(1)/(q-1)$ respectively from (3.1) and (3.2), which shows that $L_K(1) = h$. Also, putting $t = 1$ in (2.3) gives $L(q)^{-1} \neq 0$.

Finally, taking the derivative of the equality $L_K(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} b_n t^n$ gives

$$L'_K(t) = \big(-(q+1) + p(t) + (1 - qt - t + qt^2)(b_1 + b_2 t + \cdots)\big)$$

where $p(t)$ is a polynomial with no constant term. Putting $t = 0$ in the above equation and using $b_1 = a_1$ we get

$$L'_K(0) = -(q+1) + b_1 = a_1 - q - 1$$

□

Definition 2.2.8. *The polynomial $L(t) = (1-t)(1-qt)Z_K(t) \in \mathbb{Z}[t]$ is called the L-polynomial of $K/\mathbb{F}$.*

Corollary 2.2.9. *The zeta function of a function field K over $\mathbb{F}$, with genus g has a functional equation*

$$Z_K(t) = q^{g-1}t^{2g-2}Z_K(\frac{1}{qt})$$

Since the L-polynomial of $K/\mathbb{F}$ has coefficients in $\mathbb{Z}$ it can be factored over the complex numbers

$$L_K(t) = \prod_{i=1}^{2g}(1 - w_i t)$$

In this representation, w_i are called the *inverse roots* of $L_K(t)$. Note that $\zeta_K(s)$ has no zeros in the region $\{t \in \mathbb{C} \mid |t| < q^{-1}\}$ so we must have $|w_i| \leq q$. In fact, the following theorem tells much more about the zeros of $\zeta_K(s)$ and the L-polynomial.

Theorem 2.2.10. *([6], Theorem 5.10, p.55) (The Riemann Hypothesis for Function Fields) Let K be a global function field whose constant field $\mathbb{F}$ has q elements. All the roots of $\zeta_K(s)$ lie on the line $\Re(s) = 1/2$. Equivalently, the inverse roots of $L_K(t)$ all have absolute value $\sqrt{q}$.*

CHAPTER 3

Elliptic Curves

3.1 Curves

Throughout this section, we fix a field F with its closure $\bar{F}$. The *affine n-space over* $\bar{F}$, $\mathbb{A}^n = \mathbb{A}^n(\bar{F})$, is the set of n-tuples $(x_1, x_2, \ldots, x_n)$ with each $x_i \in \bar{F}$. The *F-rational points of* $\mathbb{A}^n$ is the set $\mathbb{A}^n(F) = \{(x_1, x_2, \ldots, x_n) \mid x_i \in F\}$. Let $\bar{F}[X] = \bar{F}[X_1, \ldots, X_n]$ and I an ideal of this ring. Then the *affine algebraic set of* I is defined as $V = V(I) = \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ for all } f \in I\}$ and the *ideal of* V is defined as $I(V) = \{f \in \bar{F}[X] \mid f(P) = 0 \text{ for all } P \in V\}$. If the generators of $I(V)$ are all in $F[X]$ then V is said to be *defined over* F and denoted by V/F. For an algebraic set defined over F, $V(F) = V \cap \mathbb{A}^n(F)$ is the set of *F-rational points of* V.

An affine algebraic set V is called an *affine variety* if $I(V)$ is a prime ideal in $\bar{F}[X]$. Now, let V be a variety. Then, $\bar{F}[V] = \bar{F}[X]/I(V)$ is an integral domain. The quotient field of this integral domain is called the *function field of* V and denoted by $\bar{F}(V)$. Similarly, if V/F is a variety defined over F then $I(V/F) = I(V) \cap F[X]$ is a prime ideal in $F[X]$ and so $F[V] = F[X]/I(V/F)$ is an integral domain and the quotient field of this integral domain is called the *function field of* V/F and denoted by $F(V)$.

Let V be a variety and $I(V) =< f_1, \ldots, f_m >$. The *dimension of* V is defined to be the transcendence degree of the field extension $\bar{F}(V)$ over $\bar{F}$. The variety V is called *non-singular*(or *smooth*) *at* P if the matrix of the generators of $I(V)$

$$(\partial f_i/\partial X_j(P))_{1\leq i\leq m, 1\leq j\leq n}$$

has rank $n-\dim(V)$.

The *projective n-space over* $\bar{F}$, $\mathbb{P}^n = \mathbb{P}^n(\bar{F})$, is given by $\mathbb{A}^{n+1} - (0, 0, \cdots, 0)/\sim$ where $\sim$ is an equivalence relation on its defined set and $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if and only if there exists a $\lambda \in \bar{F}^*$ such that $x_i = \lambda y_i$ for all i. A representative in each equivalence class is denoted by $[x_0 : \cdots : x_n]$. The set of *F-rational points of* $\mathbb{P}^n$ is the set $\mathbb{P}^n(F) = \{P \in \mathbb{P}^n \mid P^\sigma = P \text{ for all } \sigma \in \mathrm{Gal}(\bar{F}/F)\}$ where $P^\sigma = [x_0 : \cdots : x_n]^\sigma = [\sigma(x_0) : \cdots : \sigma(x_n)]$

Let $\bar{F}[X] = \bar{F}[X_0, \ldots, X_n]$. Then, I is an *homogenous ideal of* $\bar{F}[X]$ if it is generated by homogeneous polynomials. Similarly as above, we define the *projective algebraic set of* I by $V = V(I) = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homogenous } f \in I\}$ and the *homogenous ideal of* V by $I(V) = \{f \in \bar{F}[X] \mid f \text{ homogenous and } f(P) = 0 \text{ for all } P \in V\}$. Again, if the generators of $I(V)$ are all homogenous polynomials in $F[X]$ then V is said to be *defined over* F and denoted by V/F. For an algebraic set defined over F, $V(F) = V \cap \mathbb{P}^n(F)$ is the set of *F-rational points of* V.

