

Riemann Hypothesis for the Zeta Function of a Function Field over a Finite Field

by

Marie Brilland Yann Ranorovelonalohotsy

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



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

Supervisor: Prof. Florian Breuer

December 2013

Declaration

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

Date: 2013/11/26

Copyright © 2013 Stellenbosch University
All rights reserved.

Abstract

Riemann Hypothesis for the Zeta Function of a Function Field over a Finite Field

Marie Brilland Yann Ranorovelonalohotsy

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

Thesis: MSc (Math)

December 2013

Let K be a function field over a finite field. Fix a place (∞) of K , which we shall call the prime at infinity. We consider the ring $A = \{y \in K : y \text{ is regular at } P \text{ for every place } P \neq (\infty)\}$, which we call the ring of integers of K with respect to (∞) . There is a bijection between the set of proper ideals of A and the places of K different from (∞) . We define the zeta function $\zeta_A(s)$ for the ring A in a way analogous to the Dedekind zeta function of the ring of integers of a number field. The analogue of the Riemann Hypothesis for $\zeta_A(s)$ was first proved by André Weil in 1948, and our goal is to give an exposition of a simpler proof of this theorem due to Enrico Bombieri.

Uittreksel

Riemannvermoeding vir die Zeta-Funksie van 'n Funksieliggaam oor 'n Eindige Liggaam.

(“Riemann Hypothesis for the Zeta Function of a Function Field over a Finite Field”)

Marie Brilland Yann Ranorovelonalohotsy

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

Tesis: MSc (Wisk)

Desember 2013

Gestel K is 'n funksie-liggaam oor 'n eindige liggaam. Ons lê 'n plek (∞) vas, wat ons die plek by oneindig noem. Ons beskou die ring $A = \{y \in K : y \text{ is reëlmatig by } P \text{ vir elke plek } P \neq (\infty)\}$, wat ons die ring van heelgetalle van K met betrekking tot (∞) noem. Daar is 'n bijeksie tussen die versameling van eintlike ideale van A en die plekke van K wat van (∞) verskil. Ons definieer die zeta-funksie $\zeta_A(s)$ van die ring A analoog met die definisie van die Dedekind zeta-funksie van die ring van heelgetalle van 'n getalleliggaam. Die analoog van die Riemannvermoeding vir $\zeta_A(s)$ is in 1948 deur André Weil bewys, en ons doel is om 'n makliker bewys hiervan van Ernico Bombieri ten toon te stel.

Acknowledgements

I would like to express my sincere gratitude to Prof. Florian Breuer for his assistance and advise throughout all of this project. It was a great pleasure to get the opportunity of working with him.

I would like to thank the department of Mathematical Sciences of the University of Stellenbosch which offered me the courses during the period of my Master.

Thanks go to the Faculty of Sciences of Stellenbosch University, and the African Institute of Mathematical Sciences (AIMS) in South Africa by offering me financial and material supports.

Thanks also go to the Malagasy students in the Mathematical Sciences department of the University of Stellenbosch, especially those from the field of number theory, for their help.

I finally would like to thanks my family, especially Nantsoina, for their love, encouragement and support throughout my studies.

Dedications

This work is dedicated to Nantsoina C. Ramiharimanana.

Contents

Declaration	i
Abstract	ii
Uittreksel	iii
Acknowledgements	iv
Dedications	v
Contents	vi
Notation	vii
1 Introduction	1
2 Preliminaries	3
2.1 Global Function Fields	3
2.2 Riemann-Roch Theorem	7
2.3 Finite Extensions of Global Function Fields.	9
2.4 Some Tools From Commutative Algebra.	12
3 The Riemann Zeta Function for Global Function Fields.	13
3.1 The Ring of Integers	13
3.2 The Riemann Zeta Function of the Ring of Integers	15
3.3 The Functional Equation for ζ_A	24
4 The Riemann Hypothesis for ζ_A.	29
4.1 The Riemann Hypothesis	29
4.2 The Proof of the Riemann Hypothesis for ζ_A	34
4.3 Constant Field Extensions	45
4.4 End of the Proof of the Riemann Hypothesis for ζ_A	53
Bibliography	58

Notation

$\mathbb{N} = \{0, 1, 2, \dots\}$ the set of natural numbers

\mathbb{Z} = the ring of rational integers.

\mathbb{Q} = the field of rational numbers.

\mathbb{R} = the field of real numbers.

$\text{Quot}(R)$ = the quotient field of an integral domain R .

R^\times = the group of the units of the ring R

\mathbb{F} = the field with q elements.

\tilde{K} = the algebraic closure of a field K .

$\text{Gal}(L/K)$ = the Galois group of a Galois extension L/K .

$|A|$ = the cardinality of the set A

Chapter 1

Introduction

It is well known that the classical Riemann zeta function $\zeta(z) = \sum_{n=1}^{\infty} n^{-z}$ is an analytic function in the half plane $\mathcal{H} = \{s \in \mathbb{C} : \mathbf{Re}(s) > 1\}$, and can be analytically continued into the whole complex plane to a meromorphic function with only one pole which occurs at the point $z = 1$.

The function ζ does not vanish in \mathcal{H} , and away from the non trivial zeroes of ζ , the only points of \mathbb{C} which can be the roots of ζ lay in the strip $\{s \in \mathbb{C} : 0 < \mathbf{Re}(s) < 1\}$.

In fact, the Riemann hypothesis for the classical ζ function states that any non-trivial roots of ζ lay in the line given by the equation $\mathbf{Re}(z) = \frac{1}{2}$. This has a lot of important consequences in the arithmetic of the ring \mathbb{Z} .

By considering a global function field K/\mathbb{F} , we have an analogue of the classical Riemann ζ function. For that, we fix a place of K , (∞) , which is named the place at infinity.

The set $A = \{y \in K : y \text{ is regular at } P, \text{ for every place } P \neq (\infty)\}$ is called the ring of integers of K with respect to the place (∞) . And an analogue of the classical ζ function for number fields is the function ζ_A , which is defined by for any $z \in \mathcal{H}$, $\zeta_A(z) = \sum_{I \in Id(A) - \{(0)\}} \mathcal{N}_A(I)^{-z}$, where $Id(A)$ is the set of ideals of A , and $\mathcal{N}_A(I) = |A/I|$. ζ_A is analytic in \mathcal{H} , and can be uniquely extended to a meromorphic function of \mathbb{C} which has a unique pole of order one at the point $z = 1$.

Moreover, $\zeta_A(z) = \frac{L_A(q^{-z})}{1 - q^{1-z}}$, where $L_A(u) \in \mathbb{Z}[u]$, and $L_A(q^{-1}) \neq 0$.

The classical ξ function associated to the classical ζ function for number fields has also an analogue for K , which is denoted by ξ_A , and satisfies that for all $z \in \mathbb{C} - \{1\}$, $\xi_A(1 - z) = \xi_A(z)$.

The Riemann hypothesis for the global function field K states that the non-trivial zeroes of ζ_A all have real parts $\frac{1}{2}$. Despite the number fields case, this is no longer a conjecture. The Riemann hypothesis for K has many applications, in particular to the distribution of the places of degree one of K .

In this work, the Chapter 2 is basically the essential tools for function fields over finite field. In the first section, we give the definition of a global function

field K , and discuss some properties of it, in particular the properties of valuation rings of K . The section one of Chapter 2 ends by an important result, Corollary 2.1.18, which says that the set of places of K is not empty.

The section 2 discusses about Riemann-Roch theorem. There, we begin by the notion of divisors of K , and state some properties of it.

In the section 3, we will talk about extensions of K .

The section 4 discusses tools from commutative algebra, in particular the theorem of Samuel-Zariski (1958).

The main result of the first section of Chapter 3 is to show that the ring A is a Dedekind domain. This result comes from the fact that there is a bijection between the set of proper prime ideals of A and the set of places of K different from the place at infinity.

In the second section, we define the Riemann ζ_A function, and give some important properties of this, in particular the Euler product of and the functional equation of ζ_A .

The last chapter provides the Riemann hypothesis for a global function field which is the goal of this work. The main result is the Theorem 4.1.1. The first section gives us a description of the Riemann hypothesis. From the difficulties which occur in constant field extension, the proof of Theorem 4.1.1 needs to introduce the function ζ_K (see [1, Chapter 5] or [2, Chapter 5]). The proof of the Riemann hypothesis gets started only in the second section, following an elementary method from Bombieri. Then, the third section tells us about constant field extensions, and gives some results from group theory. An important tool is the automorphism of Frobenius. The last section concludes the Theorem 4.1.1.

Chapter 2

Preliminaries

This Chapter introduces the basic notions of global function fields. After defining a global function field, we present some properties of its places, the Riemann-Roch theorem, and the notions of extensions of a global function field. The last section is devoted to some tools from commutative algebra. Most of the results in this Chapter are presented without proof, for more details the reader might consult [1, Chapter 1, Chapter 3, Chapter 5].

2.1 Global Function Fields

In this section, we present a brief notion of global function fields. We define places and show that the set of places a global function field is not empty.

Definition 2.1.1. Let K be a field extension of \mathbb{F} . We say that K is a global function field over \mathbb{F} if there exists $x \in K$ such that x is transcendental over \mathbb{F} and the field extension $K/\mathbb{F}(x)$ is finite.

We denote by K/\mathbb{F} the global function field K over \mathbb{F} .

Definition 2.1.2. The subfield $\tilde{\mathbb{F}} = \{\lambda \in K : \lambda \text{ is algebraic over } \mathbb{F}\}$ of K is the algebraic closure of \mathbb{F} in K . We call $\tilde{\mathbb{F}}$ the constant field of K .

We give here a simple example of a global function field.

Example 2.1.3. Let T be an indeterminate, and $A = \mathbb{F}[T]$ the polynomial ring with coefficients in \mathbb{F} . Then $\text{Quot}(A) = \mathbb{F}(T)$ is a global function field over \mathbb{F} , whose constant field is \mathbb{F} .

Remark 2.1.4. A global function field over \mathbb{F} is also called an algebraic function field over \mathbb{F} .

Definition 2.1.5. Let K be a global function field over \mathbb{F} . We say that K is a rational function field if there exists $x \in K$ such that $K = \mathbb{F}(x)$.

Clearly x is transcendental over \mathbb{F} .

Definition 2.1.6. Let K/\mathbb{F} be a global function field. A subring \mathcal{O} of K is said to be a valuation ring of K , if it satisfies:

- (i) $\mathbb{F} \subsetneq \mathcal{O} \subsetneq K$.
- (ii) For any $z \in K$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Here are some important properties of the valuations rings of an algebraic function field over a finite field.

Proposition 2.1.7. Suppose that \mathcal{O} is a valuation ring of K/\mathbb{F} . Then, the following hold:

- (i) \mathcal{O} is a discrete valuation ring with maximal ideal $P = \mathcal{O} - \mathcal{O}^\times$;
- (ii) for every $x \in K - \{0\}$, $x \in P$ if and only if $x^{-1} \notin \mathcal{O}$.
- (iii) $K = \text{Quot}(\mathcal{O})$
- (iv) $\tilde{\mathbb{F}} \subseteq \mathcal{O}$.
- (v) $\tilde{\mathbb{F}} \cap P = \{0\}$.

Proof. (i) By [1, Proposition 1.1.5 (a)] and [1, Theorem 1.1.6 (a)], \mathcal{O} is a local ring with maximal ideal P , which is principal. Moreover, from [1, Theorem 1.1.6 (c)], any non-zero ideal of \mathcal{O} is a power of P . Therefore, \mathcal{O} is a discrete valuation ring.

- (ii) Let $x \in K - \{0\}$, and assume $x \in P$.
If $x^{-1} \in \mathcal{O}$, then $xx^{-1} = 1 \in P$. That is impossible since P is a maximal ideal of \mathcal{O} . So, $x^{-1} \notin \mathcal{O}$.

Conversely, suppose $x^{-1} \notin \mathcal{O}$. Since \mathcal{O} is a valuation ring of K/\mathbb{F} , $x \in \mathcal{O}$. If $x \in \mathcal{O}^\times$, then $x^{-1} \in \mathcal{O}$. That contradicts our assumption. So, $x \in P$.

- (iii) It is clear that

$$\text{Quot}(\mathcal{O}) \subseteq K. \quad (2.1.1)$$

Let $z \in K$, and suppose $z \notin \mathcal{O}$. As \mathcal{O} is a valuation ring, $z^{-1} \in P$ by (ii), so $z = \frac{1}{z^{-1}} \in \text{Quot}(\mathcal{O})$. Thus

$$K \subseteq \text{Quot}(\mathcal{O}). \quad (2.1.2)$$

(2.1.1) and (2.1.2) show that $K = \text{Quot}(\mathcal{O})$.

- (iv) Let $x \in \tilde{\mathbb{F}}$. If $x \notin \mathcal{O}$, then $x^{-1} \in \mathcal{O}$ since \mathcal{O} is a valuation ring. As $x^{-1} \in \tilde{\mathbb{F}}$ and \mathbb{F} is a field, we can find a_1, a_2, \dots, a_r in \mathbb{F} , with $r \in \mathbb{N}$, such that

$$a_r(x^{-1})^r + a_{r-1}(x^{-1})^{r-1} + \dots + a_1(x^{-1}) + 1 = 0 \quad (2.1.3)$$

So

$$(x^{-1})(a_r(x^{-1})^{r-1} + a_{r-1}(x^{-1})^{r-2} + \dots + a_1) = -1. \quad (2.1.4)$$

It follows that $x = -(a_r(x^{-1})^{r-1} + a_{r-1}(x^{-1})^{r-2} + \dots + a_1)$.

Since $\mathbb{F}[x^{-1}] \subseteq \mathcal{O}$ and \mathcal{O} is a ring, $x \in \mathcal{O}$. That is a contradiction of our assumption.

- (v) Assume that there exists $x_0 \in K - \{0\}$, with $x_0 \in \tilde{\mathbb{F}} \cap P$. On one hand, $x_0 \in \tilde{\mathbb{F}}$, then we can find $b_1, b_2, \dots, b_r \in \mathbb{F}$ such that

$$-(b_r(x_0)^r + b_{r-1}(x_0)^{r-1} + \dots + b_1x_0) = 1.$$

On the other hand, $x_0 \in P$, $\mathbb{F} \subseteq \mathcal{O}$ and P is a maximal ideal of \mathcal{O} , then $-(b_r(x_0)^r + b_{r-1}(x_0)^{r-1} + \dots + b_1x_0) \in P$. In other words $1 \in P$. That contradicts the fact that P is maximal ideal of \mathcal{O} . □

Definition 2.1.8. Let \mathcal{O} be a valuation ring of an algebraic function field K over the finite field \mathbb{F} , $P = t\mathcal{O}$ be its maximal ideal, with $t \in \mathcal{O} - \{0\}$.

- (i) We say that t is a uniformizing parameter of P .
- (ii) The map $v_P : K \rightarrow \mathbb{Z} \cup \{\infty\}$, such that for $x = ut^m$, with $m \in \mathbb{Z}$ and $u \in \mathcal{O}^\times$, $v_P(x) = m$, and $v_P(0) = \infty$, is called the discrete valuation of K/\mathbb{F} associated to the valuation ring \mathcal{O} .

The next lemma shows that the map v_P given above is well defined.

Lemma 2.1.9. Using the same notation as in Definition 2.1.8, if z is another uniformizing parameter of P , then $v_P(z) = v_P(t) = 1$. In particular, v_P is well defined.

Proof. Let $z \in \mathcal{O}$ be an uniformizing parameter of P . Then $t = \alpha z$, with $\alpha \in \mathcal{O}$. Since $P = t\mathcal{O}$, then $z = \beta t$, where $\beta \in \mathcal{O}$. It follows $t = \alpha\beta t$. As $t \neq 0$ and \mathcal{O} is an integral domain, then $\alpha\beta = 1$. Thus $\beta \in \mathcal{O}^\times$. Hence $v_P(z) = v_P(t) = 1$. □

Definition 2.1.10. Let K/\mathbb{F} be a global function field. We say that P is a place of K if there exist a valuation ring \mathcal{O}_P of K such that P is its maximal ideal.

We denote by \mathcal{M}_K the set of places of K .

Theorem 2.1.11. Let K/\mathbb{F} be a global function field, and let $P \in \mathcal{M}_K$. Then the map v_P associated to P has the following properties:

- (i) For any $(y, z) \in \mathcal{O}_P^2$, $v_P(y + z) \geq \min(v_P(y), v_P(z))$.

- (ii) For any $(y, z) \in \mathcal{O}_P^2$, if $v_P(z) \neq v_P(y)$, then $v_P(y+z) = \min(v_P(y), v_P(z))$. This is called the strict triangle inequality.

Proof. (i) Let $(y, z) \in \mathcal{O}_P^2$, and let t be a uniformizing parameter of P . We may assume that $y \neq 0$, and $z \neq 0$. Then $y = ut^{v_P(y)}$, and $z = \beta t^{v_P(z)}$, where u, β belong to \mathcal{O}_P^\times . Set $m = \min(v_P(y), v_P(z))$. Then, $y + z = t^m(ut^{v_P(y)-m} + \beta t^{v_P(z)-m})$. Since $v_P(y) - m \geq 0$ and $v_P(z) - m \geq 0$, and \mathcal{O}_P is a discrete valuation ring, $ut^{v_P(y)-m} + \beta t^{v_P(z)-m} \in \mathcal{O}_P$. It follows that $v_P(y+z) \geq \min(v_P(y), v_P(z))$.