Every point in $\mathbb{A}^n$ can be embedded in $\mathbb{P}^n$ as

$$\begin{aligned} \phi_i : \mathbb{A}^n &\rightarrow \mathbb{P}^n \\ (x_1, \ldots, x_n) &\mapsto [x_1 : \ldots, x_{i-1} : 1 : \cdots : x_n] \end{aligned}$$

for $0 \leq i \leq n$. In this way, $n+1$ copies of $\mathbb{A}^n$ is contained in $\mathbb{P}^n$. Conversely, for a point $[x_0 : \cdots : x_n] \in \mathbb{P}^n$ there exists i with $x_i \neq 0$ and the map on the set $U_i = \{[x_0 : \cdots : x_n] \mid x_i \neq 0\}$

$$\begin{aligned} \psi_i : U_i &\rightarrow \mathbb{A}^n \\ [x_0 : \cdots : x_n] &\mapsto (x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i) \end{aligned}$$

is the inverse of the above specified map, ϕ_i. Therefore, we have a bijection

$$\{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_i \neq 0\} \leftrightarrow \mathbb{A}^n \tag{3.1}$$

and the left points in $\mathbb{P}^n$, $\{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_i = 0\}$, are called the *points of* $\mathbb{P}^n$ *at infinity.*

The above argument shows that $V = \cup_{i=0}^{n} V_i$ where $V_i = V \cap U_i$. Now, let $V = V(I)$ be a projective variety and suppose that $V_i \neq \emptyset$. Then, the points of V are the union of points of V_i and the points of $V \cap H_i$ where $H_i = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_i = 0\}$ is the *hyperplane at infinity.* For each $G \in I$, the zeros of the polynomial, $G(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n)$, give the points of V_i. The left points, $\{[x_0 : \cdots : x_n] \in \mathbb{P}^2 \mid x_i = 0\} \cap V$, on $V \cap H_i$ are called the *points of* V *at infinity.* Hence, using the bijection 3.1, every projective variety, V, except its points at infinity, can be seen as an affine variety and the corresponding points are called the *affine points* of V. We denote the affine part of V by $V \cap \mathbb{A}^n$. Then, the *dimension of* V, $\dim(V)$, and the *function field of* V, $\bar{F}(V)$ is defined as respectively, the dimension of $V \cap \mathbb{A}^n$ and the function field of $V \cap \mathbb{A}^n$.

Example 3.1.1. *Let* V *be the projective variety in* $\mathbb{P}^2$*, defined over a field* F *by*

$$V : Y^2Z = X^3 + XZ^2 + Z^3$$

Putting $Z = 0$ *in the equation of* V *gives that* $X = 0$ *and* $Y \in \bar{F}$ *so there is only one point at infinity, namely* $[0 : 1 : 0]$*. For the affine points of* V *we put* $Z = 1$ *and conclude that* $V = \{[x : y : 1] \in \mathbb{P}^2 \mid y^2 = x^3 + x + 1\} \cup [0 : 1 : 0]$.

We define a *curve* to be a one dimensional projective variety and the *genus* of a curve is the genus of the function field $F(C)/F$. Note that $F(C)/F$ is a field extension with transcendence degree 1.

3.2 Elliptic Function Fields and Elliptic Curves

A function field K/F of genus 1 with a prime O of degree 1 is called an *elliptic function field.* For a positive integer n, consider the vector space $\mathscr{L}(nO)$. Then, $l(nO) = \deg\,(nO) - g + 1 = n$ since $\deg\,(nO) = n > 2g - 2 = 0$. In particular, for $D = O$, $l(D) = 1$ and since $\mathscr{L}(D)$ already contains constant functions, there is

no function in K with a single pole at O. Now, set $D_n = nO$ and choose a basis for $\mathscr{L}(D_2)$, say $\{1, x\}$. Then, x must have a pole of exact order 2 at O. We have $\mathscr{L}(D_2) \subseteq \mathscr{L}(D_3)$ and $l(D_3) = 3$ so choose $\{1, x, y\}$ as a basis for $\mathscr{L}(D_3)$ where x is the same as above. Again, y cannot have a pole of order one at O. Also it cannot have a pole of order two at O since x and y must be linearly independent. Hence, y must have a pole of exact order 3 at O. Consider the set of functions $\{1, x, y, x^2, xy, y^2, x^3\}$. Clearly, all these functions are contained in $\mathscr{L}(D_6)$. The set contains 7 elements but $l(D_6) = 6$. Hence, there is a linear relation

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

and $A_i \in F$. By ([6], Proposition 5.1, p.47), $[K : F(x)]$ =deg $(x)_\infty = 2$ and $[K : F(y)]$ =deg $(y)_\infty = 3$ so that $K = F(x, y)$. Also, we must have $A_6 \neq 0$ and $A_7 \neq 0$ because otherwise we would have $[K : F(x)] < 2$ and $[K : F(y)] < 3$ which leads a contradiction. Now, writing $x = -A_6A_7x$ and $y = A_6A_7^2y$ in the above equation gives that x and y satisfy a cubic polynomial with coefficients in F of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{3.2}$$

Equation (3.2) is called the *Weierstrass equation*. Considering this equation in $\mathbb{P}^2$, we obtain a projective curve defined over F, namely

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and the points of C is given by

$$C(\bar{F}) = \{[x : y : 1] \in \mathbb{P}^2 \ \mid \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup [0 : 1 : 0]$$

The curve, C, defined by the Weierstrass equation is called the *Weierstrass curve*.

If $\text{char}(\bar{F}) \neq 2, 3$, some suitable change of variables for x and y gives the Weierstrass equation in the form

$$Y^2 = X^3 - 27c_4X - 54c_6$$

where

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3,$$
$$b_6 = a_3^2 + 4a_6,$$
$$c_4 = b_2^2 - 24b_4,$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

We define the *discriminant*, Δ, and the *j-invariant*, j, for a Weierstrass equation as

$$b_8 = a_1^2 + a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$
$$j = c_4^3/\Delta$$

If a curve, C, is given by a Weierstrass equation, Δ gives information about the smoothness of C.