- (ii) Let $(y, z) \in \mathcal{O}_P^2$, let t be a uniformizing parameter of P . Suppose $v_P(z) \neq v_P(y)$. We may assume that both z , and y are not 0. We also can assume that $m = \min(v_P(y), v_P(z)) = v_P(y)$. From (i), we have $y + z = t^m(u + \beta t^{v_P(z)-m})$. Since $v_P(z) - m > 0$ and a discrete valuation ring is a local ring, $u + \beta t^{v_P(z)-m} \in \mathcal{O}_P^\times$. Therefore, $v_P(y+z) = m = \min(v_P(y), v_P(z))$. \square

Proposition 2.1.12. Let K/\mathbb{F} be a global function field and $P \in \mathcal{M}_K$. Let v_P be the map associated to P . Then, we have

- (i) $\mathcal{O}_P = \{y \in K : v_P(y) \geq 0\}$.
- (ii) $P = \{y \in K : v_P(y) > 0\}$.
- (iii) $\mathcal{O}_P^\times = \{y \in K : v_P(y) = 0\}$.

Proof. From Proposition 2.1.7, (iii), $K = \text{Quot}(\mathcal{O}_P)$, and \mathcal{O}_P is a discrete valuation ring, then we get the result. \square

Definition 2.1.13. Let K/\mathbb{F} be a global function field over \mathbb{F} , let $P \in \mathcal{M}_K$, and let $y \in K$. We say that P is a zero (respectively pole) of y if $v_P(y) > 0$ (respectively $v_P(y) < 0$).

Remark 2.1.14. Let K/\mathbb{F} be a global function field. Let $P \in \mathcal{M}_K$ and $y \in K$. Then $|v_P(y)|$ is the order of the pole or zero P of y .

Proposition 2.1.15. Let K/\mathbb{F} be a global function field, and let $P \in \mathcal{M}_K$. Then \mathcal{O}_P/P is a finite extension of \mathbb{F} . We call $\deg_K(P) = [\mathcal{O}_P/P : \mathbb{F}]$ the degree of the place P .

Remark 2.1.16. Often, for a global function field K , we denote by K_P the residue class field of a place P of K .

Proof of Proposition 2.1.15. Let $y \in P - \{0\}$. Since P is a maximal ideal of \mathcal{O}_P , y is transcendental over \mathbb{F} . So, by [1, Proposition 1.1.15], $[\mathcal{O}_P/P : \mathbb{F}] \leq [K : \mathbb{F}(y)]$. As $[K : \mathbb{F}(y)]$ is finite, then \mathcal{O}_P/P is a finite extension of \mathbb{F} . \square

Theorem 2.1.17. Let K/\mathbb{F} be a global function field, and let $y \in K$ which is transcendental over \mathbb{F} . Then, there exists a place P of K such that $v_P(y) < 0$.

Proof. See [1, Corollary 1.1.20]. \square

We finish this section with a fundamental property of global function fields.

Corollary 2.1.18. Let K/\mathbb{F} be a global function field over \mathbb{F} . Then, $\mathcal{M}_K \neq \emptyset$.

Proof. Since K/\mathbb{F} is a global function field over \mathbb{F} . By definition, there exists $y_0 \in K$ which is transcendental over \mathbb{F} . From Theorem 2.1.17, y_0 has a pole P . Thus, $\mathcal{M}_K \neq \emptyset$. \square

2.2 Riemann-Roch Theorem

The aim of this section is to give the Riemann-Roch theorem and present some of its important consequences.

We start with the notion of divisors of a global function field.

Definition 2.2.1. Let K/\mathbb{F} be a global function field. The free abelian group generated by \mathcal{M}_K is called the divisors group of K , and denoted by $(\mathcal{D}_K, +)$.

Remark 2.2.2. If $D \in \mathcal{D}_K$, then $D = \sum_{P \in \mathcal{M}_K} n_P(D)P$, where $n_P(D) \in \mathbb{Z}$ for all $P \in \mathcal{M}_K$ and there are only finitely many $P \in \mathcal{M}_K$ such that $n_P(D) \neq 0$.

Definition 2.2.3. The relation \leq on \mathcal{D}_K defined by, for $(D, D') \in \mathcal{D}_K^2$, $D \leq D'$ if and only if $n_P(D) \leq n_P(D')$ for every $P \in \mathcal{M}_K$, is a partial ordering.

Definition 2.2.4. Let $y \in K$, and denote the set of zeros (respectively poles) of y by $\mathbf{Z}(y)$ (respectively $\mathbf{P}(y)$).

- (i) The divisor $(y)_0 = \sum_{P \in \mathbf{Z}(y)} v_P(y)P$ is called the zero divisor of y .
- (ii) The divisor $(y)_\infty = \sum_{Q \in \mathbf{P}(y)} (-v_Q(y))Q$ is called the pole divisor of y .
- (iii) The divisor $(y) = (y)_0 - (y)_\infty = \sum_{P \in \mathcal{M}_K} v_P(y)P$ is called the principal divisor of y .

Proposition 2.2.5. For all $(y, z) \in K^2 - \{(0, 0)\}$, $(yz) = (y) + (z)$. In particular, the set of principal divisors of K is a subgroup of \mathcal{D}_K .

Proof. Let $(y, z) \in K^2 - \{(0, 0)\}$, and $P \in \mathcal{M}_K$. As v_P is a discrete valuation on K , then $v_P(yz) = v_P(y) + v_P(z)$. So we obtain the result. \square

Definition 2.2.6. Let K/\mathbb{F} be a global function field and let $D = \sum_{P \in \mathcal{M}_K} n_P(D)P$ in \mathcal{D}_K . The Riemann-Roch space associated to D is the set

$$L(D) = \{y \in K : v_P(y) \geq -n_P(D), \text{ for all } P \in \mathcal{M}_K\} \cup \{0\}.$$

Proposition 2.2.7. Let K/\mathbb{F} be a global function field and let $D \in \mathcal{D}_K$. Then $L(D)$ is a finite dimensional \mathbb{F} -vector space. We denote the dimension of $L(D)$ over \mathbb{F} by $l(D)$.

Proof. Let us show that $L(D)$ is an \mathbb{F} -vector space.

From the definition, $L(D) \neq \emptyset$. Let $(x, y) \in L(D)^2$, and $P \in \mathcal{M}_K$. We may assume that $x \neq 0$, and $y \neq 0$. From 2.1.11 (i), we have $v_P(x + y) \geq \min(v_P(x), v_P(y))$. Since $(x, y) \in L(D)^2$, $v_P(x) \geq -n_P(D)$, and $v_P(y) \geq -n_P(D)$. Hence $\min(v_P(x), v_P(y)) \geq -n_P(D)$. Then $v_P(x + y) \geq -n_P(D)$. It follows that $x + y \in L(D)$.

Let $a \in \mathbb{F}$, $x \in L(D)$, and $P \in \mathcal{M}_K$.

Since $a \in \mathcal{O}_P^\times$ and v_P is a discrete valuation, $v_P(a) = 0$. Hence $v_P(ax) = v_P(x) \geq -n_P(D)$. Then, $ax \in L(D)$. These imply that $L(D)$ is an \mathbb{F} -vector space.

From [1, Proposition 1.4.9], $l(D)$ is finite. □

Proposition 2.2.8. The map $\deg : \mathcal{D}_K \rightarrow \mathbb{Z}$ given by $\sum_{P \in \mathcal{M}_K} n_P(D)P \mapsto \sum_{P \in \mathcal{M}_K} n_P(D) \deg_K(P)$ is a homomorphism of abelian groups, and is called the degree map of \mathcal{D}_K .

Proof. From Proposition 2.1.15, we have $\deg_K(P) = [\mathcal{O}_P/P : \mathbb{F}]$ is finite. So, \deg is a well defined and clearly a homomorphism. □

An important theorem is the Riemann-Roch theorem.

Theorem 2.2.9. Let K/\mathbb{F} be a global function field. Then, there exists $W \in \mathcal{D}_K$ and there exists a unique $g_K \in \mathbb{N}$ such that for any $D \in \mathcal{D}_K$,

$$l(D) = \deg(D) + 1 - g_K + l(W - D). \quad (2.2.1)$$

Proof. See [1, Theorem 1.5.15]. □

Definition 2.2.10. Let K/\mathbb{F} be a global function field. The integer g_K defined in the Theorem 2.2.9 is called the genus of K .

A divisor $W \in \mathcal{D}_K$ such that for any $D \in \mathcal{D}_K$,

$$l(D) = \deg(D) + 1 - g_K + l(W - D) \quad (2.2.2)$$

is a canonical divisor of K .

We give two important consequences of the Riemann-Roch theorem in the following corollaries. Often, the Riemann-Roch theorem is used via these corollaries.

Corollary 2.2.11. Let K/\mathbb{F} be a global function field, and let W be a canonical divisor of K . Then, $l(W) = g_K$, and $\deg(W) = 2g_K - 2$.

Proof. By Theorem 2.1.17, we get

$$l(0) = \deg(0) + 1 - g_K + l(W - 0). \quad (2.2.3)$$

From [1], Lemma 1.4.7, (a) $l(0) = 1$, and $\deg(0) = 0$, then $l(W) = g_K$.

On the other hand, we have $l(W) = \deg(W) + 1 - g_K + l(0)$. It follows that $\deg(W) = 2g_K - 2$. \square

Corollary 2.2.12. Let K/\mathbb{F} be a global function field, and let $D \in \mathcal{D}_K$. If $\deg(D) > 2g_K - 2$, then $l(D) = \deg(D) + 1 - g_K$.

Proof. Let $D \in \mathcal{D}_K$ such that $\deg(D) > 2g_K - 2$. From Theorem 2.2.9, we can find $W \in \mathcal{D}_K$ such that $l(D) = \deg(D) + 1 - g_K + l(W - D)$. By Corollary 2.1.18, $\deg(W) = 2g_K - 2$. Thus $\deg(W - D) < 0$. We deduce from [1, Corollary 1.4.12 (b)] that $l(W - D) = 0$. Consequently, $l(D) = \deg(D) + 1 - g_K$. \square

2.3 Finite Extensions of Global Function Fields.

The principal goal in this section is to investigate the finite extensions of a global function field.

Let K/\mathbb{F} be a global function field.

Definition 2.3.1. Let K'/\mathbb{F}_1 be a global function field over a finite field \mathbb{F}_1 . We say that K'/\mathbb{F}_1 is an algebraic extension of K/\mathbb{F} if K' is an algebraic extension of K , and $\mathbb{F}_1 \supseteq \mathbb{F}$.

Definition 2.3.2. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} .

- (i) This extension is said to be finite if $[K' : K] < \infty$.
- (ii) We say that the extension K'/K is a constant field extension if $K' = K\mathbb{F}_1$.

Definition 2.3.3. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} , $P' \in \mathcal{M}_{K'}$, and $P \in \mathcal{M}_K$. We say that P' lies above P if $P' \supseteq P$. In this case, we write $P'|P$.

Proposition 2.3.4. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} , $P' \in \mathcal{M}_{K'}$, and $P \in \mathcal{M}_K$. Let v_P (respectively $v_{P'}$) be the discrete valuation associated to P (respectively P'). The following assertions are equivalent:

- (i) $P'|P$.
- (ii) $\mathcal{O}_{P'} \subseteq \mathcal{O}_P$.

(iii) There exists $e \in \mathbb{N} - \{0\}$, such that for all $y \in K$, $v_{P'}(y) = ev_P(y)$.

Proof. See [1, Proposition 3.1.4]. \square

Corollary 2.3.5. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} , $P' \in \mathcal{M}_{K'}$, and $P \in \mathcal{M}_K$. Suppose that $P'|P$. Then $\mathcal{O}_P = \mathcal{O}_{P'} \cap K$ and $P = P' \cap K$.

Proof. Assume that $P'|P$. Then, by Proposition 2.1.15, (ii), $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. So,

$$\mathcal{O}_P \subseteq \mathcal{O}_{P'} \cap K. \quad (2.3.1)$$

Now, let $y \in \mathcal{O}_{P'} \cap K$. By Proposition 2.1.15, (iii), there exists $e \in \mathbb{N} - \{0\}$ with $v_{P'}(y) = ev_P(y)$. Since $y \in \mathcal{O}_{P'}$, by Proposition 2.1.12, $v_{P'}(y) \geq 0$. It follows that $v_P(y) \geq 0$. Equivalently, $y \in \mathcal{O}_P$. Hence

$$\mathcal{O}_P \supseteq \mathcal{O}_{P'} \cap K. \quad (2.3.2)$$

From (2.3.1) and (2.3.2), we get $\mathcal{O}_P = \mathcal{O}_{P'} \cap K$.

On the other hand, since $P'|P$, $P \subseteq P' \cap K$. By the same reason as above, we deduce that $P \supseteq P' \cap K$. Therefore, $P = P' \cap K$. \square

Definition 2.3.6. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} , $P' \in \mathcal{M}_{K'}$, and $P \in \mathcal{M}_K$ such that $P'|P$.

- (i) The integer $e = e(P'|P)$, which is defined by Proposition 2.3.4, is called the ramification index of P' over P .
- (ii) $P'|P$ is said to be ramified (respectively unramified) if $e(P'|P) > 1$ (respectively $e(P'|P) = 1$).
- (iii) The integer $f(P'|P) = [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$ is called the relative degree of P' over P .

Remark 2.3.7. If $P'|P$, then $e(P'|P)$ is finite. In a global function field, $f(P'|P)$ is also finite.

Proposition 2.3.8. Let K'/\mathbb{F}_1 be a finite algebraic extension of K/\mathbb{F} , and K''/\mathbb{F}_2 a finite algebraic extension of K'/\mathbb{F}_1 . Let $P'' \in \mathcal{M}_{K''}$, $P' \in \mathcal{M}_{K'}$, and $P \in \mathcal{M}_K$ with $P''|P'$, and $P'|P$. Then,

- (i) $f(P''|P) = f(P''|P')f(P'|P)$.
- (ii) $e(P''|P) = e(P''|P')e(P'|P)$.

Proof. See [1, Proposition 3.1.6, (b)]. \square

Definition 2.3.9. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} . The map $\text{Con}_{K'/K} : \mathcal{D}_K \rightarrow \mathcal{D}_{K'}$, $\sum_{P \in \mathcal{D}_K} n_P P \mapsto \sum_{P \in \mathcal{D}_K} n_P (\sum_{P'|P} e(P'|P) P')$, is called the conorm map of K'/K .

The following proposition implies that the map $\text{Con}_{K'/K}$ is well defined.

Proposition 2.3.10. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} , and let $P \in \mathcal{M}_K$. Then $\{P' \in \mathcal{M}_{K'} : P'|P\}$ is finite.

Proof. See [1, Proposition 3.1.7]. □

Corollary 2.3.11. Let K'/\mathbb{F}_1 be an algebraic extension of K/\mathbb{F} . Then the map $\text{Con}_{K'/K}$ is well defined.

Here are some important properties of a particular case of algebraic extension of a function field.

Theorem 2.3.12. Let $r \in \mathbb{N} - \{0, 1\}$, and let $K' = K\mathbb{F}_r$. Suppose that \mathbb{F} is the full constant field of K . Then,

- (i) For all $P \in \mathcal{M}_K$, for all $P' \in \mathcal{M}_{K'}$ such that $P'|P$, we have $e(P'|P) = 1$.
- (ii) \mathbb{F}_r is the full constant field of K' .
- (iii) $g_{K'} = g_K$.
- (iv) If $D \in \mathcal{D}_K$, then $\deg(\text{Con}_{K'/K}(D)) = \deg(D)$.
- (v) Suppose that $P' \in \mathcal{M}_{K'}$, $P' \cap K = P$, then $\mathcal{O}_{P'}/P' = (\mathcal{O}_P/P)\mathbb{F}_r$, the compositum of \mathcal{O}_P/P , and \mathbb{F}_r .

Proof. (i) Let $P \in \mathcal{M}_K$, $P' \in \mathcal{M}_{K'}$ such that $P'|P$. Since K'/K is a constant field extension, then, from [1, Theorem 3.6.3 (a)], we get $e(P'|P) = 1$.

(ii) As K'/K is a constant field extension, then, from [1, Theorem 3.6.1 (a)], \mathbb{F}_r is the full constant field of K' .

(iii) Since K'/K is a constant field extension, then, from [1, Theorem 3.6.3 (b)], we obtain $g_{K'} = g_K$.

(iv) Suppose $D \in \mathcal{D}_K$, then, by [1, Theorem 3.6.3 (c)], $\deg(\text{Con}_{K'/K}(D)) = \deg(D)$.

(v) Suppose that $P' \in \mathcal{M}_{K'}$, $P' \cap K = P$, then, by [1, Theorem 3.6.3 (g)], $\mathcal{O}_{P'}/P' = (\mathcal{O}_P/P)\mathbb{F}_r$. □

2.4 Some Tools From Commutative Algebra.

In this section, we present some of the important properties of Dedekind domains.

Lemma 2.4.1. Let R be a Dedekind domain. Then

$$R = \bigcap_{\mathfrak{p} \in \mathcal{M}_R} R_{\mathfrak{p}}. \quad (2.4.1)$$

Proof. Since a Dedekind domain is an integral domain, then, from [3, Lemma 3.17], we get the result. \square

Theorem 2.4.2. Let R be a Dedekind domain with quotient field K . Let L be a finite algebraic extension of K , and R' be the integral closure of R in K . If \mathfrak{p} is a proper prime ideal of R such that $\mathfrak{p}R' = \prod_{i=1}^s \mathfrak{P}_i^{e_i}$, where $s \in \mathbb{N} - \{0\}$, and for any $j \in \{1, \dots, s\}$, $e_j \in \mathbb{N} - \{0\}$, and $\{\mathfrak{P}_j : j \in \{1, \dots, s\}\}$ is the set of prime ideals of R' laying above \mathfrak{p} . Then, we obtain:

(i)

$$\sum_{j=1}^s e_j f(\mathfrak{P}_j | \mathfrak{p}) \leq [L : K], \quad (2.4.2)$$

where, for any $j \in \{1, \dots, s\}$, $f(\mathfrak{P}_j | \mathfrak{p}) = [R'/\mathfrak{P}_j : R/\mathfrak{p}]$.

(ii)

$$\sum_{j=1}^s e_j f(\mathfrak{P}_j | \mathfrak{p}) = [L : K], \quad (2.4.3)$$

if and only if $R'_{(R-\mathfrak{p})}$ is a finitely generated $R_{\mathfrak{p}}$ -module.

Proof. See [4, Theorem 21, p. 285]. \square

Proposition 2.4.3. With the same assumptions as in Theorem 2.4.2, if L/K is a Galois extension, then

$$[L : K] = e_1 f(\mathfrak{P}_1 | \mathfrak{p}) s. \quad (2.4.4)$$

Proof. See [4, Theorem 22, p. 289]. \square

Chapter 3

The Riemann Zeta Function for Global Function Fields.

In this Chapter, we define the Riemann zeta function for global function fields. We start with the notion of the ring of integers A of a global function field K/\mathbb{F} . Then, we define the function zeta and see an analogue of the functional equation of the Riemann zeta function in the number fields case.

3.1 The Ring of Integers

Considering a place (∞) of a global function field K/\mathbb{F} and the ring of integers A of K/\mathbb{F} with respect to (∞) , the main goal of this section is to show that A is a Dedekind domain, and there is a bijective correspondence between the set of prime ideals of A and the set of the places of K/\mathbb{F} without (∞) .

Let K/\mathbb{F} be a global function field with constant field \mathbb{F} and genus g_K . Let (∞) be a place of K . Let \mathcal{M}_K be the set of all places of K/\mathbb{F} . If R is a ring, we denote by \mathcal{M}_R the set of all nonzero prime ideals of R .

Definition 3.1.1. The subring $A = \{f \in K : v_P(f) \geq 0, \text{ for any } P \in \mathcal{M}_K - \{(\infty)\}\}$ of K is called the ring of integers of K with respect to (∞) .

Our main study in this section is the ring A .

If $x \in K$, we recall that $\mathbf{P}(x)$ is the set of all poles of x .

Proposition 3.1.2. There exists $x \in K$ such that $\mathbf{P}(x) = \{(\infty)\}$.

Proof. Let $M \in \mathbb{N}$ with $M \geq 2g_K - 2$. Then $\deg(M(\infty)) > 2g_K - 2$. By Corollary 2.2.12, $\dim_{\mathbb{F}}(L(M(\infty))) = M \deg_K((\infty)) - g_K + 1$ and $\dim_{\mathbb{F}}(L((M+1)(\infty))) = (M+1) \deg_K((\infty)) - g_K + 1$. Since $M+1 > M$, $L(M(\infty)) \subseteq L((M+1)(\infty))$, and $\dim_{\mathbb{F}}(L((M+1)(\infty))) > \dim_{\mathbb{F}}(L(M(\infty)))$. Hence, $L(M(\infty)) \subsetneq L((M+1)(\infty))$. Thus, there exists $x \in L((M+1)(\infty))$ such that $x \notin L(M(\infty))$.

$L(M(\infty))$. These imply that $v_P(x) \geq 0$, for every $P \in \mathcal{M}_K - \{(\infty)\}$, $v_{(\infty)}(x) < -M$, and $v_{(\infty)}(x) \geq -(M + 1)$. Therefore, (∞) is the only pole of x . \square

Theorem 3.1.3. *Consider the element x given in Proposition 3.1.2. Let R be the integral closure of $\mathbb{F}[x]$ in K . Then, the map $\psi : \mathcal{M}_R \longrightarrow \mathcal{M}_K - \{(\infty)\}$ given by $\mathfrak{p} \longmapsto \mathfrak{p}R_{\mathfrak{p}}$, is well defined and bijective.*

In order to prove this theorem, let us show the following lemmas.

Lemma 3.1.4. We use the same notation as in Theorem 3.1.3. Let $P \in \mathcal{M}_K - \{(\infty)\}$. Then $P \cap R \neq \{0\}$.

Proof. Suppose $P \cap R = \{0\}$. Since R is the integral closure of $\mathbb{F}[x]$ in K , then $\text{Quot}(R) = K$. On one hand, $R/(P \cap R) \simeq R$, then the map $i : R/(P \cap R) \longrightarrow \mathcal{O}_P/P$, $y \longmapsto y + P$ is an embedding of rings. This gives an embedding of fields $i_1 : \text{Quot}(R) \longrightarrow \mathcal{O}_P/P$, such that for any $\frac{u}{v} \in \text{Quot}(R) - \{0\}$, $i_1(\frac{u}{v}) = \frac{i(u)}{i(v)}$.

Since $\text{Quot}(R) = K$ and, by Proposition 2.1.15, $(\mathcal{O}_P/P)/\mathbb{F}$ is a finite extension of fields, K/\mathbb{F} is a finite extension. Thus,

- (1) K/\mathbb{F} is an algebraic extension.

On the other hand, since K/\mathbb{F} is a global function field with constant field \mathbb{F} ,

- (2) K/\mathbb{F} is transcendental

(1) and (2) give us a contradiction. \square

Lemma 3.1.5. Using the same notation as in Theorem 3.1.3, let $P \in \mathcal{M}_K - \{(\infty)\}$. If $\mathfrak{p} = P \cap R$, then $R_{\mathfrak{p}} = \mathcal{O}_P$.

Proof. From Lemma 3.1.4, \mathfrak{p} is non-zero prime ideal of R . Since R is the integral closure of $\mathbb{F}[x]$, $\mathbb{F}[x]$ is a Dedekind domain, and $K/\mathbb{F}(x)$ is a finite extension of function fields, then R is a Dedekind domain. It follows that $R_{\mathfrak{p}}$ is a discrete valuation ring.

Claim 1: $R_{\mathfrak{p}} \subseteq \mathcal{O}_P$. Indeed, let $\frac{a}{b} \in R_{\mathfrak{p}}$. Then $a \in R$, and $b \in R - \mathfrak{p}$. If $R \subseteq \mathcal{O}_P$, then $v_P(a) \geq 0$ and $b \in \mathcal{O}_P^{\times}$. It follows that $v_P(\frac{a}{b}) \geq 0$ and the claim follows. So, let us so that $R \subseteq \mathcal{O}_P$.

Since $P \in \mathcal{M}_K - \{(\infty)\}$, Proposition 3.1.2 implies that $x \in \mathcal{O}_P$. Since \mathcal{O}_P is a valuation ring of the function field K/\mathbb{F} , $\mathbb{F} \subsetneq \mathcal{O}_P$. Hence, $\mathbb{F}[x] \subseteq \mathcal{O}_P$. Thus, $i_{c_K}(\mathbb{F}[x]) \subseteq \mathcal{O}_P$, because \mathcal{O}_P is integrally closed with $\text{Quot}(\mathcal{O}_P) = K$. This implies that $R \subseteq \mathcal{O}_P$.

Now, since R is a Dedekind domain, and \mathfrak{p} is proper prime ideal of R , $R_{\mathfrak{p}}$ is a discrete valuation ring of R . Hence, $R_{\mathfrak{p}}$ is a maximal proper subring of $K = \text{Quot}(R_{\mathfrak{p}})$. The Claim 1 and the fact that \mathcal{O}_P is a proper subring of K imply that $R_{\mathfrak{p}} = \mathcal{O}_P$. \square

Proof of Theorem 3.1.3. First of all let us show that ψ is well defined. Let $\mathfrak{p} \in \mathcal{M}_R$. Since $\mathbb{F}[x]$ is a Dedekind domain, and $R = ic_K(\mathbb{F}[x])$, R is also a Dedekind domain. It implies that $R_{\mathfrak{p}}$ is a discrete valuation ring of K with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. Moreover $\mathbb{F} \subsetneq R_{\mathfrak{p}}$, so $R_{\mathfrak{p}}$ is a valuation ring of K/\mathbb{F} . Hence $\mathfrak{p}R_{\mathfrak{p}} \in \mathcal{M}_K$. If $\mathfrak{p}R_{\mathfrak{p}} \neq (\infty)$, then ψ is well defined. Set $P_0 = \mathfrak{p}R_{\mathfrak{p}}$. Since $x \in R$, and $R \subseteq R_{\mathfrak{p}}$, then $v_{P_0}(x) \geq 0$. From Proposition 3.1.2, we deduce that $\mathfrak{p}R_{\mathfrak{p}} \neq (\infty)$.

Let us prove that ψ is one to one. Let \mathfrak{p}_0 , and \mathfrak{p}_1 be elements of \mathcal{M}_R such that $\psi(\mathfrak{p}_0) = \psi(\mathfrak{p}_1)$. Then, $\mathfrak{p}_0R_{\mathfrak{p}_0} \cap R = \mathfrak{p}_1R_{\mathfrak{p}_1} \cap R$, that is $\mathfrak{p}_0 = \mathfrak{p}_1$.

Finally, if $P \in \mathcal{M}_K - \{(\infty)\}$, by Lemma 3.1.5, there exists $\mathfrak{p} = P \cap R \in \mathcal{M}_R$ with $R_{\mathfrak{p}} = \mathcal{O}_P$. Hence, there exists $\mathfrak{p} \in \mathcal{M}_R$ which satisfies $P = \psi(\mathfrak{p})$. Thus, ψ is onto.

We deduce that ψ is a bijective map. \square

Corollary 3.1.6. The ring of integers A is equal to the ring R defined in Theorem 3.1.3. In particular, A is a Dedekind domain.

Proof. Since R is a Dedekind domain, then, from Lemma 2.4.1

$$R = \bigcap_{\mathfrak{p} \in \mathcal{M}_R} R_{\mathfrak{p}}.$$

By Theorem 3.1.3, we obtain

$$\begin{aligned} R &= \bigcap_{P \in \mathcal{M}_K - \{(\infty)\}} R_{\psi^{-1}(P)} \\ R &= \bigcap_{P \in \mathcal{M}_K - \{(\infty)\}} \mathcal{O}_P \\ R &= A. \end{aligned}$$

Moreover, since R is a Dedekind domain then A is a Dedekind domain. \square

3.2 The Riemann Zeta Function of the Ring of Integers

In the previous section, we have seen, from Corollary 3.1.6, that the ring of integers A is a Dedekind domain. In this section, we discuss the analogue of the Riemann zeta function for number fields. We begin by giving the definition of a norm of an integral ideal of A .

Recall that \mathcal{M}_A is the set of non-zero prime ideals of A .

Definition 3.2.1. Let I be a non-zero ideal of A . The norm of I is defined by $\mathcal{N}_A(I) = |A/I|$.

Definition 3.2.2. Consider the element x defined in Proposition 3.1.2. Let $g(x)$ be a nonzero polynomial in $\mathbb{F}[x]$. The degree of $I = (g(x))$ is defined by $\deg_{\mathbb{F}[x]}(I) = \deg_x(g(x))$.

Proposition 3.2.3. Let \mathfrak{p} be a non-zero prime ideal of A . Then $\mathcal{N}_A(\mathfrak{p})$ is finite and we have

$$\mathcal{N}_A(\mathfrak{p}) = q^{[A/\mathfrak{p}:\mathbb{F}]}.$$

Proof. Since $(A/\mathfrak{p}) \simeq A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, by Theorem 3.1.3, $\mathfrak{p}A_{\mathfrak{p}}$ is a place of K . Therefore, from Proposition 2.1.15, $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is finite. Thus A/\mathfrak{p} is finite.

Now, the embeddings of fields

$$\mathbb{F} \hookrightarrow \mathbb{F}[x]/(\mathfrak{p} \cap \mathbb{F}[x]) \hookrightarrow A/\mathfrak{p}$$

imply that A/\mathfrak{p} is an \mathbb{F} -vector space of dimension $[A/\mathfrak{p} : \mathbb{F}]$. Since $|\mathbb{F}| = q$, $\mathcal{N}_A(\mathfrak{p}) = q^{[A/\mathfrak{p}:\mathbb{F}]}$. \square

Definition 3.2.4. Let \mathfrak{p} be a non-zero prime ideal of A . The degree of \mathfrak{p} is the positive integer defined by $\deg_A(\mathfrak{p}) = [A/\mathfrak{p} : \mathbb{F}]$.

Proposition 3.2.5. Let \mathfrak{p} be a non-zero prime ideal of A , and let e be a non-zero natural number. Then A/\mathfrak{p}^e is an A/\mathfrak{p} -vector space of finite dimension e , and

$$\mathcal{N}_A(\mathfrak{p}^e) = q^{e \deg_A(\mathfrak{p})}.$$

Proof. For $i \in \{1, \dots, e\}$, let us show that the map $\cdot : A/\mathfrak{p} \times \mathfrak{p}^i/\mathfrak{p}^{i+1} \longrightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1}$ given by $(a + \mathfrak{p}, c + \mathfrak{p}^{i+1}) \longmapsto ac + \mathfrak{p}^{i+1}$ yields a vector space structure over A/\mathfrak{p} on $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. It suffices to prove that this map is well defined. So, suppose we have $a + \mathfrak{p} = b + \mathfrak{p}$, and $c + \mathfrak{p}^{i+1} = d + \mathfrak{p}^{i+1}$, where $a, b \in A$, and $c, d \in \mathfrak{p}^i$. Hence, $bd + \mathfrak{p}^{i+1} = (a + \mathfrak{p})(c + \mathfrak{p}^{i+1}) + \mathfrak{p}^{i+1}$. That is $bd + \mathfrak{p}^{i+1} = ac + \mathfrak{p}^{i+1}$. Since $c \in \mathfrak{p}^i$, $\mathfrak{p}c \subseteq \mathfrak{p}^{i+1}$. Thus, $bd + \mathfrak{p}^{i+1} = ac + \mathfrak{p}^{i+1}$. Therefore, the map \cdot is well defined. Moreover, since A is a Dedekind domain, $\dim_{A/\mathfrak{p}}(\mathfrak{p}^i/\mathfrak{p}^{i+1}) = 1$.

Claim 1: $A/\mathfrak{p}^e \simeq A/\mathfrak{p} \oplus \mathfrak{p}/\mathfrak{p}^2 \oplus \mathfrak{p}^2/\mathfrak{p}^3 \oplus \dots \oplus \mathfrak{p}^{e-1}/\mathfrak{p}^e$, as A/\mathfrak{p} -vector space. Indeed, by the third ring isomorphism theorem we have $A/\mathfrak{p} \simeq (A/\mathfrak{p}^e)/(\mathfrak{p}/\mathfrak{p}^e)$. This implies that $A/\mathfrak{p}^e \simeq A/\mathfrak{p} \oplus \mathfrak{p}/\mathfrak{p}^e$ as an A/\mathfrak{p} -vector space. Using again the third ring isomorphism theorem, $\mathfrak{p}/\mathfrak{p}^2 \simeq (\mathfrak{p}/\mathfrak{p}^e)/(\mathfrak{p}^2/\mathfrak{p}^e)$. Thus $\mathfrak{p}/\mathfrak{p}^e \simeq \mathfrak{p}/\mathfrak{p}^2 \oplus \mathfrak{p}^2/\mathfrak{p}^e$ as an A/\mathfrak{p} -vector space. It follows that $A/\mathfrak{p}^e \simeq A/\mathfrak{p} \oplus \mathfrak{p}/\mathfrak{p}^2 \oplus \mathfrak{p}^2/\mathfrak{p}^e$. And so on, we have $A/\mathfrak{p}^e \simeq A/\mathfrak{p} \oplus \mathfrak{p}/\mathfrak{p}^2 \oplus \dots \oplus \mathfrak{p}^{e-1}/\mathfrak{p}^e$ as an A/\mathfrak{p} -vector space as claimed.

Now, since $\dim_{A/\mathfrak{p}}(\mathfrak{p}^i/\mathfrak{p}^{i+1}) = 1$, for $i = 1, \dots, e$, Claim 1 implies that $\dim_{A/\mathfrak{p}}(A/\mathfrak{p}^e) = e$, as desired.

For the second assertion, since A/\mathfrak{p}^e is an A/\mathfrak{p} - vector space of finite dimension e , then

$$|A/\mathfrak{p}^e| = |A/\mathfrak{p}|^e.$$

Using Proposition 3.2.3, we get

$$|A/\mathfrak{p}^e| = q^{e[A/\mathfrak{p}:\mathbb{F}]}.$$

□

Proposition 3.2.6. If I is a non-zero ideal of A , then $\mathcal{N}_A(I)$ is finite. More precisely, if $I = \prod_{j=1}^s \mathfrak{p}_j^{e_j}$, where $s \in \mathbb{N} - \{0\}$, $e_j \in \mathbb{N} - \{0\}$, and \mathfrak{p}_j is a non-zero prime ideal of A for $j \in \{1, \dots, s\}$, then

$$\mathcal{N}_A(I) = q^{\sum_{j=1}^s e_j [A/\mathfrak{p}_j:\mathbb{F}]}.$$

Proof. By the chinese reminder theorem, we have $A/I \simeq \prod_{j=1}^s A/\mathfrak{p}_j^{e_j}$. From Proposition 3.2.5, we deduce that for any $j \in \{1, \dots, s\}$, $A/\mathfrak{p}_j^{e_j}$ is finite so A/I is finite, and

$$\begin{aligned} \mathcal{N}_A(I) &= \prod_{j=1}^s q^{e_j [A/\mathfrak{p}_j:\mathbb{F}]}, \\ \mathcal{N}_A(I) &= q^{\sum_{j=1}^s e_j [A/\mathfrak{p}_j:\mathbb{F}]}. \end{aligned}$$

□

Corollary 3.2.7. Suppose that I , and J are non-zero ideals of A , with $I + J = A$. Then, $\mathcal{N}_A(IJ) = \mathcal{N}_A(I)\mathcal{N}_A(J)$.