Theorem 3.2.1. *([7], Proposition 1.4, p.50) Let C be a curve given by a Weierstrass equation. Then, C is smooth if and only if $\Delta \neq 0$.*

In the case that the Weierstrass equation is smooth, the Weierstrass curve is called the *elliptic curve* and it is denoted by E.

Let us turn back to the elliptic function field, K/F, with a prime O of degree 1. Take a divisor $D \in \mathcal{D}_K^0$ and consider $\mathscr{L}(D+O)$. Since $\deg(D+O) = 1 > 2g-2 = 0$ we get $l(D+O)$ $=\deg(D+O) - g + 1 = 1$. Then, there exists a nonzero $z \in K$ such that $(z) + D + O \geq 0$. Note that $(z) + D + O$ is a positive divisor and $\deg(z) + D + O = 1$. Therefore, $(z) + D + O = P_D$ for some $P_D \in \mathbb{P}_K$ with $\deg P_D = 1$ and $D \sim P_D - O$. Suppose now, Q_D is another prime of degree 1 such that $D \sim Q_D - O$. If $Q_D \neq P_D$ we get $P_D \sim Q_D$ implying $P_D - Q_D = (z)$ for some $0 \neq z \in K$. Then, by ([6], Proposition 5.1, p.47), $[K : F(z)]$ $=\deg(z)\infty = 1$ that gives a contradiction. Hence, for any divisor $D \in \mathcal{D}_K^0$ there exists a unique prime, $P_D \in \mathbb{P}_K$, of degree 1 such that $D \sim P_D - O$. Now, let $\mathbb{P}_K^{(1)}$ be the set of all primes

in K of degree 1 and define a map

$$\begin{aligned} \sigma : \mathcal{D}_K^0 &\rightarrow \mathbb{P}_K^{(1)} \\ D &\mapsto P_D \end{aligned}$$

The map is surjective, since for $P \in \mathbb{P}_K^{(1)}$ we can choose $D = P - O \in \mathcal{D}_K^0$ so that $\sigma(D) = P$. Now, let $\sigma(D_1) = P_1$ and $\sigma(D_2) = P_2$. Then, $P_1 - P_2 \sim D_1 - D - 2$ and if $P_1 = P_2$ we get $D_1 \sim D_2$. Conversely, if $D_1 \sim D_2$ then $P_1 \sim P_2$ and using the same uniqueness argument in the above, we conclude $P_1 = P_2$. Hence, σ induces a bijection between $\mathbb{P}_K^{(1)}$ and the group of divisor classes of degree zero, $\mathcal{C}_K^0$. Namely,

$$\begin{aligned} \sigma : \mathcal{C}_K^0 &\rightarrow \mathbb{P}_K^{(1)} \\ [D] &\mapsto P_D \end{aligned}$$

Clearly, the inverse map of σ is

$$\begin{aligned} \kappa : \mathbb{P}_K^{(1)} &\rightarrow \mathcal{C}_K^0 \\ P &\rightarrow [P - O] \end{aligned}$$

Now, for P and $Q \in \mathbb{P}_K^{(1)}$ define

$$P \oplus Q = \sigma(\kappa(P) + \kappa(Q)) \tag{3.3}$$

Then, using definition of the map κ we can deduce

$$P \oplus Q = R \Longleftrightarrow P + Q \sim R + O \tag{3.4}$$

From the condition 3.4, it easily follows that $(\mathbb{P}_K^{(1)}, \oplus)$ is an abelian group with O as the identity element and κ is a group isomorphism.

In general, for every function field K/F, there exists a non-singular curve C defined over F such that the function field of C is isomorphic to K, that is $F(C) \cong K$, ([8], Appendix B.9, p.247). Using this isomorphism, we get a one-to-one correspondence between the F-rational points of C, $C(F)$, and the degree 1 primes of K. Now, we can define the *divisor group of* C as the formal group generated by the F-rational points of C. Hence, a *divisor of* C is of the form $D = \sum_{P \in C(F)} n_P P$

where $n_P \in \mathbb{Z}$ and almost all $n_P = 0$. Because of the correspondence between the points $P \in C(F)$ and the degree 1 primes of K, the *degree of* D is defined as deg D=$\sum_{P \in C(F)} n_P$. In the case that K/F is the elliptic function field the corresponding curve is the elliptic curve, E. In particular, the prime O of K corresponds to the point $[0 : 1 : 0]$ of E, ([7], Proposition 3.1, p.63). Hence, applying the analogous arguments in the above to E , we can define an addition operation on the F-rational points of E and get that $(E(F), \oplus)$ is an abelian goup with $O = [0 : 1 : 0]$ as the identity element.

We can also define an addition operation on $E(F)$ using geometry as follows. Let P, $Q \in E(F)$ and $L \subset \mathbb{P}^2$ be the line connecting P and Q. Since the equation of E has degree 2, L intersects the curve E at a third point, say R. Let $L' \subset \mathbb{P}^2$ be another line connecting O and R on the curve E. Again, L' intersects E at a third point and we define this point as $P \oplus Q$. It is easy to check that under this operation $E(F)$ is an abelian group. In fact, the two operations coming from algebra and geometry turn to be the same. For more details, see ([7], Chapter III.3).