Proof. By assumption we have, $I = \prod_{j=1}^s \mathfrak{p}_j^{e_j}$, and $J = \prod_{j=1}^t \mathfrak{q}_j^{l_j}$, where $e_j \in \mathbb{N} - \{0\}$, for $j \in \{1, \dots, s\}$, $s \in \mathbb{N} - \{0\}$, $l_j \in \mathbb{N} - \{0\}$, for $j \in \{1, \dots, t\}$, and $t \in \mathbb{N} - \{0\}$. Moreover, since $I + J = A$, for all $j \in \{1, \dots, s\}$, and for all $k \in \{1, \dots, t\}$, $\mathfrak{p}_j \neq \mathfrak{q}_k$. From Proposition 3.2.6, it follows that

$$\begin{aligned} \mathcal{N}_A(IJ) &= \mathcal{N}_A\left(\prod_{j=1}^s \mathfrak{p}_j^{e_j} \prod_{j=1}^t \mathfrak{q}_j^{l_j}\right) \\ \mathcal{N}_A(IJ) &= \prod_{j=1}^s q^{e_j [A/\mathfrak{p}_j:\mathbb{F}]} \prod_{j=1}^t q^{l_j [A/\mathfrak{p}_j:\mathbb{F}]} \end{aligned}$$

Thus, we get $\mathcal{N}_A(IJ) = \mathcal{N}_A(I)\mathcal{N}_A(J)$.

□

An important theorem is the following,

Theorem 3.2.8. *Let $Id(A)$ be the set of non-zero ideals of A . Then, the power series $\sum_{I \in Id(A)} \mathcal{N}_A(I)^{-z}$ converges absolutely in the region $\{z \in \mathbb{C} : Re(z) > 1\}$.*

Before proving this theorem, let us show a lemma.

Lemma 3.2.9. The power series $\theta(z) = \sum_{\mathfrak{p} \in \mathcal{M}_A} \mathcal{N}_A(\mathfrak{p})^{-z}$ converges absolutely in the region $\{s \in \mathbb{C} : Re(s) > 1\}$.

Proof. Let $z \in \{s \in \mathbb{C} : Re(s) > 1\}$. We have the disjoint union $\mathcal{M}_A = \sqcup_{p \in \mathcal{M}_{\mathbb{F}[x]}} \{\mathfrak{p} \in \mathcal{M}_A : \mathfrak{p}|p\}$. Then

$$\theta(z) = \sum_{p \in \mathcal{M}_{\mathbb{F}[x]}} \sum_{\mathfrak{p}|p} \mathcal{N}_A(\mathfrak{p})^{-z}.$$

Since x is transcendental over \mathbb{F} , and K is a function field over \mathbb{F} , then $K/\mathbb{F}(x)$ is finite.

Since the ring $\mathbb{F}[x]$ is a Dedekind domain with integral closure A in K , and $K/\mathbb{F}(x)$ is a finite extension of fields, if $p \in \mathcal{M}_{\mathbb{F}[x]}$, by Theorem 2.4.2, we have

$$\sum_{j=1}^s e(\mathfrak{p}_j|p) f(\mathfrak{p}_j|p) \leq [K : \mathbb{F}(x)], \quad (3.2.1)$$

where s is the number of prime ideals of A lying above p . Since, for any $j \in \{1, \dots, s\}$, $e(\mathfrak{p}_j|p) \geq 1$, and $f(\mathfrak{p}_j|p) \geq 1$, then $s \leq [K : \mathbb{F}(x)]$. That is

$$|\{\mathfrak{p} \in \mathcal{M}_A : \mathfrak{p}|p\}| \leq n, \quad (3.2.2)$$

where $n = [K : \mathbb{F}(x)]$.

By the triangle inequality:

$$\left| \sum_{\mathfrak{p}|p} \mathcal{N}_A(\mathfrak{p})^{-z} \right| \leq \sum_{\mathfrak{p}|p} \mathcal{N}_A(\mathfrak{p})^{-Re(z)}.$$

As, for any $\mathfrak{p}|p$, $\mathcal{N}_A(\mathfrak{p}) = q^{\deg_{\mathbb{F}[x]}(p)f(\mathfrak{p}|p)}$, $f(\mathfrak{p}|p) \geq 1$, and $Re(z) > 1$, then, for any $\mathfrak{p}|p$,

$$\mathcal{N}_A(\mathfrak{p})^{-Re(z)} \leq q^{-\deg_{\mathbb{F}[x]}(p)Re(z)}.$$

From (3.2.2), we deduce that

$$\sum_{\mathfrak{p}|p} \mathcal{N}_A(\mathfrak{p})^{-Re(z)} \leq nq^{-\deg_{\mathbb{F}[x]}(p)Re(z)}. \quad (3.2.3)$$

Now, let $T \in \mathbb{R}$ with $T > 0$ and set $\mathcal{M}_{\mathbb{F}[x],T} = \{p \in \mathcal{M}_{\mathbb{F}[x]} : \deg_{\mathbb{F}[x]}(p) \leq T\}$. Then, by (3.2.3), we get

$$\sum_{p \in \mathcal{M}_{\mathbb{F}[x],T}} \sum_{\mathfrak{p}|p} \mathcal{N}_A(\mathfrak{p})^{-\operatorname{Re}(z)} \leq n \sum_{p \in \mathcal{M}_{\mathbb{F}[x],T}} q^{-\deg_{\mathbb{F}[x]}(p)\operatorname{Re}(z)}.$$

That is

$$\sum_{p \in \mathcal{M}_{\mathbb{F}[x],T}} \sum_{\mathfrak{p}|p} \mathcal{N}_A(\mathfrak{p})^{-\operatorname{Re}(z)} \leq n \sum_{d=1}^{\lfloor T \rfloor} |\{p \in \mathcal{M}_{\mathbb{F}[x],T} : \deg_{\mathbb{F}[x]}(p) = d\}| q^{-d\operatorname{Re}(z)},$$

where $\lfloor T \rfloor$ denotes the greatest integer less than or equal to T . Since

$$|\{p \in \mathcal{M}_{\mathbb{F}[x],T} : \deg_{\mathbb{F}[x]}(p) = d\}| \leq q^d,$$

by setting $M = n \sum_{d=1}^{\infty} q^{d-d\operatorname{Re}(z)}$, we have

$$\sum_{p \in \mathcal{M}_{\mathbb{F}[x],T}} \sum_{\mathfrak{p}|p} \mathcal{N}_A(\mathfrak{p})^{-\operatorname{Re}(z)} \leq M.$$

Since $\operatorname{Re}(z) > 1$, $M < \infty$. Moreover, it is clear that M does not depend on T . That proves that there exists $M \in \mathbb{R}$ such that for any $T \in \mathbb{R}$ with $T > 0$

$$\sum_{p \in \mathcal{M}_{\mathbb{F}[x],T}} \sum_{\mathfrak{p}|p} \mathcal{N}(\mathfrak{p})^{-\operatorname{Re}(z)} \leq M.$$

In other words, $\sum_{p \in \mathcal{M}_{\mathbb{F}[x]}} \sum_{\mathfrak{p}|p} \mathcal{N}(\mathfrak{p})^{-\operatorname{Re}(z)}$ is finite. It follows that $\sum_{\mathfrak{p} \in \mathcal{M}_A} \mathcal{N}_A(\mathfrak{p})^{-z}$ converges absolutely when $\operatorname{Re}(z) > 1$. \square

Now, let us prove our theorem.

Proof of Theorem 3.2.8. Let $T \in \mathbb{R}$ with $T > 0$, and $z \in \mathbb{C}$ such that $\operatorname{Re}(z) > 1$. Set $\operatorname{Id}(A, T) = \{I \in \operatorname{Id}(A) : \mathcal{N}_A(I) \leq T\}$, and $\mathcal{M}_{A,T} = \{\mathfrak{p} \in \mathcal{M}_A : \mathcal{N}_A(\mathfrak{p}) \leq T\}$.

Claim 1:

$$\left| \sum_{I \in \operatorname{Id}(A,T)} \mathcal{N}_A(I)^{-z} \right| \leq \prod_{\mathfrak{p} \in \mathcal{M}_{A,T}} \left(\sum_{j=0}^{\infty} \mathcal{N}_A(\mathfrak{p})^{-j\operatorname{Re}(z)} \right). \quad (3.2.4)$$

Indeed, we have

$$\mathcal{M}_{A,T} = \sqcup_{p \in \mathcal{M}_{\mathbb{F}[x],T}} \{\mathfrak{p} \in \mathcal{M}_A : \mathfrak{p}|p\}.$$

From Theorem 2.4.2, $\{\mathfrak{p} \in \mathcal{M}_A : \mathfrak{p}|p\}$ is finite for every $p \in \mathcal{M}_{\mathbb{F}[x],T}$. Since $\mathcal{M}_{\mathbb{F}[x],T}$ is clearly finite, $\mathcal{M}_{A,T}$ is finite. It follows that

$$\prod_{\mathfrak{p} \in \mathcal{M}_{A,T}} \left(\sum_{j=0}^{\infty} \mathcal{N}_A(\mathfrak{p})^{-j\operatorname{Re}(z)} \right) = 1 + \sum_{\substack{l \in \mathbb{N} - \{0\}, k_1, \dots, k_l \geq 1, \\ \mathcal{N}_A(\mathfrak{p}_{i_j}) \leq T, \text{ for } j \in \{1, \dots, l\}}} \prod_{j=1}^l \mathcal{N}_A(\mathfrak{p}_{i_j})^{-k_j \operatorname{Re}(z)}.$$

Since the norm map \mathcal{N}_A is multiplicative by Corollary 3.3.3, we have

$$\prod_{\mathfrak{p} \in \mathcal{M}_{A,T}} \left(\sum_{j=0}^{\infty} \mathcal{N}_A(\mathfrak{p})^{-jRe(z)} \right) = 1 + \sum_{\substack{l \in \mathbb{N} - \{0\}, k_1, \dots, k_l \geq 1, \\ \mathcal{N}_A(\mathfrak{p}_{i_j}) \leq T, \text{ for } j \in \{1, \dots, l\}}} (\mathcal{N}_A(\prod_{j=1}^l \mathfrak{p}_{i_j}^{k_j}))^{-Re(z)}.$$

So,

$$1 + \sum_{\substack{l \in \mathbb{N} - \{0\}, k_1, \dots, k_l \geq 1, \\ \mathcal{N}_A(\mathfrak{p}_{i_j}) \leq T, \text{ for } j \in \{1, \dots, l\}}} (\mathcal{N}_A(\prod_{j=1}^l \mathfrak{p}_{i_j}^{k_j}))^{-Re(z)} \geq \sum_{I \in Id(A,T)} \mathcal{N}_A(I)^{-Re(z)}.$$

And this is because if $I \in Id(A, T)$, then $I = \prod_{t=1}^s \mathfrak{p}_{i_t}^{k_t}$, for some $s \in \mathbb{N} - \{0\}$, such that for any $t \in \{1, \dots, s\}$, $k_t \geq 1$, and $\mathfrak{p}_{i_t} \in \mathcal{M}_{A,T}$. Using the triangle inequality, we get the Claim 1.

We observe also that for $\mathfrak{p} \in \mathcal{M}_{A,T}$, the geometric series $\sum_{j \geq 0} \mathcal{N}_A(\mathfrak{p})^{-jRe(z)}$ converges absolutely when $Re(z) > 1$.

Claim 2: For $\mathfrak{p} \in \mathcal{M}_{A,T}$, we have

$$\sum_{j=0}^{\infty} \mathcal{N}_A(\mathfrak{p})^{-jRe(z)} \leq 1 + 3(\mathcal{N}_A(\mathfrak{p}))^{-Re(z)}.$$

Indeed, let $\mathfrak{p} \in \mathcal{M}_{A,T}$. Then

$$\sum_{j=0}^{\infty} \mathcal{N}_A(\mathfrak{p})^{-jRe(z)} = \frac{1}{1 - \mathcal{N}_A(\mathfrak{p})^{-Re(z)}}.$$

Since $q \geq 2$, $Re(z) > 1$, and $\deg_A(\mathfrak{p}) \geq 1$, we have

$$q^{-Re(z) \deg_A(\mathfrak{p})} < \frac{1}{2}.$$

So,

$$\begin{aligned} 1 + 3q^{-Re(z) \deg_A(\mathfrak{p})} &< \frac{5}{2}, \\ 1 + 3q^{-Re(z) \deg_A(\mathfrak{p})} &< 3. \end{aligned}$$

Thus,

$$\frac{1}{1 - \mathcal{N}_A(\mathfrak{p})^{-Re(z)}} \leq 3.$$

It follows that

$$1 + \frac{\mathcal{N}_A(\mathfrak{p})^{-Re(z)}}{1 - \mathcal{N}_A(\mathfrak{p})^{-Re(z)}} \leq 1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)},$$

that is

$$\frac{1}{1 - \mathcal{N}_A(\mathfrak{p})^{-Re(z)}} \leq 1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)},$$

as claimed.

It follows from Claim 1 and Claim 2 that

$$\sum_{I \in Id(A, T)} |\mathcal{N}_A(I)^{-z}| \leq \prod_{\mathfrak{p} \in \mathcal{M}_{A, T}} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}).$$

As $1 + 3\mathcal{N}(\mathfrak{p})^{-Re(z)} > 1$, for any $\mathfrak{p} \in \mathcal{M}_A$, then

$$\prod_{\mathfrak{p} \notin \mathcal{M}_{A, T}} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}) > 1.$$

Since $\prod_{\mathfrak{p} \in \mathcal{M}_{A, T}} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}) > 0$, then

$$\prod_{\mathfrak{p} \in \mathcal{M}_{A, T}} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}) \prod_{\mathfrak{p} \notin \mathcal{M}_{A, T}} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}) > \prod_{\mathfrak{p} \in \mathcal{M}_{A, T}} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}).$$

That is,

$$\prod_{\mathfrak{p} \in \mathcal{M}_A} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}) > \prod_{\mathfrak{p} \in \mathcal{M}_{A, T}} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}).$$

Therefore,

$$\sum_{I \in Id(A, T)} |\mathcal{N}_A(I)^{-z}| \leq \prod_{\mathfrak{p} \in \mathcal{M}_A} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}).$$

From Lemma 3.2.9, the power series $3 \sum_{\mathfrak{p} \in \mathcal{M}_A} \mathcal{N}_A(\mathfrak{p})^{-z}$ converges absolutely, then by the theory of the infinite product ([5, Theorem 1, p. 133]), $\prod_{\mathfrak{p} \in \mathcal{M}_A} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)})$ converges. Thus, there exists $B(z) = \prod_{\mathfrak{p} \in \mathcal{M}_A} (1 + 3\mathcal{N}_A(\mathfrak{p})^{-Re(z)}) \in \mathbb{R}$ such that for every $T > 0$

$$\sum_{I \in Id(A, T)} |\mathcal{N}_A(I)^{-z}| \leq B(z).$$

That is, the series $\sum_{I \in Id(A)} \mathcal{N}_A(I)^{-z}$ converges absolutely. □

Definition 3.2.10. The function $\zeta_A : \mathbb{C} \rightarrow \mathbb{C}$ which is given by $\zeta_A(z) = \sum_{I \in Id(A)} \mathcal{N}_A(I)^{-z}$ for $z \in \{s \in \mathbb{C} : Re(s) > 1\}$ is called the Riemann zeta function for the ring A .

As in the number fields case, the Riemann zeta function for the ring A also satisfies the Euler product formula.

Proposition 3.2.11. The infinite product $\prod_{\mathfrak{p} \in \mathcal{M}_A} (1 - \mathcal{N}_A(\mathfrak{p})^{-z})^{-1}$ converges absolutely in $\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Re}(z) > 1\}$, and for $z \in \mathcal{H}$, we have

$$\zeta_A(z) = \prod_{\mathfrak{p} \in \mathcal{M}_A} (1 - \mathcal{N}_A(\mathfrak{p})^{-z})^{-1}$$

Proof. Let $z \in \mathcal{H}$. Set $E(z) = \prod_{\mathfrak{p} \in \mathcal{M}_A} (1 - \mathcal{N}_A(\mathfrak{p})^{-z})^{-1}$. Then,

$$\begin{aligned} E(z) &= \prod_{\mathfrak{p} \in \mathcal{M}_A} (1 - q^{-z \deg_A(\mathfrak{p})})^{-1}, \\ E(z) &= \prod_{n=1}^{\infty} (1 - q^{-zn})^{-a_n}, \end{aligned}$$

where $a_n = |\{\mathfrak{p} \in \mathcal{M}_A : \deg_A(\mathfrak{p}) = n\}|$ for every $n \in \mathbb{N} - \{0\}$.

Claim 1: For each $n \in \mathbb{N} - \{0\}$, a_n is finite. Moreover $a_n = O(q^n)$.

Proof of Claim 1. Let $n \in \mathbb{N} - \{0\}$. Set $\Lambda_n = \{\mathfrak{p} \in \mathcal{M}_A : \deg_A(\mathfrak{p}) = n\}$, and $\Lambda = \bigcup_{p \in \mathbb{F}[x], 1 \leq \deg_{\mathbb{F}[x]}(p) \leq n} \{\mathfrak{p} \in \mathcal{M}_A : \mathfrak{p}|p\}$. Let us show that $\Lambda_n \subseteq \Lambda$. Let $\mathfrak{p} \in \Lambda_n$. Since $\deg_A(\mathfrak{p}) = \deg_{\mathbb{F}[x]}(\mathfrak{p} \cap \mathbb{F}[x])f(\mathfrak{p}|\mathfrak{p} \cap \mathbb{F}[x])$, $1 \leq \deg_{\mathbb{F}[x]}(\mathfrak{p} \cap \mathbb{F}[x]) \leq n$. But $\mathfrak{p} \in \{\mathfrak{q} \in \mathcal{M}_A : \mathfrak{q}|\mathfrak{p} \cap \mathbb{F}[x]\}$, so, $\mathfrak{p} \in \Lambda$. That shows $\Lambda_n \subseteq \Lambda$. As Λ is now clearly a finite set, then Λ_n is finite.

Now let us show that $|\Lambda_n| = O(q^n)$. Let $p \in \mathcal{M}_{\mathbb{F}[x]}$. Since x is transcendental over \mathbb{F} , and \mathbb{F} is the full constant field of K , $K/\mathbb{F}(x)$ is a finite algebraic extension of function fields. Hence, Theorem 2.4.2 implies that $|\{\mathfrak{p} \in \mathcal{M}_A : \mathfrak{p}|p\}| \leq [K : \mathbb{F}(x)]$. Since $\Lambda_n \subseteq \Lambda$, and Λ is a disjoint union of the family

$$\{\{\mathfrak{p} \in \mathcal{M}_A : \mathfrak{p}|p\} : p \in \mathbb{F}[x], 1 \leq \deg_{\mathbb{F}[x]}(p) \leq n\},$$

we have $|\Lambda_n| \leq [K : \mathbb{F}(x)] |\{p \in \mathcal{M}_{\mathbb{F}[x]} : 1 \leq \deg_{\mathbb{F}[x]}(p) \leq n\}|$. As

$$|\{p \in \mathcal{M}_{\mathbb{F}[x]} : 1 \leq \deg_{\mathbb{F}[x]}(p) \leq n\}| \leq q^n,$$

because $|\mathbb{F}| = q$, then $|\Lambda_n| = O(q^n)$, as claimed. \square

Claim 2: For any $n \in \mathbb{N} - \{0\}$, the series $\theta_n(z) = a_n \sum_{k \geq 1} \frac{q^{-znk}}{k}$ converges absolutely.

Proof of Claim 2. Let $n \in \mathbb{N} - \{0\}$, and let $k \in \mathbb{N} - \{0\}$. Then,

$$\left| \frac{q^{-znk}}{k} \right| \leq q^{-n \operatorname{Re}(z)k}.$$

Since $\operatorname{Re}(z) > 1$, the series $\sum_{k \geq 1} q^{-\operatorname{Re}(z)nk}$ converges. Thus, by the comparison test, the series $a_n \sum_{k \geq 1} \frac{q^{-znk}}{k}$ converges absolutely. \square

Claim 3: The series $\sum_{n \geq 1} \theta_n(z)$ converges absolutely.

Proof of Claim 3. Let $n \in \mathbb{N} - \{0\}$. We have

$$\begin{aligned} |\theta_n(z)| &\leq a_n \sum_{k=1}^{\infty} \frac{q^{-nRe(z)k}}{k}, \\ |\theta_n(z)| &\leq a_n \sum_{k=1}^{\infty} q^{-nRe(z)k}, \\ |\theta_n(z)| &\leq \frac{a_n q^{-nRe(z)}}{1 - q^{-nRe(z)}}, \end{aligned}$$

so

$$|\theta_n(z)| \leq \frac{a_n}{q^{nRe(z)} - 1}. \quad (3.2.5)$$

Now, it is clear that

$$q^{nRe(z)} - 1 \sim_{n \rightarrow \infty} q^{nRe(z)},$$

then,

$$\frac{a_n}{q^{nRe(z)} - 1} \sim_{n \rightarrow \infty} a_n q^{-nRe(z)}.$$

Since $a_n = O(q^n)$, $a_n q^{-nRe(z)} = O(q^{n-nRe(z)})$. Furthermore, $Re(z) > 1$, then the geometric series $\sum_{n \geq 1} q^{n-nRe(z)}$ converges. It follows that the series $\sum_{n \geq 1} a_n q^{-nRe(z)}$ converges. Thus, by the equivalence property of the positive series, $\sum_{n \geq 1} \frac{a_n}{q^{nRe(z)} - 1}$ converges. Therefore, from (3.2.5), $\sum_{n \geq 1} \theta_n(z)$ converges absolutely. \square

By Claim 3, we get

$$\begin{aligned} \sum_{n=1}^{\infty} \theta_n(z) &= \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} a_n \frac{q^{-nzk}}{k} \\ \sum_{n=1}^{\infty} \theta_n(z) &= - \sum_{n=1}^{\infty} a_n \log(1 - q^{-nz}), \end{aligned}$$

where \log is the principal complex logarithm. Hence,

$$\sum_{n=1}^{\infty} \theta_n(z) = \log\left(\prod_{n=1}^{\infty} ((1 - q^{-nz}))^{-a_n}\right).$$

Then, $\prod_{n \geq 1} ((1 - q^{-nz}))^{-a_n}$ converges.

Now, let us show that, $\zeta_A(z) = E(z)$. Since

$$\begin{aligned} E(z) &= \prod_{\mathfrak{p} \in \mathcal{M}_A} \sum_{k=0}^{\infty} q^{-zk \deg_A(\mathfrak{p})}, \\ E(z) &= \sum_{\substack{r \in \mathbb{N} - \{0\}, k_1, \dots, k_r \geq 0, \\ \mathfrak{p}_j \in \mathcal{M}_A, \text{ for } j \in \{1, \dots, r\}}} \prod_{j=1}^r q^{-zk_j \deg_A(\mathfrak{p}_j)}, \\ E(z) &= \sum_{\substack{r \in \mathbb{N} - \{0\}, k_1, \dots, k_r \geq 0, \\ \mathfrak{p}_j \in \mathcal{M}_A, \text{ for } j \in \{1, \dots, r\}}} q^{-\sum_{j=1}^r z k_j \deg_A(\mathfrak{p}_j)}. \end{aligned}$$

Thus, $E(z) = \sum_{I \in Id(A)} \mathcal{N}_A(I)^{-z}$. Hence the result. □

3.3 The Functional Equation for ζ_A .

In this section, we discuss the analogue of the functional equation for the Riemann zeta function of number field.

Set $\mathcal{H} = \{s \in \mathbb{C} : \text{Re}(s) > 1\}$. First of all we give some properties of the function ζ_K , for the function field K/\mathbb{F} with genus g_K .

Proposition 3.3.1. The function $\zeta_K : \mathbb{C} \rightarrow \mathbb{C}$ given by

$$\zeta_K(z) = \prod_{\mathfrak{p} \in \mathcal{M}_K} (1 - q^{-z \deg_K(\mathfrak{p})})^{-1},$$

for $z \in \mathcal{H}$, is holomorphic on \mathcal{H} , and has an analytic continuation to a meromorphic function into \mathbb{C} . In particular, $\zeta_K(z) = (1 - q^{-z \deg_K(\infty)})^{-1} \zeta_A(z)$.

Proof. Let $z \in \mathcal{H}$. Then,

$$\begin{aligned} \zeta_K(z) &= \prod_{\mathfrak{p} \in \mathcal{M}_K} (1 - q^{-z \deg_K(\mathfrak{p})})^{-1}, \\ \zeta_K(z) &= (1 - q^{-z \deg_K(\infty)})^{-1} \prod_{\mathfrak{p} \in \mathcal{M}_A} (1 - q^{-z \deg_K(\psi(\mathfrak{p}))})^{-1}, \\ \zeta_K(z) &= (1 - q^{-z \deg_K(\infty)})^{-1} \zeta_A(z), \end{aligned}$$

where ψ is defined in Theorem 3.1.3. Since ζ_A and $z \mapsto (1 - q^{-z \deg(\infty)})^{-1}$ are holomorphic on \mathcal{H} , so is ζ_K . By analytic continuation theorem, ζ_K has an analytic continuation to a meromorphic function into \mathbb{C} . □

Proposition 3.3.2. Let $z \in \mathbb{C} - \{0, 1\}$.

(i) If $g_K = 0$, then

$$\zeta_K(z) = \frac{1}{(1 - q^{-z})(1 - q^{1-z})}.$$

(ii) If $g_K \geq 1$, then

$$\zeta_K(z) = \frac{L_K(q^{-z})}{(1 - q^{-z})(1 - q^{1-z})},$$

where $L_K(u) \in \mathbb{Z}[u]$ with degree less than or equal to $2g_K$, $L_K(q^{-1}) \neq 0$, and $L_K(1) \neq 0$.

Proof. Since \mathcal{H} is a connected open subset of the connected open subset $\mathbb{C} - \{0, 1\}$ of \mathbb{C} , by the analytic continuation theorem, it is sufficient to prove the statement for \mathcal{H} .

Let $z \in \mathcal{H}$. Then $\operatorname{Re}(z) > 1$, therefore $|q^{-z}| = q^{-\operatorname{Re}(z)} < q^{-1}$. From [1, Corollary 5.1.2], we get the result. \square

Corollary 3.3.3. The function ζ_A has a pole of order 1 at 1, and no other poles.

Proof. Let $z \in \mathcal{H}$. Then, by Proposition 3.3.1, $\zeta_A(z) = (1 - q^{-z \deg_K(\infty)})\zeta_K(z)$. From Proposition 3.3.2, ζ_K has a pole of order 1 at 1, a pole of order 1 at 0, and no other poles. Then, ζ_A has a pole of order 1 at 1, and 1 is the only pole of ζ_A . \square

Proposition 3.3.4. The function $\xi_A : \mathbb{C} \rightarrow \mathbb{C}$, such that for any $z \in \mathbb{C} - \{1\}$,

$$\xi_A(z) = q^{g_K z} \zeta_A(z) (1 - (\mathcal{N}((\infty))^{-z}))^{-1} (1 - q^{-z})(1 - q^{1-z}),$$

satisfies $\xi_A(1 - z) = \xi_A(z)$.

This is exactly the analogue of the functional equation of the Riemann zeta function for a number fields.

Proof. Let $z \in \mathbb{C} - \{1\}$. Since

$$\zeta_K(z) = \zeta_A(z) (1 - (\mathcal{N}((\infty))^{-z}))^{-1},$$

we have,

$$\xi_A(1 - z) = q^{g_K(1-z)} \zeta_K(1 - z) (1 - q^{1-z})(1 - q^{1-(1-z)}).$$

From [1, Proposition 5.1.13], we get

$$\zeta_K(z) = q^{g_K - 1} q^{-(2g_K - 2)z} \zeta_K(1 - z).$$

Hence,

$$\begin{aligned} \xi_A(1 - z) &= q^{g_K(1-z)} \zeta_K(1 - z) (1 - q^{-1+z})(1 - q^z), \\ \xi_A(1 - z) &= q^{g_K(1-z)} q^{-g+1+2g_K-2z} q^{-1+z} q^z \zeta_K(z) (1 - q^{-z})(1 - q^{1-z}), \\ \xi_A(1 - z) &= q^{g_K z} \zeta_K(z) (1 - q^{-z})(1 - q^{1-z}) \end{aligned}$$

Therefore, $\xi_A(1 - z) = \xi_A(z)$. \square

Definition 3.3.5. The L_K -polynomial of K/\mathbb{F} is defined by, for all $u \in \mathcal{H}$,

$$L_K(u) = (1-u)(1-uv)\zeta_K\left(-\frac{\log(u)}{\ln(q)}\right) \quad (3.3.1)$$

where \log is the principal complex logarithm.

Remark 3.3.6. Since \mathcal{H} is a connected open subset of \mathbb{C} , by the analytic continuation theorem, the polynomial L_K is well defined.

Proposition 3.3.7. If $L_K(u) = a_0 + a_1u + \dots + a_{2g_K}u^{2g_K}$, then, for all $j = 1, \dots, g_K$, $a_{2g_K-j} = q^{g_K-j}a_j$. Moreover, $a_0 = 1$, and $a_{2g_K} = q^{g_K}$.

Proof. Let $u \in \mathcal{H}$. We have, from Proposition 3.3.4,

$$\xi_A\left(-\frac{\log(u)}{\ln(q)}\right) = \xi_A\left(1 + \frac{\log(u)}{\ln(q)}\right), \quad (3.3.2)$$

where the \log is the principal complex logarithm. By Proposition 3.3.2, (ii), we also have $\zeta_K\left(-\frac{\log(u)}{\ln(q)}\right) = \frac{L_K(u)}{(1-u)(1-qu)}$. As $\xi_A\left(-\frac{\log(u)}{\ln(q)}\right) = u^{-g_K}\zeta_K\left(-\frac{\log(u)}{\ln(q)}\right)(1-u)(1-qu)$, then $\xi_A\left(-\frac{\log(u)}{\ln(q)}\right) = u^{-g_K}L_K(u)$.

On the other hand, by setting $B = \xi_A\left(1 + \frac{\log(u)}{\ln(q)}\right)$, we have

$$B = q^{g_K}\left(1 + \frac{\log(u)}{\ln(q)}\right)\zeta_K\left(1 + \frac{\log(u)}{\ln(q)}\right)(1-q^{-\left(1 + \frac{\log(u)}{\ln(q)}\right)})(1-q^{1-\left(1 + \frac{\log(u)}{\ln(q)}\right)}).$$

Thus, $B = q^{g_K}u^{g_K}\zeta_K\left(1 + \frac{\log(u)}{\ln(q)}\right)(1-q^{-1}u^{-1})(1-u^{-1})$. Again, using Proposition 3.3.2, (ii), we obtain

$$\zeta_K\left(1 + \frac{\log(u)}{\ln(q)}\right) = \frac{L_K(q^{-1}u^{-1})}{(1-q^{-1}u^{-1})(1-u^{-1})}.$$

It follows that $B = q^{g_K}u^{g_K}L_K(q^{-1}u^{-1})$. From (3.3.2), we have $u^{-g_K}L_K(u) = q^{g_K}u^{g_K}L_K(q^{-1}u^{-1})$, that is, $L_K(u) = q^{g_K}u^{2g_K}L_K(q^{-1}u^{-1})$. Then, we get $a_0 + a_1u + \dots + a_{2g_K}u^{2g_K} = a_{2g_K}q^{-g_K} + a_{2g_K-1}q^{-g_K+1}u + \dots + a_0q^{g_K}u^{2g_K}$. Since \mathcal{H} is a connected open subset of \mathbb{C} and the two polynomials $a_0 + a_1u + \dots + a_{2g_K}u^{2g_K}$, $a_{2g_K}q^{-g_K} + a_{2g_K-1}q^{-g_K+1}u + \dots + a_0q^{g_K}u^{2g_K}$ are entire functions, by the analytic continuation theorem, for all $u \in \mathbb{C}$, $a_0 + a_1u + \dots + a_{2g_K}u^{2g_K} = a_{2g_K}q^{-g_K} + a_{2g_K-1}q^{-g_K+1}u + \dots + a_0q^{g_K}u^{2g_K}$. That implies that for any $j \in \{1, \dots, g_K\}$,

$$q^{j-g_K}a_j = a_{2g_K-j} \quad (3.3.3)$$

Let us show that $a_0 = 1$. Let $u \in \mathbb{C}$ such that $0 < |u| < q^{-1}$. Then, by [1, Proposition 5.1.6], $\zeta_K\left(\frac{\log(u)}{\ln(q)}\right) = \sum_{l=0}^{\infty} A_l u^l$, where for every $l \in \mathbb{N}$, A_l is the number of positive divisors of K of degree l . It follows that $L_K(u) = (1-u)(1-qu) \sum_{l=0}^{\infty} A_l u^l$. By doing some computations, we obtain $L_K(u) = A_0 + A_1 u - (q+1)A_0 u + \dots$. By identification of coefficients, we thus have $a_0 = A_0 = 1$.

Now, from (3.3.3), we have $a_{2g_K} = q^{g_K} a_0 = q^{g_K}$. □

Corollary 3.3.8. $\deg_u(L_K(u)) = 2g_K$.

Proof. From Proposition 3.3.2, we have $L_K(u) = a_0 + a_1 u + \dots + a_{2g_K} u^{2g_K}$, where a_1, \dots, a_{2g_K} are integers. Thus, from Proposition 3.3.7, $a_{2g_K} = q^{g_K} \neq 0$. It implies that $\deg_u(L_K(u)) = 2g_K$. □

Theorem 3.3.9. *Suppose that, in $\mathbb{C}[u]$, we have*

$$L_K(u) = \prod_{i=1}^{2g_K} (1 - \pi_i u), \quad (3.3.4)$$

where $\pi_1, \dots, \pi_{2g_K} \in \mathbb{C}$. Then, $\{\pi_1, \dots, \pi_{2g_K}\}$ can be ordered in such a way $\pi_j \pi_{g_K+j} = q$ for all $j = 1, \dots, g_K$.

Proof. Set $L_K^\top(u) = u^{2g_K} L_K(u^{-1})$. Then, $L_K^\top(u) = a_0 u^{2g_K} + a_1 u^{2g_K-1} + \dots + a_{2g_K}$. From Proposition 3.3.7, we obtain $L_K^\top(u) = u^{2g_K} + a_1 u^{2g_K-1} + \dots + q^{g_K}$. Hence, $L_K^\top(u)$ is a monic polynomial with coefficients in \mathbb{Z} , and has degree $2g_K$. Thus $L_K^\top(u) = \prod_{j=1}^{2g_K} (u - \pi_j)$, because of relation (3.3.4).