3.3 Reduction of Elliptic Curves

Let K be a field with discrete valuation v. Let $\mathcal{O}$ be the dicrete valuation ring and $\mathcal{P}$ the unique maximal ideal of $\mathcal{O}$ and t a generator for $\mathcal{P}$. The valuation v defines an absolute value on K and we can complete the field K with respect to this valuation. So we can assume K is a complete field with respect to v. Consider an elliptic curve E/K with Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

After changing of variables (x, y) by $(t^{-2}x, t^{-3}y)$ in the equation, each a_i becomes $t^i a_i$ and so each $v(a_i)$ increases. Repeating this process we get another equation for E with coefficients in $\mathcal{O}$. Consequently, we can assume E has an ellliptic curve with coefficients in O, $v(\Delta) \geq 0$. Since the valuation function is discrete, there exists one equation with $v(\Delta)$ minimal called the *minimal Weierstrass equation*.

Now, let E be an elliptic curve given by a Weierstrass equation. If $v(\Delta) = 0$, by reducing the coefficients $a_i \in \mathcal{O}$ to $\tilde{a}_i = a_i (\text{mod } \mathcal{P})$ we get a new curve, $\tilde{E}$ over the residue field $k = \mathcal{O}/\mathcal{P}$ and it is called the *reduction of E modulo $\mathcal{P}$*. The reduction process can also be applied to the points of $E(K)$ for producing points of $\tilde{E}(k)$. Let $P = [x_0, y_0, z_0] \in E(K)$. Since v is discrete, we can choose $i \in \mathbb{Z}$ such that each $t^i x_0, t^i y_0, t^i z_0$ is in $\mathcal{O}$ and at least one of them is in $O^* = \mathcal{O} \backslash \mathcal{P}$. Then, $\tilde{P} = [t^i \tilde{x_0}, t^i \tilde{y_0}, t^i \tilde{z_0}] \in \mathbb{P}^2$ and satisfies the equation of $\tilde{E}(k)$.

Now, let $E_1(K) = \{P \in E(K) \mid \tilde{P} = \tilde{O}\}$ of $E(K)$. Then, $E_1(K)$ is a subgroup of $E(K)$ and we have an exact sequence of abelian groups

$$0 \to E_1(K) \to E(K) \to \tilde{E}(k) \to 0 \tag{3.5}$$

and

Proposition 3.3.1. *Let m be a positive integer relatively prime to char k.*

i. *$E_1(K)$ has no non-trivial points of order m.*

ii. *The reduction map*

$$E(K)[m] \hookrightarrow \tilde{E}(k) \tag{3.6}$$

where $E(K)[m]$ is the set of points of order m in $E(K)$, is injective.

iii. *Multiplication by m map is an isomorphism on $E_1(K)$*

For details, see ([7], Chapter IV, Chapter VII).

Now, let $K/\mathbb{F}$ be a global function field and E/K an elliptic curve defined over K. For every $\mathcal{P} \in K$ we can take the completion of K, say $K_\mathcal{P}$ with ring of integers $\mathcal{O}_{K_\mathcal{P}}$, maximal ideal $\mathcal{P}_{K_\mathcal{P}}$. Since $K \hookrightarrow K_\mathcal{P}$, we will consider E as defined over $K_\mathcal{P}$ with having a minimal Weierstrass equation. Note that $\mathcal{P} \mid \Delta$ for only finitely many $\mathcal{P} \in K$, hence $v_\mathcal{P}(\Delta) > 0$ for finitely many $\mathcal{P} \in K$ and $v_\mathfrak{P}(\Delta) = 0$ for the rest of infinitely many primes $\mathcal{P} \in K$. So, for all but finitely many $\mathcal{P}$ we get an elliptic curve $\tilde{E}$ and say E has a *good reduction at $\mathcal{P}$*. The reduction of E modulo $\mathcal{P}_{K_\mathcal{P}}$, is the curve $\tilde{E}$ defined over the residue field $k_\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}_{K_\mathfrak{p}}$. Note that, for $k = \mathcal{O}_\mathcal{P}/\mathcal{P}$

we have $k_{\mathcal{P}} \cong k$ Also, K is a finite extension of the rational function field $\mathbb{F}(x)$ and so k is a finite extension of the residue field $\mathbb{F}[x]/p(x)$ where $p(x)$ is the monic irreducible polynomial over $\mathbb{F}$ corresponding to the prime $\mathfrak{p} \cap \mathbb{F}[x] \in \mathbb{F}[x]$. Thus, $k_{\mathcal{P}}$ is a finite extension of $\mathbb{F}$, say $k_{\mathcal{P}} \cong \mathbb{F}_{q^d}$ for some $d \geq 1$ and we get an elliptic curve $\tilde{E}(k_{\mathcal{P}})$ over a finite field.

Theorem 3.3.2. *Let E be an elliptic curve defined over a finite field $\mathbb{F}$. Then the set of points on E is a finite abelian group with group structure*

$$E(\mathbb{F}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ n \mid m,\ gcd(n,p)= 1.$$

Proof. In the finite group $E(\mathbb{F})$ choose a point with highest order, say with order m. Then, order of any point in the group divides m and so $E(\mathbb{F}) \subseteq E[m]$.
Case 1. $\gcd(m,p)= 1$

$E(\mathbb{F}) \subseteq \widetilde{E}[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ([7], Corollary 6.4, p.89). Hence, $E(\mathbb{F}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, for some $n \mid m$ and $\gcd(n,p)= 1$ since $\gcd(m,p)= 1$.
Case 2. $m = m_1 p^{\alpha}$, $\gcd(m_1,p)= 1$.

In this case $E[m_1]$ and $E[p^{\alpha}]$ are non-empty subgroups of $E[m]$ because by assumption the group $E(\mathbb{F})$, and so the group $E[m]$ contains a point of order $m_1 p^{\alpha}$. Hence, $E[p^{\alpha}] \cong \mathbb{Z}/p^{\alpha}\mathbb{Z}$ and $E[m_1] \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_1\mathbb{Z}$ which implies $E(\mathbb{F}) \subseteq E[m] \cong \mathbb{Z}/m_1 p^{\alpha}\mathbb{Z} \times \mathbb{Z}/m_1\mathbb{Z}$ and results in

$$E(\mathbb{F}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ n \mid m_1,\ \gcd(n,p)= 1.$$

□

By the above theorem, $\tilde{E}(k_{\mathcal{P}})$ is either cyclic or it is product of two cyclic groups. Let $M = \{\mathcal{P} \in K \mid \tilde{E}(k_{\mathcal{P}}) \text{ is cyclic}\}$. We are interested in the Dirichlet density of the primes in M. Since we have good reduction of E at $\mathcal{P}$ for all but finitely many primes in K, $\delta(M) = \delta(M')$ where $M' = \{\mathcal{P} \in K \mid E \text{ has good reduction and } \tilde{E}(k_{\mathfrak{p}}) \text{ is cyclic}\}$.

Theorem 3.3.3. *Let E/K be an elliptic curve defined over a field K. Let $\mathcal{P}$ be a prime of good reduction and $m \in \mathbb{Z}^+$ with $(m,p) = 1$. Then, $\tilde{E}(k)$ is cyclic if and only if $\mathcal{P}$ does not split completely in any $K([m])$ which is the smallest Galois extension of K in which the m-torsion points are defined.*

Proof. Suppose $\mathcal{P}$ splits in some $L = K([m])$. Let $\mathfrak{P}$ be a prime of L lying above $\mathcal{P}$ and $L_{\mathfrak{P}}$ is the local complete field with respect to $\mathfrak{P}$. Then, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \subseteq E(L_{\mathfrak{P}})[m]$ since all m-torsion points of E are contained in L. Now, using injection (3.6) and $[\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : \mathcal{O}_{\mathcal{P}}/\mathcal{P}] = f = 1$ we get

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \subseteq E(L_{\mathfrak{P}})[m] \hookrightarrow \tilde{E}(\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}) = \tilde{E}(\mathcal{O}_{\mathcal{P}}/\mathcal{P}) \tag{3.7}$$

that is, $\tilde{E}(k)$ is not cyclic.

Conversely assume that $\tilde{E}(k)$ is not cyclic. Then, there exists m such that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \subseteq \tilde{E}(k)$. By our assumption, $\mathcal{P}$ is a prime of good reduction and by (3.5) we have an onto homomorphism

$$E(K_{\mathcal{P}}) \to \tilde{E}(k)$$

Now, let $P_i \in E(K_{\mathfrak{p}})$ be the pre-image of $\tilde{P}_i$ satisfying $m\tilde{P}_i = \tilde{O}$ for $i = 1, ..., m^2$. Then, we get $\tilde{mP_i} = m\tilde{P}_i = \tilde{O}$, that is $mP_i \in E_1(K_{\mathcal{P}})$. By Proposition 3.3.1 there exists $Q_i \in E_1(K_{\mathcal{P}})$, such that $mP_i = mQ_i$. Hence, $P_i - Q_i \in E_1(K_{\mathcal{P}}) \subseteq E(K_{\mathcal{P}})$ is a point of order m, for $i = 1, ..., m^2$. This implies $K_{\mathcal{P}} = K_{\mathcal{P}}(E[m]) = L_{\mathfrak{P}}$ for some $\mathfrak{P} \in L$ lying above $\mathcal{P}$ so that $ef = [L_{\mathfrak{P}} : K_{\mathcal{P}}] = 1$ and $e = f = 1$, which finishes the proof. □

CHAPTER 4

Dirichlet Density and Cyclicity of Elliptic Curves

Let E/K be an elliptic curve defined over a global function field $K/\mathbb{F}$. In the previous chapter, we showed that the reduced curve $\tilde{E}$ is defined over a finite field and the points on $\tilde{E}$ is either a cyclic group or it is a product of two cyclic groups. We also determined the necessary and sufficient conditions on the prime $\mathcal{P}$ in K such that E mod $\mathcal{P}$ has a cyclic group structure. In this chapter, we define the Dirichlet density of a subset of primes in the global function field $K/\mathbb{F}$. Then, we finish by the Dirichlet density of primes $\mathcal{P}$ in K such that E mod $\mathcal{P}$ has a cyclic group structure, which is calculated in [1].

Let K be a global function field over the constant field $\mathbb{F}$ with q elements. Let L/K be a Galois extension. Define (L) to be the set of all primes in K that splits in L. Consequently, (K) becomes the set of all primes in K. Let $M \subseteq (K)$. Then the Dirichlet density of M, $\delta(M)$, is defined by

$$\delta(M) = lim_{s \to 1^+} \delta(s, M)$$

where

$$\delta(s, M) = \frac{\sum_{P \in M} NP^{-s}}{\sum_{P \in (K)} NP^{-s}}$$

and s approaches to 1 from above in the real line. If the limit does not exist we say M does not have a Dirichlet density.

Now, we will establish a relation of the zeta function of K with the Dirichlet density of M. Recall that

$$\zeta_K(s) = \sum_{D \geq 0} ND^{-s} = \prod_{P \in (K)} (1 - NP^{-s})^{-1}$$

Taking logarithms of both sides in the above equation we get

$$\begin{aligned} \log \zeta_K(s) &= \sum_{P \in (K)} \log(1 - NP^{-s})^{-1} = \sum_{P \in (K)} \sum_{k=1}^{\infty} \frac{NP^{-ks}}{k} \\ &= \sum_{P \in (K)} NP^{-s} + \sum_{P \in (K)} \sum_{k=2}^{\infty} \frac{NP^{-ks}}{k} \end{aligned} \tag{4.1}$$

In the case that s is taking real values we can write

$$\sum_{k \geq 2} \frac{NP^{-ks}}{k} \leq \sum_{k \geq 2} NP^{-ks} = NP^{-2s} \frac{1}{1 - NP^{-s}} < 2NP^{-2s}$$

so for the second sum in equation (4.1) we have

$$\sum_{P \in (K)} \sum_{k=2}^{\infty} \frac{NP^{-ks}}{k} < 2 \sum_{P \in (K)} NP^{-2s} < 2\zeta_K(2s)$$