Since $2g_K$ is an even integer, using the symmetric functions of the roots of $L_K^\top(u)$, we have

$$q^{g_K} = \prod_{j=1}^{2g_K} \pi_j \quad (3.3.5)$$

Claim 1: $\prod_{j=1}^{2g_K} (u - \pi_j) = \prod_{j=1}^{2g_K} (u - q\pi_j^{-1})$.

Proof of Claim 1. Setting $u = qt$, we have $L_K^\top(qt) = q^{2g_K} t^{2g_K} L_K(q^{-1}t^{-1})$. We have seen from the proof of Proposition 3.3.7 that $q^{g_K} t^{2g_K} L_K(q^{-1}t^{-1}) = L_K(t)$. This implies that $\prod_{j=1}^{2g_K} (u - \pi_j) = q^{g_K} L_K(q^{-1}u)$, that is $\prod_{j=1}^{2g_K} (u - \pi_j) = q^{g_K} \prod_{j=1}^{2g_K} (1 - q^{-1}\pi_j u)$. Hence, $\prod_{j=1}^{2g_K} (u - \pi_j) = q^{g_K} \prod_{j=1}^{2g_K} (q^{-1}\pi_j) \prod_{j=1}^{2g_K} (u - q\pi_j^{-1})$. From (3.3.5), we deduce that $\prod_{j=1}^{2g_K} (u - \pi_j) = \prod_{j=1}^{2g_K} (u - q\pi_j^{-1})$ as claimed. □

Now, we return to the proof of Theorem 3.3.9.

Set $B_1 = \{j \in \{1, \dots, 2g_K\} : \pi_j = q\pi_j^{-1}\}$, $C_1 = \{j \in \{1, \dots, 2g_K\} : \pi_j \neq q\pi_j^{-1}\}$. From Claim 1, we obtain $\{1, \dots, 2g_K\} = B_1 \sqcup C_1$, that is a disjoint union. Set

CHAPTER 3. THE RIEMANN ZETA FUNCTION FOR GLOBAL FUNCTION FIELDS. 28

$k = |C_1|$. Then we can arrange the roots of $L^\top(u)$ as follow: $\pi_1, q\pi_1^{-1}, \dots, \pi_k, q\pi_k^{-1}, \sqrt{q}, \dots, \sqrt{q}, -\sqrt{q}, \dots, -\sqrt{q}$, where \sqrt{q} is a root of multiplicity m , and $-\sqrt{q}$ is a root of multiplicity s . Using again (3.3.5), we get $(\pi_1)(q\pi_1^{-1}) \cdots (\pi_k)(q\pi_k^{-1})(\sqrt{q})^m(-\sqrt{q})^s = q^{g_K}$. Therefore,

$$(-1)^s(\sqrt{q})^{2k+m+s} = q^{g_K}. \quad (3.3.6)$$

From (3.3.6), since $q^{g_K} > 0$ and $(\sqrt{q})^{2k+m+s} > 0$, we deduce that m and s are both even integers. Since $k = g_K - (\frac{m+s}{2})$, we can rearrange the roots of L_K^\top as follow : $\pi_1, \dots, \pi_k, \pi_{k+1} = \sqrt{q}, \dots, \pi_{k+\frac{s}{2}} = \sqrt{q}, \pi_{k+\frac{s}{2}+1} = -\sqrt{q}, \dots, \pi_{k+\frac{s}{2}+\frac{m}{2}} = \pi_{g_K} = -\sqrt{q}, \pi_{g_K+1} = \frac{q}{\pi_1}, \dots, \pi_{g_K+k} = \frac{q}{\pi_k}, \pi_{g_K+k+1} = \sqrt{q}, \dots, \pi_{g_K+k+\frac{s}{2}} = \sqrt{q}, \pi_{g_K+k+\frac{s}{2}+1} = -\sqrt{q}, \dots, \pi_{g_K+k+\frac{s}{2}+\frac{m}{2}} = \pi_{2g_K} = -\sqrt{q}$. One can check easily that for any $j \in \{1, \dots, g_K\}$, $\pi_j \pi_{g_K+j} = q$. □

Chapter 4

The Riemann Hypothesis for ζ_A .

The main goal of this chapter is to prove the Riemann hypothesis for ζ_A . In this chapter, K/\mathbb{F} is a global function field with constant field \mathbb{F} , g_K its genus, and $\bar{K} = K\bar{\mathbb{F}}$ the compositum of K and $\bar{\mathbb{F}}$. If L/\mathbb{F} is a global function field over \mathbb{F} , then \mathcal{M}_L still denotes the set of all places of L .

4.1 The Riemann Hypothesis

Theorem 4.1.1. *If $z \in \mathbb{C}$ is a non-trivial zero of ζ_A then $\operatorname{Re}(z) = 1/2$.*

Remark 4.1.2. Although this Theorem 4.1.1 is not any more a conjecture, we still call it the Riemann hypothesis for global function fields, and this is an important theorem. For instance, one can deduce from it information about the distribution of the proper prime ideals of A . In Chapter 3, we introduced the function ζ_K because the proof of Theorem 4.1.1, we have chosen in this work, depends essentially on it.

There are many problems to solve if we want to prove that theorem using only ζ_A , for instance, we need to know how does the place (∞) of K behave under constant field extension?. More precisely, does (∞) split, split totally, or stay inert under constant field extensions?.

Another question is that, since we want to consider the integral closure of A under constant field extensions, is there any relation between the integral closure of A in K_r , where K_r is a finite constant field extension of K of degree r , and the set of places of K_r ?

First of all we need to understand what are the non-trivial zeroes of ζ_A ?. Let $z \in \mathbb{C} - \{1\}$. From Proposition 3.3.1, we have

$$\zeta_A(z) = (1 - q^{-z \deg_K((\infty))}) \zeta_K(z).$$

And by Proposition 3.3.2, we have

$$\zeta_K(z) = \frac{L_K(q^{-z})}{(1 - q^{-z})(1 - q^{1-z})},$$

where $L_K(u) = 1$ if $g_K = 0$.

Setting $L_A(u) = L_K(u)(1 - u^{\deg_K((\infty))})$,

$\zeta_A(z) = 0$ if and only if $L_A(q^{-z}) = 0$.

But

$$L_A(q^{-z}) = L_K(q^{-z})(1 - q^{-z \deg_K((\infty))}),$$

Hence we have the following definition.

Definition 4.1.3. The non-trivial zeroes of ζ_A are exactly the roots of the equation

$$L_K(q^{-z}) = 0. \quad (4.1.1)$$

We may assume that $g_K \geq 1$.

Indeed, if $g_K = 0$, then the set of non-trivial zeroes of ζ_A is empty and therefore the non-trivial zeroes of ζ_A obviously satisfy the condition of the Theorem 4.1.1.

We will show in the next three sections of this chapter that the complex numbers which satisfy (4.1.1) all have real part $\frac{1}{2}$.

We begin our study with the constant field extensions.

Let $\bar{\mathbb{F}}$ be an algebraic closure of \mathbb{F} . The first lemma is just a recall from field theory.

Lemma 4.1.4. For all $r \in \mathbb{N} - \{0\}$, there exists a unique extension \mathbb{F}_r/\mathbb{F} with $[\mathbb{F}_r : \mathbb{F}] = r$ and $\mathbb{F}_r \subseteq \bar{\mathbb{F}}$.

Proof. See [6, Corollary, p. 246]. □

Lemma 4.1.5. Let $r \in \mathbb{N} - \{0, 1\}$, and let us set $K_r = K\mathbb{F}_r$ the compositum of K and \mathbb{F}_r . We have

- (i) K_r/K is a Galois extension with Galois group $\text{Gal}(K_r/K) = \langle \sigma \rangle$, where σ is the K -automorphism of K_r such that $\sigma(\alpha) = \alpha^q$ for any $\alpha \in \mathbb{F}_r$.
- (ii) \mathbb{F}_r is the full constant field of K_r .

Proof. (i) We know that \mathbb{F}_r/\mathbb{F} is a Galois extension of degree r , and $\text{Gal}(\mathbb{F}_r/\mathbb{F}) = \langle \sigma_0 \rangle$, such that for any $\alpha \in \mathbb{F}_r$, $\sigma_0(\alpha) = \alpha^q$. As $K_r = K\mathbb{F}_r$, $\text{Gal}(K_r/K) = \langle \sigma \rangle$, where σ is defined by, for any $y = \sum_{j=1}^t \alpha_j \gamma_j \in K_r$, with $t \in \mathbb{N} - \{0\}$, and for all $j \in \{1, \dots, t\}$, $\alpha_j \in K$, and $\gamma_j \in \mathbb{F}_r$, we have $\sigma(y) = \sum_{j=1}^t \alpha_j \sigma_0(\gamma_j)$.

- (ii) This follows directly from Theorem 2.3.12, (ii). □

Definition 4.1.6. Let $r \in \mathbb{N} - \{0\}$, and let $K_r = K\mathbb{F}_r$ be the compositum of K and \mathbb{F}_r .

The K -automorphism of K_r , which is defined in the Lemma 4.1.5, is called the Frobenius automorphism of K_r/K .

The Frobenius automorphism plays an important role in the proof of the Riemann hypothesis for ζ_A .

Lemma 4.1.7. Let $r \in \mathbb{N} - \{0\}$, and let $K_r = K\mathbb{F}_r$ be the compositum of K and \mathbb{F}_r , then

- (i) $g_{K_r} = g_K$.
- (ii) If $\mathfrak{p} \in \mathcal{M}_K$ such that $\deg_K(\mathfrak{p}) = m$, then $\text{Con}_{K_r/K}(\mathfrak{p}) = \mathfrak{p}_1 + \dots + \mathfrak{p}_d$, where $d = \gcd(m, r)$, $\mathfrak{p}_1, \dots, \mathfrak{p}_d$ are distinct places of K_r , for any $i = 1, \dots, d$, $\deg(\mathfrak{p}_i) = \frac{m}{d}$, and $\text{Con}_{K_r/K}$ is the conorm map, defined in Definition 2.3.9, associated to the field extension K_r/K .

Proof. (i) Since K/\mathbb{F}_r is a constant field extension of the function field K/\mathbb{F} , then, by Theorem 2.3.12, (iii), we deduce that $g_{K_r} = g_K$.

- (ii) Let $\mathfrak{p} \in \mathcal{M}_K$ such that $\deg_K(\mathfrak{p}) = m$.
 Let $\mathfrak{p}' \in \mathcal{M}_{K_r}$ such that $\mathfrak{p}'|\mathfrak{p}$. From Theorem 2.3.12, (v), $\mathcal{O}_{\mathfrak{p}'/\mathfrak{p}'} = (\mathcal{O}_{\mathfrak{p}/\mathfrak{p}})\mathbb{F}_r$, the compositum of $\mathcal{O}_{\mathfrak{p}/\mathfrak{p}}$ and \mathbb{F}_r .
 Let us set $l = \text{lcm}(m, r)$, where $[\mathcal{O}_{\mathfrak{p}/\mathfrak{p}} : \mathbb{F}] = m$.
 Then $\mathcal{O}_{\mathfrak{p}/\mathfrak{p}} = \mathbb{F}_m$, and so $\mathcal{O}_{\mathfrak{p}'/\mathfrak{p}'} = \mathbb{F}_l$. It follows that $\deg_{K'}(\mathfrak{p}') = [\mathbb{F}_l : \mathbb{F}_r] = \frac{l}{r}$, that is $\deg_{K_r}(\mathfrak{p}') = \frac{\text{lcm}(m, r)}{r} = \frac{m}{d}$, because $\text{lcm}(m, r) \gcd(m, r) = mr$.

That shows that for any $\mathfrak{p}' \in \mathcal{M}_{K_r}$ such that $\mathfrak{p}'|\mathfrak{p}$, $\deg_{K_r}(\mathfrak{p}') = \frac{m}{d}$.
 On the other hand, we have from Theorem 2.3.12, (i), K_r/K is unramified. This implies that \mathfrak{p} is unramified in K_r/K .
 So, $\text{Con}_{K_r/K}(\mathfrak{p}) = \sum_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{p}' = \mathfrak{p}_1 + \dots + \mathfrak{p}_w$, where $w \in \mathbb{N} - \{0\}$. It follows that $\deg_{K_r}(\text{Con}_{K_r/K}(\mathfrak{p})) = \deg_{K_r}(\mathfrak{p}_1) + \dots + \deg_{K_r}(\mathfrak{p}_w)$.
 But we have seen that $\deg_{K_r}(\mathfrak{p}_j) = \frac{m}{d}$, for any $j \in \{1, \dots, w\}$, thus

$$\deg_{K_r}(\text{Con}_{K_r/K}(\mathfrak{p})) = \frac{wm}{d}. \quad (4.1.2)$$

From Theorem 2.3.12, iv., we have

$$\deg_{K_r}(\text{Con}_{K_r/K}(\mathfrak{p})) = \deg_K(\mathfrak{p}) = m. \quad (4.1.3)$$

We deduce, from (4.1.2), and (4.1.3), that $w = d$.
 Hence $\text{Con}_{K_r/K}(\mathfrak{p}) = \mathfrak{p}_1 + \dots + \mathfrak{p}_d$, with $d = \gcd(m, r)$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_d$ are pairwise distinct places of degree $\frac{m}{d}$. \square

Lemma 4.1.8. Let m, r be positive integers and let $d = \gcd(m, r)$. Then, in $\mathbb{C}[X]$

$$(X^{r/d} - 1)^d = \prod_{\zeta \in \mathbb{C}, \zeta^r=1} (X - \zeta^m).$$

Proof. Let us set $f(X) = \prod_{\zeta \in \mathbb{C}, \zeta^r=1} (X - \zeta^m)$, and let ζ_0 be an r -th primitive root of unity.

We set $m = kd$. Then $\gcd(k, r) = 1$. So, $(\zeta_0^k)^d$ is an $\frac{r}{d}$ -th root of unity. Indeed, suppose that $(\zeta_0^k)^d$ is not an $\frac{r}{d}$ -primitive root of unity, then, $(\zeta_0^k)^{d\frac{r}{dt}} = 1$, for some $t \in \mathbb{N}$ such that $t \geq 2$, and $t|r$. So, $(\zeta_0^k)^{\frac{r}{t}} = 1$.

As $t \geq 2$, then $\frac{r}{t} < r$. Therefore ζ_0^k is not anymore an r -th primitive root (1). On the other hand, as $\gcd(k, r) = 1$, then ζ_0^k is an r -primitive root of unity (2).

(1), and (2) give us a contradiction.

Let us set $\zeta_1 = \zeta_0^{kd}$. Then,

$$f(X) = (X - \zeta_1^0)(X - \zeta_1) \dots (X - \zeta_1^{\frac{r}{d}-1}) \quad (4.1.4)$$

$$\cdot (X - \zeta_1^{\frac{r}{d}})(X - \zeta_1^{\frac{r}{d}+1}) \dots (X - \zeta_1^{\frac{2r}{d}-1}) \quad (4.1.5)$$

$$\dots (X - \zeta_1^{\frac{(d-1)r}{d}})(X - \zeta_1^{\frac{(d-1)r}{d}+1}) \dots (X - \zeta_1^{\frac{dr}{d}-1}). \quad (4.1.6)$$

That is to say

$$f(X) = [(X - \zeta_1^0)(X - \zeta_1) \dots (X - (\zeta_1)^{\frac{r}{d}-1})] \quad (4.1.7)$$

$$\cdot [(X - \zeta_1^0)(X - \zeta_1) \dots (X - (\zeta_1)^{\frac{r}{d}-1})] \quad (4.1.8)$$

$$\dots [(X - \zeta_1^0)(X - \zeta_1) \dots (X - (\zeta_1)^{\frac{r}{d}-1})], \quad (4.1.9)$$

where we have d factors in the right hand-side. It follows that $f(X) = [(X - \zeta_1^0)(X - \zeta_1) \dots (X - \zeta_1^{\frac{r}{d}-1})]^d$.

But ζ_1 is an $\frac{r}{d}$ -primitive root of unity, then $[(X - \zeta_1^0)(X - \zeta_1) \dots (X - \zeta_1^{\frac{r}{d}-1})] = X^{\frac{r}{d}} - 1$.

Hence $f(X) = (X^{\frac{r}{d}} - 1)^d$ □

Definition 4.1.9. For $z \in \mathcal{H}$, where $\mathcal{H} = \{s \in \mathbb{C} : \operatorname{Re}(s) > 1\}$,

$$\zeta_{K_r}(z) = \prod_{\mathfrak{p} \in \mathcal{M}_{K_r}} (1 - q^{-zr \deg_{K_r}(\mathfrak{p})}).$$

Proposition 4.1.10. The infinite product $\prod_{\mathfrak{p} \in \mathcal{M}_{K_r}} (1 - q^{-zr \deg_{K_r}(\mathfrak{p})})$ converges absolutely in \mathcal{H} .

Proof. Let $z \in \mathcal{H}$. Since K_r/\mathbb{F}_r is a global function field and $|\mathbb{F}_r| = q^r$, then, by Proposition 3.3.1, $\prod_{\mathfrak{p} \in \mathcal{M}_{K_r}} (1 - q^{-zr \deg_{K_r}(\mathfrak{p})})$ converges absolutely when $z \in \mathcal{H}$. □

Proposition 4.1.11. For $z \in \mathcal{H}$, we have

$$\zeta_{K_r}(rz) = \prod_{\zeta^r=1} \zeta_K \left(-\frac{\log_\zeta(\zeta)}{\ln(q)} + z \right),$$

where for any $\zeta \in \mathbb{C}$ with $\zeta^r = 1$, \log_ζ is a branch of the logarithm complex such that $\exp(\log_\zeta(\zeta)) = \zeta$.