Note that $\zeta_K(2s)$ is bounded as $s \to 1^+$. Hence, we can replace the denominator in Dirichlet density with $\log \zeta_K(s)$. Using the similar arguments above, we can replace the numerator by $\sum_M \sum_{k \geq 1} NP^{-ks}/k$ and conclude

Remark 4.0.4. ***i.*** $\delta(M) = lim_{s \to 1^+} \frac{\sum_{P \in M} \sum_{k \geq 1} NP^{-ks}/k}{\log \zeta_K(s)}$

ii. *We proved in Theorem 2.2.7 that $\zeta_K(s)$ has a simple pole at $s = 1$. Hence, $\log(s-1)\zeta_K(s) = \log(s-1) + \log \zeta_K(s)$ is bounded as $s \to 1^+$. Now, writing $f(s) \approx g(s)$ when $f(s) - g(s)$ is bounded, we conclude*

$$\sum_{P \in K} NP^{-s} \approx \log \zeta_K(s) \approx -log(s-1)$$

Proposition 4.0.5. *Let L/K be a Galois extension of global function fields. Let $M = (L)$. Then*

$$\delta((L)) = \frac{1}{[L:K]}$$

Proof. Let $[L:K]=n$. By Remark 4.0.4 we can write $\log\zeta_L(s)\approx\sum_{\mathfrak{P}}N\mathfrak{P}^{-s}$. Also

$$\begin{aligned}\sum_{\mathfrak{P}}N\mathfrak{P}^{-s} &= \sum_{P\in K}\sum_{\mathfrak{P}|P}N\mathfrak{P}^{-s}\\ &= \sum_{\substack{P\in K\\ \text{ramified}}}\sum_{\mathfrak{P}|P}N\mathfrak{P}^{-s}+\sum_{\substack{P\in K\\ \text{unramified}}}\sum_{\mathfrak{P}|P}N\mathfrak{P}^{-s}\end{aligned}$$

There are finitely many ramified primes in K ([6], p.83) and for an unramified prime $P\in K$ there are $g=n/ef=n/f$ primes in L which lie above P and for each $\mathfrak{P}\mid P$ we have $N\mathfrak{P}=NP^{-f}$. Therefore,

$$\begin{aligned}\sum_{\mathfrak{P}}N\mathfrak{P}^{-s} &= C_1+\sum_{f|n}\frac{n}{f}\sum_{\substack{P\in K\\ f(\mathfrak{P}/P)=f}}NP^{-fs}\\ &= C_1+n\sum_{f=1}NP^{-s}+\sum_{\substack{f\mid n\\ 2\le f\le n}}\frac{n}{f}\sum_{\substack{P\in K\\ f(\mathfrak{P}/P)=f}}NP^{-fs}\\ &= C_1+C_2+n\sum_{P\in(L)}NP^{-s}\end{aligned}$$

for some positive constants C_1 and C_2 which come from the sum of the terms over finitely many ramified primes and the sum of the terms for $f\ge 2$, respectively, in the above equation. Then, $\sum_{P\in(L)}NP^{-s}\approx\frac{\log\zeta_L(s)}{n}$. Finally, dividing both sides by $-\log(s-1)$ and using Remark 4.0.4 we conclude

$$\delta((L))=\frac{1}{[L:K]}.$$

□

$L(\mathscr{F})$ will denote the lattice of fields spanned by $\mathscr{F}=\{K_v\}_{v\in\mathbf{N}}$ which is a countable family of finite Galois extensions of K.

Theorem 4.0.6. *([1]) Let $F=\{K_v\}_{v\in\mathbb{N}}$ be a countable family of Galois extensions of K, $\mathbb{F}_v$ the algebraic closure of $\mathbb{F}$ in K_v, and M the set of prime ideals in K that do*

not split completely in any of the fields in $L(F)$. Set $n(v) = [K_v : K]$, $c(v) = [\mathbb{F}_v : \mathbb{F}]$ and define for a set of positive integers $I = \{v_1, ..., v_r\}$ $K_I = K_{v_1} \cdots K_{v_r}$ as the compositum field. Suppose that the following conditions hold

i. $\sum_{v=1}^{\infty} \frac{1}{n(v)} < \infty$

ii. $\sum_{v=1}^{\infty} \frac{1}{c(v)q^{\frac{1}{2}c(v)}} < \infty$, *and*

iii. *There exists a constant C such that $g(K_v) \leq C\frac{n(v)}{c(v)}$ for all v.*

Then, the Dirichlet density of M exists and is given by

$$\delta(M) = \sum_{I} \frac{\mu(I)}{[K_I : K]}$$

where $\mu(I) = (-1)^{|I|}$

Proof. We are looking for the density of primes in M which is the set of primes that do not split completely in any of the fields in $L(\mathscr{F})$. Defining $M_n = \bigcap_{v \leq n}[(K)-(K_v)]$ we get $M = \lim_{n\to\infty} M_n$ and deduce

$$\delta(M) = \lim_{s\to 1^+} \lim_{n\to\infty} \delta(s, M_n) \tag{4.2}$$

Recall that by Theorem 1.3.14 a prime $P \in K$ splits in the Galois extensions K_{v_1} and K_{v_2} if and only if it splits in the compositium field $K_{v_1}K_{v_2}$. Hence, using the inclusion exclusion principle we obtain another equation for M_n

$$M_n = (K) - \sum_{v \leq n}(K_v) + \sum_{v_1, v_2 \leq n} (K_{v_1}K_{v_2}) - \cdots + (-1)^n (K_{v_1} \cdots K_{v_n})$$

Now, suppose that the limits in Equation (4.2) can be interchanged. Then, using the Proposition 4.0.5 we complete the proof of the theorem. Note that $\delta(s, M) < \delta(s, M_n)$ and $\delta(s, M_n) - \delta(s, M) < \sum_{v>n} \delta(s, (K_v))$. Thus, proving the convergence of $\sum_v \mid \delta(s, (K_v)) \mid$ will suffice for interchanging the limits. By Remark 4.0.4 we have

$$\delta(s, (K_v)) = \frac{\sum_{k=1}^{\infty} \sum_{P \in (K_v)} NP^{-ks}/k}{\log \zeta_K(s)}.$$

Note that for $P \in (K_v)$ there are $n(v)$ primes, $\mathfrak{P}$, in K_v lying above P with $e(\mathfrak{P}/P) = f(\mathfrak{P}/P) = 1$ and so $N\mathfrak{P} - NP$. Then, we can write the below inequality

$$\sum_{k=1}^{\infty} \sum_{P \in (K_v)} \frac{NP^{-ks}}{k} = \frac{1}{n(v)} \sum_{k=1}^{\infty} \sum_{\substack{\mathfrak{P} \in K_v \\ deg\mathfrak{P} = 1}} \frac{N\mathfrak{P}^{-ks}}{k} \leq \frac{1}{n(v)} \log \zeta_{K_v}(s)$$

and we get

$$\sum_{v} |\delta(s, (K_v))| \leq \frac{1}{n(v)} \left| \frac{\log \zeta_{K_v}(s)}{\log \zeta_K(s)} \right|$$

By Theorem 2.2.7 we can write

$$\begin{aligned} \frac{1}{n(v)} \left| \frac{\log \zeta_{K_v}(s)}{\log \zeta_K(s)} \right| &= \sum_{v} \frac{1}{n(v)} \left| \frac{\log L_{K_v}(q^{-sc(v)})}{\log \zeta_K(s)} \right| + \\ &\quad \sum_{v} \frac{1}{n(v)} \left| \frac{\log(1 - q^{-sc(v)})^{-1}(1 - q^{(1-s)c(v)})^{-1}}{\log \zeta_K(s)} \right| \end{aligned}$$

By Example 2.2.6 the second term in the above sum is equal to $\sum_v \frac{1}{n(v)} \left| \frac{\log \zeta_{k_v(X)}(s)}{\log \zeta_K(s)} \right|$. Using condition (i), it is convergent as $s \to 1^+$ since $\left| \frac{\log(1-q^{-sc(v)})^{-1}(1-q^{(1-s)c(v)})^{-1}}{\log \zeta_K(s)} \right|$ is also convergent as $s \to 1^+$ by Example 2.2.6 and Theorem 2.2.7. For the first term, using Theorem 2.2.10 and condition (iii)

$$L_{K_v}(q^{-sc(v)}) = \prod_{i=1}^{2g(K_v)} (1 - w_i q^{-sc(v)}) \begin{cases} \leq (1 + q^{-\frac{sc(v)}{2}})^{2g(K_v)} < (1 + q^{-\frac{c(v)}{2}})^{Cn(v)/c(v)} \\ \geq (1 - q^{-\frac{sc(v)}{2}})^{2g(K_v)} > (1 - q^{-\frac{c(v)}{2}})^{Cn(v)/c(v)} \end{cases}$$

Now, using $\log(1 + q^{-\frac{c(v)}{2}}) < q^{-\frac{c(v)}{2}}$ and

$$-\log(1 - q^{-\frac{c(v)}{2}}) < \frac{q^{\frac{c(v)}{2}}}{q^{\frac{c(v)}{2}} - 1} q^{-\frac{c(v)}{2}} < 4q^{-\frac{c(v)}{2}}$$

we get

$$\left| \log L_{K_v}(q^{-sc(v)}) \right| < 4C \frac{n(v)}{c(v)}$$

and since $\zeta_K(s)$ has a simple pole at $s = 1$

$$\left| \frac{1}{n(v)} \frac{\log L_{K_v}(q^{-sc(v)})}{\log \zeta(s)} \right| < 4CC' \frac{1}{c(v) q^{\frac{c(v)}{2}}}$$

Finally, condition (ii) guarantees the interchanging limits as we required. □

Recall that we are looking for the Dirichlet density of primes, $\mathcal{P}$ of good reduction such that $\tilde{E}$ mod $\mathcal{P}$ is cyclic. By Theorem 3.3.3 we have to calculate the density of the primes that do not split completely in any of the fields in $L(\mathcal{F})$ where $\mathcal{F} = \{K([l])\}_{l:prime, l\neq p}$.

Theorem 4.0.7. *[1] Let $K/\mathbb{F}_q$ be a global function field. The Dirichlet density δ of the set of primes, $\mathcal{P}$, such that $\tilde{E}$ mod $\mathcal{P}$ is cyclic is given by*

$$\delta = \sum_{(m,p)=1} \frac{\mu(m)}{[K([m]) : K]}$$

Proof. We will show that the conditions in Theorem 4.0.6 are satisfied by $\mathcal{F} = \{K([l])\}_{l:prime, l\neq p}$.