Proof. Let $z \in \mathcal{H}$, then

$$\begin{aligned} \zeta_{K_r}(rz) &= \prod_{\mathfrak{p}' \in \mathcal{M}_{K_r}} (1 - q^{-rz \deg_{K_r}(\mathfrak{p}')})^{-1} \\ &= \prod_{\mathfrak{p} \in \mathcal{M}_K} \prod_{\mathfrak{p}' | \mathfrak{p}} (1 - q^{-rz \deg_{K_r}(\mathfrak{p}')})^{-1}. \end{aligned}$$

Fix $\mathfrak{p} \in \mathcal{M}_K$ and let us set $m = \deg_K(\mathfrak{p})$ and $d = \gcd(r, m)$. Then, from Lemma 4.1.7, (ii), for all $\mathfrak{p}' \in \mathcal{M}_{K_r}$ such that $\mathfrak{p}' | \mathfrak{p}$, we have $\deg_{K_r}(\mathfrak{p}') = \frac{m}{d}$; and there are exactly d places of K_r above \mathfrak{p} . So,

$$\prod_{\mathfrak{p}' | \mathfrak{p}} (1 - q^{-rz \deg_{K_r}(\mathfrak{p}')}) = \left(1 - q^{-\frac{zrm}{d}}\right)^d$$

It follows that, by Lemma 4.1.8,

$$\begin{aligned} \prod_{\mathfrak{p}' | \mathfrak{p}} (1 - q^{-rz \deg(\mathfrak{p}')}) &= (-1)^d \left(q^{-\frac{zrm}{d}} - 1 \right)^d \\ &= (-1)^d \prod_{\zeta \in \mathbb{C}, \zeta^r=1} \left((q^{-z})^m - \zeta^m \right) \\ &= (-1)^{d+r} \prod_{\zeta \in \mathbb{C}, \zeta^r=1} \left[\zeta^m \left(1 - (\zeta^{-1} q^{-z})^{\deg(\mathfrak{p})} \right) \right]. \end{aligned}$$

As $\zeta \mapsto \zeta^{-1}$ is an automorphism of the group $(\{\gamma \in \mathbb{C} : \gamma^r = 1\}, \cdot)$, then

$$\prod_{\mathfrak{p}' | \mathfrak{p}} (1 - q^{-rz \deg(\mathfrak{p}')}) = (-1)^{d+r} \left(\prod_{\zeta \in \mathbb{C}, \zeta^r=1} \zeta^m \right) \prod_{\zeta \in \mathbb{C}, \zeta^r=1} \left(1 - (\zeta q^{-z})^{\deg(\mathfrak{p})} \right).$$

From the fact that $\prod_{\zeta \in \mathbb{C}, \zeta^r=1} (X - \zeta) = X^r - 1$, and using the symmetric functions of the r -th roots of unity, we have $\prod_{\zeta \in \mathbb{C}, \zeta^r=1} \zeta = (-1)^{r+1}$.

It follows that

$$\prod_{\mathfrak{p}' | \mathfrak{p}} (1 - q^{-rz \deg(\mathfrak{p}')}) = (-1)^{d+r+mr+m} \prod_{\zeta \in \mathbb{C}, \zeta^r=1} \left(1 - (\zeta q^{-z})^{\deg(\mathfrak{p})} \right).$$

Claim 1: $d + r + mr + m$ is an even integer.

Proof of Claim 1.

Proof. There are 4 cases to consider.

Case 1: Suppose r and m are both even.

In that case, $d = \gcd(r, m)$ must be even and rm is also even, so $d + r + mr + m$ is even.

Case 2: Suppose r is even and m is odd.

So, $d = \gcd(r, m)$ is odd, mr is even, and $r + m$ is odd. Thus $d + r + mr + m$ is even.

Case 3: Suppose r is odd and m is even.

With similar reason as in Case 2, we obtain that $d + r + mr + m$ is even.

Case 4: Suppose r and m are both odd.

In this case, $d = \gcd(r, m)$ must be odd and rm is also odd. Therefore $d + r + mr + m$ is even. \square

From Claim 1, we obtain

$$\prod_{\mathfrak{p}'|\mathfrak{p}} (1 - q^{-r z \deg(\mathfrak{p}')}) = \prod_{\zeta \in \mathbb{C}, \zeta^r=1} \left(1 - (\zeta q^{-z})^{\deg(\mathfrak{p})} \right).$$

Thus, using the absolute convergence of the infinite product in Proposition 4.1.10,

$$\begin{aligned} \zeta_{K_r}(rz) &= \prod_{\mathfrak{p} \in \mathcal{M}_{K_r}} \prod_{\zeta^r=1} (1 - (\zeta q^{-z})^{\deg(\mathfrak{p})})^{-1} \\ &= \prod_{\zeta^r=1} \prod_{\mathfrak{p} \in \mathcal{M}_K} (1 - (\zeta q^{-z})^{\deg(\mathfrak{p})})^{-1} \\ &= \prod_{\zeta^r=1} \zeta_K \left(z - \frac{\log_\zeta(\zeta)}{\ln(q)} \right). \end{aligned}$$

\square

4.2 The Proof of the Riemann Hypothesis for ζ_A

In the previous section, we have just stated the Riemann hypothesis for ζ_A , and gave some tools in order to prove that theorem.

Although the proof we have chosen is due to Bombieri, and which is long, then this section is just the first part of the proof.

Definition 4.2.1. Let $m \in \mathbb{N} - \{0, 1\}$. The polynomial $L_{K_m}(u) \in \mathbb{Z}[u]$ which is defined by, for all $u \in \mathbb{C}$ with $0 < |u| < q^{-1}$, $L_{K_m}(u) = (1 - u)(1 - q^m u) \zeta_{K_m} \left(-\frac{\log(u)}{\ln(q)} \right)$ is called the L_{K_m} -polynomial of K_m/\mathbb{F}_m , where \log is the principal branch of the logarithm complex.

The next lemma tells us that proving the Riemann hypothesis for a global function field K is the same as proving the Riemann hypothesis for a finite constant field extension of K .

Lemma 4.2.2. Let $m \in \mathbb{N} - \{0, 1\}$. Then the following assertions are equivalent.

- (i) Any reciprocal root $\alpha \in \mathbb{C}$ of L_K satisfies $|\alpha| = \sqrt{q}$.
- (ii) Every reciprocal root $\pi \in \mathbb{C}$ of L_{K^m} satisfies $|\pi| = \sqrt{q^m}$.

Proof. Let $\alpha_1, \dots, \alpha_{2g_K}$ be the reciprocal roots of $L_K(u)$.

Claim 1: Let $m \in \mathbb{N} - \{0, 1\}$, then the reciprocal roots of $L_{K^m}(u)$ in \mathbb{C} are exactly $\alpha_1^m, \dots, \alpha_{2g_K}^m$.

Proof of Claim 1.

Proof. Let $m \in \mathbb{N} - \{0, 1\}$, and let $z \in \mathcal{H}$. Then $0 < |q^{-zm}| < q^{-m} < q^{-1}$.

So, $L_{K^m}(q^{-zm}) = (1 - q^{-zm})(1 - q^m q^{-zm}) \zeta_{K^m} \left(-\frac{\log(q^{-zm})}{\ln(q)} \right)$.

As $\log(q^{-zm}) = -zm \ln(q)$, from Proposition 4.1.11, we obtain

$L_{K^m}(q^{-zm}) = (1 - q^{-zm})(1 - q^m q^{-zm}) \prod_{\zeta^m=1} \zeta_K \left(-\frac{\log(\zeta)}{\ln(q)} + z \right)$.

From Proposition 3.3.2, (ii), we have

$L_{K^m}(q^{-zm}) = (1 - q^{-zm})(1 - q^m q^{-zm}) \prod_{\zeta^m=1} \frac{L_K(\zeta q^{-z})}{(1 - \zeta q^{-z})(1 - \zeta q^{1-z})}$. That is to say $L_{K^m}(q^{-zm}) = (1 - q^{-zm})(1 - q^m q^{-zm}) \frac{\prod_{\zeta^m=1} L_K(\zeta q^{-z})}{\prod_{\zeta^m=1} (1 - \zeta q^{-z}) \prod_{\zeta^m=1} (1 - \zeta q^{1-z})}$.

As $\prod_{\zeta^m=1} L_K(\zeta q^{-z}) = \prod_{j=1}^{2g_K} \prod_{\zeta^m=1} (1 - \alpha_j \zeta q^{-z})$, because $\alpha_1, \dots, \alpha_{2g_K}$ are the reciprocal roots of $L_K(u)$. But the m -th roots of unity form a cyclic group, then

$\prod_{\zeta^m=1} L_K(\zeta q^{-z}) = \prod_{j=1}^{2g_K} \left((-1)^m (\prod_{\zeta^m=1} \zeta) \prod_{\zeta^m=1} (\alpha_j q^{-z} - \zeta) \right)$.

From the symmetric functions of the m -th roots of unity, we deduce that $(-1)^m (\prod_{\zeta^m=1} \zeta) = -1$. Since $\prod_{\zeta^m=1} (\alpha_j q^{-z} - \zeta) = \alpha_j^m q^{-mz} - 1$, for every $j = 1, \dots, 2g_K$,

$$\prod_{\zeta^m=1} L_K(\zeta q^{-z}) = (-1)^{2g_K} \prod_{j=1}^{2g_K} (1 - \alpha_j^m q^{-mz}),$$

in other words,

$$\prod_{\zeta^m=1} L_K(\zeta q^{-z}) = \prod_{j=1}^{2g_K} (1 - \alpha_j^m q^{-mz}). \quad (4.2.1)$$

With similar reason as above, we obtain $\prod_{\zeta^m=1} (1 - \zeta q^{-z}) = 1 - q^{-zm}$ (1), and $\prod_{\zeta^m=1} (1 - \zeta q^{1-z}) = 1 - q^m q^{-zm}$ (2).

From (4.2.1), (1), and (2), we obtain $L_{K_m}(q^{-zm}) = \prod_{j=1}^{2g_K} (1 - \alpha_j^m q^{-mz})$.

As L_{K_m} is an entire function, then, by the analytic continuation theorem, for any $u \in \mathbb{C}$, $L_{K_m}(u) = \prod_{j=1}^{2g_K} (1 - \alpha_j^m u)$. Thus we obtain Claim 1. \square

The Lemma 4.2.2 follows immediately from Claim 1. \square

Definition 4.2.3. Let $r \in \mathbb{N} - \{0\}$. We define by N_r the number of places of K_r of degree one.

Lemma 4.2.4. If there exist $c \in \mathbb{R}$ such that for any $r \in \mathbb{N} - \{0\}$,

$$|N_r - (q^r + 1)| \leq c\sqrt{q^r}, \quad (4.2.2)$$

then, any reciprocal root α of L_K satisfies $|\alpha| = \sqrt{q}$.

Remark 4.2.5. The Lemma 4.2.4 is analogous to the following. Suppose that $\pi(x)$ is the number of prime numbers less than x , where $x > 0$. Thus, if $\pi(x) = Li(x) + O(\sqrt{x} \log(x))$, then the Riemann hypothesis for the number fields holds, where $Li(x) = \int_0^x \frac{dt}{\log(t)}$.

Proof of Lemma 4.2.4.

Proof. Let $\alpha_1, \dots, \alpha_{2g_K}$ be the reciprocal roots of $L_K(u)$.

Let us show first that for any $i \in \{1, \dots, 2g_K\}$, $|\alpha_i| \leq \sqrt{q}$.

Let $r \in \mathbb{N} - \{0\}$, from [1, Proposition 5.1.6], we have $\zeta_{K_r}\left(\frac{\log(u)}{\ln(q)}\right) = \sum_{n=0}^{\infty} A_{n,r} u^n$, where for all $n \in \mathbb{N} - \{0\}$, $A_{n,r}$ is the number of positive divisors of K_r of degree 1.

It follows that for $u \in \mathbb{C}$, such that $0 < |u| < q^{-r}$, $L_{K_r}(u) = (1 - u)(1 - q^r u) \sum_{n=0}^{\infty} A_{n,r} u^n$. This implies that for $u \in \mathbb{C}$, such that $0 < |u| < q^{-r}$, $L_{K_r}(u) = A_{0,r} + (A_{1,r} - (q^r + 1)A_{0,r})u + \dots$.

From Claim 1 in the proof of Lemma 4.2.2, we have $L_K(u) = \prod_{j=1}^{2g_K} (1 - \alpha_j^r u)$. So, by comparing coefficients, we deduce $A_{1,r} - (q^r + 1)A_{0,r} = -\sum_{j=1}^{2g_K} \alpha_j^r$. Since $A_{0,r} = 1$ and $A_{1,r} = N_r$,

$$N_r - (q^r + 1) = -\sum_{i=1}^{2g_K} \alpha_i^r.$$

So, by (4.2.2)

$$\left| \sum_{i=1}^{2g_K} \alpha_i^r \right| \leq c\sqrt{q^r}.$$

Now, we consider the function H which is defined by, for every $z \in \mathbb{C} - \{\alpha_1^{-1}, \dots, \alpha_{2g_K}^{-1}\}$, $H(z) = \sum_{i=1}^{2g_K} \frac{\alpha_i z}{1 - \alpha_i z}$.

Then H is a meromorphic function on \mathbb{C} .

Let us set $\delta = \min \{|\alpha_1^{-1}|, \dots, |\alpha_{2g_K}^{-1}|\}$.

Claim 1: δ is the radius of convergence of the power series $\sum_{i=1}^{2g_K} \sum_{k \geq 1} (\alpha_i z)^k$, where z is a complex number.

Moreover, for any $z \in \mathbb{C}$ with $|z| < \delta$, $H(z) = \sum_{k=1}^{\infty} (\sum_{i=1}^{2g_K} \alpha_i^k) z^k$.

Proof of Claim 1.

Proof. Let $z \in \mathbb{C}$ with $|z| < \delta$, and let $i \in \{1, \dots, 2g_K\}$ then $|\alpha_i z| < 1$, because $\delta \leq |\alpha_i|^{-1}$. Therefore

$$\frac{1}{1 - \alpha_i z} = \sum_{k=0}^{\infty} (\alpha_i z)^k.$$

It follows that $\sum_{i=1}^{2g_K} \sum_{k \geq 1} (\alpha_i z)^k$ converges and $H(z) = \sum_{k=1}^{\infty} (\sum_{i=1}^{2g_K} \alpha_i^k) z^k$.

It is clear that if $z \in \mathbb{C}$ with $|z| > \delta$, then $\sum_{i=1}^{2g_K} \sum_{k \geq 1} (\alpha_i z)^k$ diverges. \square

Now, let $z \in \mathbb{C}$ with $|z| < q^{-\frac{1}{2}}$.

From (4.2.2), we have $|\sum_{i=1}^{2g_K} \alpha_i^k| \leq c \sqrt{q^k}$. Then $|(\sum_{i=1}^{2g_K} \alpha_i^k) z^k| \leq c |\sqrt{q} z|^k$.

As $|z| < q^{-\frac{1}{2}}$, then $|\sqrt{q} z| < 1$. Thus the series $\sum_{k \geq 0} (\sqrt{q} z)^k$ converges. Therefore the series $\sum_{i=1}^{2g_K} \sum_{k \geq 1} (\alpha_i z)^k$ converges.

Assume that $\delta < q^{-\frac{1}{2}}$. Then there exist $z_0 \in \mathbb{C}$ with $\delta < |z_0| < q^{-\frac{1}{2}}$. So the series $\sum_{i=1}^{2g_K} \sum_{k \geq 1} (\alpha_i z_0)^k$ converges. That contradicts the first assertion of Claim 1.

It follows that $\delta \geq q^{-\frac{1}{2}}$. Hence for any $i \in \{1, \dots, 2g_K\}$, $|\alpha_i| \leq \sqrt{q}$.

Now, let us show that for every $i \in \{1, \dots, 2g_K\}$, $|\alpha_i| \geq \sqrt{q}$.

Let $i \in \{1, \dots, 2g_K\}$. From Theorem 3.3.9, we have $\alpha_i \alpha_{g_K+i} = q$. Therefore $(\prod_{i=1}^{g_K} \alpha_i) (\prod_{j=g_K+1}^{2g_K} \alpha_j) = q^{g_K}$.

It implies that

$$\prod_{i=1}^{2g_K} |\alpha_i| = q^{g_K}. \quad (4.2.3)$$

Suppose that there exist $i_0 \in \{1, \dots, 2g_K\}$ such that $|\alpha_{i_0}| < \sqrt{q}$. Since we have seen that for every $i \in \{1, \dots, 2g_K\}$, $|\alpha_i| \leq \sqrt{q}$, then $\prod_{i=1}^{2g_K} |\alpha_i| < q^{g_K}$. This contradicts (4.2.3).

Thus for any $i \in \{1, \dots, 2g_K\}$, $|\alpha_i| \geq \sqrt{q}$.

We conclude that for any $i \in \{1, \dots, 2g_K\}$, $|\alpha_i| = \sqrt{q}$. \square

We want to find $c \in \mathbb{R}$ which satisfies the assumption of Lemma 4.2.4.

Definition 4.2.6. Let $Q \in \mathcal{M}_K$.

Let $j \in \mathbb{N}$. j is called a pole number of Q if there exists $x \in K$ with pole divisor $(x)_{\infty} = jQ$.

The next theorem gives us an upper bound.

Theorem 4.2.7. *Suppose that q is a square, and $q > (g_K + 1)^4$, then $N_1 < q + 1 + (2g_K + 1)\sqrt{q}$.*

A remark is in order before showing that important theorem.