(i) Let $\bar{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$ and E the elliptic curve with j-invariant j. Then, for $G = \mathrm{Gal}(\bar{\mathbb{F}}_q(j)([l])/\bar{\mathbb{F}}_q(j))$, we have an homomorphism

$$\begin{aligned} \rho : \quad & G \to \mathrm{Aut}(E[l]) \cong \mathrm{GL}(2,\ \mathbb{Z}/l\mathbb{Z}) \\ & \sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

where $P^\sigma = aP + bQ$, $Q^\sigma = cP + dQ$ for generators P and Q of $E[l]$. The *Weil-e_l pairing* on an E is a map $e_l : E[l] \times E[l] \to \mu_l = l^{th}$ roots of unity ([7], Chapter III.8). Using the properties of this map and the fact that $\bar{\mathbb{F}}_q$ contains l^{th} roots of unity we get that

$$e_l(P,\ Q) = e_l(P,\ Q)^\sigma = e_l(P^\sigma,\ Q^\sigma) = e_l(aP + bQ,\ cP + dQ) = e_l(P,\ Q)^{ad-bc}$$

and $ad - bc = 1$. Hence, we have an injection $G \hookrightarrow \mathrm{SL}(2,\ \mathbb{Z}/l\mathbb{Z})$. In fact, this map is onto ([3]) and gives us the isomorphism

$$\mathrm{Gal}(\bar{\mathbb{F}}_q(j)([l])/\bar{\mathbb{F}}_q(j)) \cong \mathrm{SL}(2,\ \mathbb{Z}/l\mathbb{Z})$$

Now, we can write

$$\begin{aligned} n(l) &= |\ \mathrm{Gal}(K([l]) : K)\ | \geq |\ \mathrm{Gal}(\mathbb{F}_q(j)([l])/\mathbb{F}_q(j))\ |\ /[K : \mathbb{F}_q(j)] \\ &\geq |\ \mathrm{SL}(2,\ \mathbb{Z}/l\mathbb{Z})\ |\ /[K : \mathbb{F}_q(j)] \\ &= l(l-1)(l+1)/[K : \mathbb{F}_q(j)] \end{aligned}$$

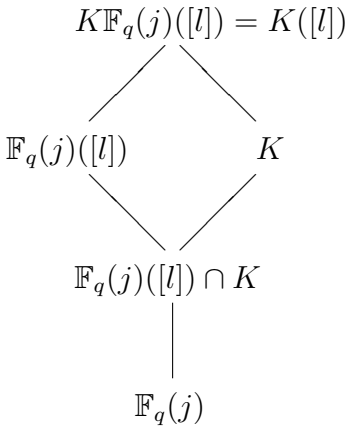
and proves the condition (i).

(ii) Since $E[l] \subset E(K([l]))$, $K([l])$ contains the l^{th} roots of unity([7], Corollary 8.1.1, p.98). Also, by definition, k_l is the algebraic closure of $k = \mathbb{F}_q$ in K_l. Then

$$c(l) = [k_l : k] \geq [k\sqrt[l]{1} : k] = l - 1$$

and condition (ii) is satisfied.

(iii) For the extensions of the fields we have the following diagram



Now, let $\mathfrak{P}$ be a prime in $K([l])$ lying above the prime $\mathfrak{a} \in K$ with ramification index e. Let $\mathfrak{p} \in \mathbb{F}_q(j)([l])$ be the prime lying below $\mathfrak{P}$, $\mathcal{P} \in \mathbb{F}_q(j)([l]) \cap K$ the prime lying below $\mathfrak{p}$, and $p \in \mathbb{F}_q(j)$ te prime lying below $\mathcal{P}$. $K([l])/K$ and $\mathbb{F}_q(j)([l])/\mathbb{F}_q(j)$ are Galois extensions. By ([4], Theorem 1.12, p.266), $\mathbb{F}_q(j)([l])/\mathbb{F}_q(j)([l]) \cap K$ is also Galois and there is an isomorphism between Galois groups $\mathrm{Gal}(K([l])/K)$ and $\mathrm{Gal}(\mathbb{F}_q(j)([l])/\mathbb{F}_q(j)([l]) \cap K)$, which is simply through the restriction of automorphisms to $\mathbb{F}_q(j)([l])$. Then, the inertia groups $I(\mathfrak{P}/\mathfrak{a})$ and $I(\mathfrak{p}/\mathcal{P})$ are isomorphic by ([5], Proposition 9.4, p.169) and we write

$$e = I(\mathfrak{P}/\mathfrak{a}) = I(\mathfrak{p}/\mathcal{P})$$

But, $\mathbb{F}_q(j)([l])/\mathbb{F}_q(j)$ is tamely ramified ([3]), that is, $\mathrm{char}(\mathbb{F}_q)$ does not divide e. So, K_l/K is tamely ramified and from the Riemann-Hurwitz formula([6], p.90) for $K([l])/Kk_l$ where k_l is the algebraic closure of $\mathbb{F}_q$ in $K([l])$ we get

$$2g(K([l])) - 2 = [K([l]) : Kk_l](2g(Kk_l) - 2) + \sum_{\mathfrak{P}} (e(\mathfrak{P}/P) - 1)\deg \mathfrak{P}.$$

Also, $n(l) = [K([l]) : K] = [K([l]) : Kk_l][Kk_l : K] = [K([l]) : Kk_l][k_l : \mathbb{F}_q] = [K([l]) : Kk_l]c(l)$, that is, $[K([l]) : Kk_l] = n(l)/c(l)$. Hence, $g(K([l])) \leq Cn(l)/c(l)$ for some positive constant C and so condition (iii) is satisfied. $\square$

Bibliography

[1] Clark, D. A., Kuwata, M., *Generalized Artin's Conjecture for Primitive Roots and Cyclicity Mod* $\mathfrak{p}$ *of Elliptic Curves over Function Fields*, Canad. Math. Bull. Vol. **38**(2) (1995), 167–173.

[2] Hungerford, T. W., *Algebra*, Springer-Verlag, Washington, 1996.

[3] Igusa, J., *Fiber System of Jacobian Varieties III*, Amer. Math. Soc. **81** (1959), 453–476.

[4] Lang, S., *Algebra*, Addison-Wesley Publishing Company U.S.A, 1993.

[5] Neukirch, J., *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg New York, 1999.

[6] Rosen, M., *Number Theory in Function Fields*, Springer-Verlag Berlin Heidelberg New York, 2002.

[7] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer-Verlag Berlin Heidelberg New York, 1986.

[8] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag Berlin Heidelberg New York, 1993.