Remark 4.2.8. If K/\mathbb{F} is a global function field with full constant field \mathbb{F} , then one can go through constant field extensions in order to get the assumptions q is a square and $q > (g_K + 1)^4$. Indeed, from Theorem 2.3.12, (ii), g_K does not depend on the cardinality of the full constant field of a constant field extension of K .

Therefore, we obtain an upper bound for the corresponding constant field of K . So, we just need to give an lower bound for this end, and then the Riemann hypothesis for K follows from Lemma 4.2.2.

Proof. If $N_1 = 0$, then the result is clear. We assume that there exists $Q \in \mathcal{M}_K$ which has degree one.

Let us set $q_0 = \sqrt{q}$, $m = q_0 - 1$, and $n = 2g_K + q_0$. One can show that

$$m + nq_0 = q - 1 + (2g_K + 1)\sqrt{q}. \quad (4.2.4)$$

Let us set $T = \{i \in \{0, \dots, m\} : i \text{ is a pole number of } Q\}$.

Since $m = \sqrt{q}$ and $q > (g_K + 1)^4$, then $m \geq 2g_K$. It follows from [1, Proposition 1.6.6], that there exists $y_0 \in K$, such that $(y_0)_\infty = mQ$, then $T \neq \emptyset$. So, for any $j \in T$, we can find $u_j \in K$, such that $(u_j)_\infty = jQ$.

Claim 1: The set $\{u_i : i \in T\}$ is an \mathbb{F} -basis of $L(mQ)$.

Proof of the Claim 1.

Proof. Since q is a square, then $m \in \mathbb{N}$.

Let us show that $\{u_i : i \in T\}$ is \mathbb{F} -linearly independent.

Let $(a_i)_{i \in T} \in \mathbb{F}^{|T|}$, such that $\sum_{i \in T} a_i u_i = 0$.

Suppose that there exists $i_0 \in T$ such that $a_{i_0} \neq 0$.

Denote by $T_1 = \{i \in T : a_i \neq 0\}$. Then $T_1 \neq \emptyset$ because $i_0 \in T_1$.

As for any $i \in T_1$, $v_Q(a_i) = 0$, then for any $i \in T_1$, $v_Q(a_i u_i) = v_Q(u_i) = -i$. It implies that $v_Q(a_i u_i) \neq v_Q(a_j u_j)$ for any $(i, j) \in T_1^2$ with $i \neq j$. It follows, from Theorem 2.1.11, that $v_Q(\sum_{i \in T} (a_i u_i)) = \min_{i \in T_1} (v_Q(a_i u_i))$. Therefore,

$$v_Q\left(\sum_{i \in T} (a_i u_i)\right) = j_0, \quad (4.2.5)$$

for some $j_0 \in T_1$.

On the other hand, we have

$$v_Q\left(\sum_{i \in T} (a_i u_i)\right) = v_Q(0) = \infty. \quad (4.2.6)$$

From the relations (4.2.5) and (4.2.6), we have a contradiction.

So, $\{u_i : i \in T\}$ is \mathbb{F} - linearly independent.

Let us show that $|\{u_i : i \in T\}| = l(mQ)$.

As $m = q_0 - 1 = \sqrt{q} - 1$, and $q > (g_K + 1)^2$, then $m > g_K^2 + 2g_K \geq 2g_K + 1$. Since $\deg_K(Q) = 1$, then $\deg(mQ) > 2g_K - 2$. Therefore, by Theorem 2.2.12, $l(mQ) = m + 1 - g_K$.

Case 1: Suppose that $g_K > 0$. Then, by [1, Theorem 1.6.8], there are exactly g_K elements of $\{1, \dots, m\}$ which are not pole numbers. But $(1)_\infty = 0Q$, thus $|\{u_i : i \in T\}| = m - g_K + 1 = l(mQ)$. Therefore $\{u_i : i \in T\}$ is an \mathbb{F} - basis of $L(mQ)$.

Case 2: If $g_K = 0$. Then, every elements of $\{1, \dots, m\}$ are pole numbers of Q . This implies that $l(mQ) = m + 1$. Hence, $\{u_i : i \in T\}$ is an \mathbb{F} - basis of $L(mQ)$. These show that $\{u_i : i \in T\}$ is an \mathbb{F} - basis of $L(mQ)$. \square

Now we return to the proof of the theorem.

We define the set

$$L = \left\{ \sum_{\nu=1}^s x_\nu y_\nu^{q_0} : s \in \mathbb{N} - \{0\}, x_1, \dots, x_s \in L(mQ), \text{ and } y_1, \dots, y_s \in L(nQ) \right\}.$$

It is clear that L is an \mathbb{F} - vector space.

Claim 2: $L \subseteq L((m + q_0n)Q)$.

Proof of Claim 2.

Proof. Let $\theta \in L$. Then $\theta = \sum_{\nu=1}^s x_\nu y_\nu^{q_0}$, with $s \in \mathbb{N} - \{0\}$, $x_1, \dots, x_s \in L(mQ)$, and $y_1, \dots, y_s \in L(nQ)$.

Let $\nu \in \{1, \dots, s\}$. By Proposition 2.2.5, we have $(x_\nu y_\nu^{q_0}) = (x_\nu) + (y_\nu^{q_0})$. As $(x_\nu) \geq -mQ$, $(y_\nu^{q_0}) \geq -q_0nQ$, then $(x_\nu y_\nu^{q_0}) \geq -(m + q_0n)Q$. So $x_\nu y_\nu^{q_0} \in L((m + q_0n)Q)$.

We know, from Proposition 2.2.7, that $L((m + q_0n)Q)$ is an \mathbb{F} - vector space, then $\theta \in L((m + q_0n)Q)$. \square

Now, we go back to the proof of the Theorem 4.2.7.

Suppose that there exists $x_0 \in L - \{0\}$ such that for every $P \in \mathcal{M}_K$ with $\deg_K(P) = 1$, and $P \neq Q$, $x_0 \in P$. That implies that

$\deg((x_0)_0) = \sum_{P \in \mathbf{Z}(x_0)} v_P(x_0) \deg_K(P) \geq N_1 - 1$, where N_1 is the number of places of K of degree 1.

Since $x_0 \in L$, and $L \subseteq L((m + q_0n)Q)$, $\deg((x_0)_0) \leq m + q_0n$. Thus $N_1 \leq q + 1 + (2g_K + 1)\sqrt{q}$.

Now we need to prove that there exists $x_0 \in L - \{0\}$ such that for every $P \in \mathcal{M}_K$ with $\deg_K(P) = 1$, and $P \neq Q$, $x_0 \in P$.

Claim 3: If $y \in L$, then $y = \sum_{i \in T} u_i z_i^{q_0}$ where $z_i \in L(nQ)$, and $\{u_i : i \in T\}$ is the basis of $L(mQ)$ defined in Claim 1, and this representation is unique.

Proof of Claim 3.

Proof. Let $y \in L$. We have $y = \sum_{i=1}^s y_i z_i^{q_0}$ with $y_i \in L(mQ)$, $z_i \in L(nQ)$ for $i \in \{1, \dots, s\}$, $s \in \mathbb{N} - \{0\}$.

Let $i \in \{1, \dots, s\}$. From Claim 1, $\{u_i : i \in T\}$ is an \mathbb{F} -basis of $L(mQ)$, then we get

$$y_i = \sum_{j=1}^r \alpha_{i,j} u_j, \text{ with } r \in \mathbb{N} - \{0\}, \alpha_{i,j} \in \mathbb{F}.$$

As $q = q_0^2$, and for all $(i, j) \in \{1, \dots, s\} \times \{1, \dots, r\}$, $\alpha_{i,j}^q = \alpha_{i,j}$, then $y = \sum_{i=1}^s \sum_{j=1}^r u_j (\alpha_{i,j}^{q_0} z_i)^{q_0}$. So, $y = \sum_{j=1}^r u_j (\sum_{i=1}^s (\alpha_{i,j}^{q_0} z_i)^{q_0})$. As $L(nQ)$ is an \mathbb{F} -vector space, then, for any $(i, j) \in \{1, \dots, s\} \times \{1, \dots, r\}$, $\alpha_{i,j}^{q_0} z_i \in L(nQ)$. So, we obtain first assertion of Claim 3.

For the uniqueness. Assume that there is an equation

$$\sum_{i \in T} u_i x_i^{q_0} = 0, \quad (4.2.7)$$

with $x_i \in L(nQ)$ for $i \in T$, and not all $x_i = 0$.

Let $j \in T$ such that $x_j \neq 0$, we have $v_Q(u_j x_j^{q_0}) \equiv -j \pmod{q_0}$.

Since $m = q_0 - 1$, if $i, j \in T$, with $i \neq j$, then $i \not\equiv j \pmod{q_0}$.

From Theorem 2.1.11, (ii), we obtain $v_Q(\sum_{i \in T} u_i x_i^{q_0}) = \min \{v_Q(u_i x_i^{q_0}) : i \in T\}$.

Therefore $v_Q(\sum_{i \in T} u_i x_i^{q_0}) \neq \infty$. This gives a contradiction to (4.2.7). That proves Claim 3. \square

We need two lemmas in order to achieve the proof of Theorem 4.2.7.

Lemma 4.2.9. The map $\lambda : L \rightarrow L((q_0 m + n)Q)$, given by $\lambda(\sum_{i \in T} u_i z_i^{q_0}) = \sum_{i \in T} u_i^{q_0} z_i$, where $\{u_i : i \in T\}$ is the basis of $L(mQ)$ defined in Claim 1, and for any $i \in T$, $z_i \in L(nQ)$, is well defined, and is a linear map which is not one to one.

Proof of the lemmas.

Proof. (i) Let $z \in L$. From Claim 3, z can be uniquely written as $z = \sum_{i \in T} u_i z_i^{q_0}$, with $z_i \in L(nQ)$ for any $i \in T$.

Let $i \in T$, then $(u_i^{q_0} z_i) = q_0(u_i) + (z_i)$. Since $(u_i) \geq -mQ$, and $(z_i) \geq -nQ$, $u_i^{q_0} z_i \in L((q_0 m + n)Q)$. As $L((q_0 m + n)Q)$ is an \mathbb{F} -vector space then $\lambda(z) \in L((q_0 m + n)Q)$. Thus λ is well defined.

(ii) Let f , and z be elements of L . Then $f = \sum_{i \in T} u_i z_i^{q_0}$, with $z_i \in L(nQ)$ for any $i \in T$, and $z = \sum_{i \in T} u_i \theta_i^{q_0}$, with $\theta_i \in L(nQ)$ for any $i \in T$. So,

$$\lambda(f + z) = \lambda\left(\sum_{i \in T} u_i (z_i^{q_0} + \theta_i^{q_0})\right),$$

$$\lambda(f + z) = \lambda\left(\sum_{i \in T} u_i (z_i + \theta_i)^{q_0}\right),$$

because q_0 is the power of the characteristic of the field K . Thus

$$\begin{aligned}\lambda(f+z) &= \sum_{i \in T} u_i^{q_0} (z_i + \theta_i) \\ \lambda(f+z) &= \lambda\left(\sum_{i \in T} u_i z_i^{q_0}\right) + \lambda\left(\sum_{i \in T} u_i \theta_i^{q_0}\right).\end{aligned}$$

In other words, $\lambda(f+z) = \lambda(f) + \lambda(z)$. That shows λ is a homomorphism of groups. Since \mathbb{F} is a finite field, then λ is an \mathbb{F} -linear map.

(iii) We want to show that $\ker(\lambda) \neq \{0\}$.

It is sufficient to show that $\dim_{\mathbb{F}} L > \dim_{\mathbb{F}} L((q_0 m + n)Q)$, because if $\ker(\lambda) = \{0\}$, then $\dim_{\mathbb{F}} L \leq \dim_{\mathbb{F}} L((q_0 m + n)Q)$.

From Claim 3, if $(z_j)_{1 \leq j \leq d}$ is an \mathbb{F} -basis of $L(nQ)$, with $d = \dim_{\mathbb{F}} L(nQ)$, then $(u_i z_j)_{\substack{1 \leq i \leq |T| \\ 1 \leq j \leq d}}$ is an \mathbb{F} -basis of L .

So, $\dim_{\mathbb{F}}(L) = l(mQ)l(nQ)$.

By Theorem 2.2.9, we have $l(mQ) \geq m \deg_K(Q) + 1 - g_K$, and $l(nQ) \geq n \deg_K(Q) + 1 - g_K$. As $\deg_K(Q) = 1$, and $n > g_K$, $l(mQ)l(nQ) > (m+1-g_K)(n+1-g_K)$.

On the other hand, since $q_0 m + n = 2g_K + q > 2g_K - 2$, we obtain, by Corollary 2.2.12, $\dim_{\mathbb{F}}(L((q_0 m + n)Q)) = (2g_K + q) + 1 - g_K = g_K + q + 1$. If $(m+1-g_K)(n+1-g_K) > g_K + q + 1$, then, we are done.

Since $(m+1-g_K)(n+1-g_K) > g_K + q + 1$ is equivalent to $(q_0 - g_K)(g_K + q_0 + 1) > g_K + q + 1$, a direct computation shows that $(q_0 - g_K)(g_K + q_0 + 1) > g_K + q + 1$ is equivalent to $q > (g_K + 1)^4$. That last assertion is true by our assumption so we get the result. \square

We still need another lemma in order to prove the Theorem 4.2.7.

Lemma 4.2.10. Let $x \in L - \{0\}$, with $\lambda(x) = 0$, and let P be a place of degree one with $P \neq Q$. Then $x \in P$.

Proof of this lemma.

Proof. Let $x \in L - \{0\}$, with $\lambda(x) = 0$, and let P be a place of degree one with $P \neq Q$. Then, from Claim 3, $x = \sum_{i \in T} u_i z_i^{q_0}$ where $z_i \in L(nQ)$ for any $i \in T$. As $L \subseteq L((q_0 m + n)Q)$, and $P \neq Q$, then, for all $y \in L$, we have $v_P(y) \geq 0$. In particular $v_P(x) \geq 0$. So, $x \in \mathcal{O}_P$, and then $x + P \in \mathcal{O}_P/P$. It follows that $(x+P)^{q_0} = \sum_{i \in T} (u_i + P)^{q_0} (z_i + P)^{q_0}$, because q_0 is a power of the characteristic of K .

Since $\deg_K(P) = 1$, $\mathbb{F} = \mathcal{O}_P/P$, and $|\mathbb{F}| = q$, $(x+P)^{q_0} = (\sum_{i \in T} (u_i + P)^{q_0} (z_i + P)^{q_0})$. Therefore $(x+P)^{q_0} = \lambda(x) + P = P$. Since a field is an integral domain, $x + P = P$. That means $x \in P$. \square

From Lemma 4.2.9, there exists $x_0 \in L - \{0\}$, such that $\lambda(x_0) = 0$. By Lemma 4.2.10, we deduce that for any $P \in \mathcal{M}_K$, with $\deg_K(P) = 1$, $x_0 \in P$. It follows that there exist $x_0 \in L - \{0\}$ such that for every $P \in \mathcal{M}_K$ with $\deg_K(P) = 1$, and $P \neq Q$, $x_0 \in P$. Therefore we get Theorem 4.2.7. \square

So far, using the Theorem 4.2.7, we have an upper bound for the numbers N_r , where $r \in \mathbb{N} - \{0, 1\}$.

More precisely, if $K_{r_0} = K\mathbb{F}_{r_0}$, with q^{r_0} is a square, and $q^{r_0} > (g_K + 1)^4$, then, by Lemma 4.2.2, we may replace K by K_{r_0} . Therefore we get the assumption of Theorem 4.2.7. It follows, since g_K is invariant under constant field extensions, that for all $r \in \mathbb{N} - \{0, 1\}$, q^r is a square, and $q^r > (g_K + 1)^4$. From Theorem 4.2.7 again, we deduce that for all $r \in \mathbb{N} - \{0, 1\}$, $N_r < q^r + 1 + (2g_K + 1)\sqrt{q^r}$. So, there exists $c_1 = 2g_K + 1 > 0$, such that for all $r \in \mathbb{N} - \{0, 1\}$, $N_r - (q^r + 1) < c_1\sqrt{q^r}$.

In order to get the assumptions of Lemma 4.2.4, we need to find $c_2 > 0$ such that for every $r \in \mathbb{N} - \{0, 1\}$, $N_r > q^r + 1 - c_2\sqrt{q^r}$. Therefore the Riemann hypothesis for ζ_A follows from this.

So, our next goal is to give a lower bound for the numbers N_r , with $r \in \mathbb{N} - \{0, 1\}$.

Before doing that we give some group theory results.

Lemma 4.2.11. Let G' be a group such that $G' \simeq \langle \sigma \rangle \times G$, where $\langle \sigma \rangle$ is a cyclic subgroup of G' , G is a subgroup of G' , $\text{ord}(G) = m$, $\text{ord}(\sigma) = n$, and $m|n$.

Let H be a subgroup of G' with $\text{ord}(H) = ne$, and $\text{ord}(H \cap G) = e$.

Then there exist exactly e subgroups U_1, \dots, U_e of H such that for all $i \in \{1, \dots, e\}$, U_i is cyclic of order n , and $U_i \cap G = \{1\}$.

Proof. Let $\tau \in G$. Consider the cyclic subgroup $\langle \sigma\tau \rangle$ of G' .

Claim 1: $\text{ord}(\sigma\tau) = n$.

Proof of the Claim 1.

Proof. It is clear that $(\sigma, 1)(\tau, 1) = (1, \tau)(\sigma, 1)$. As $\text{ord}(\sigma) = n$, $\text{ord}(\tau)|m$, and $m|n$, then $((\sigma, 1)(1, \tau))^n = (\sigma^n, 1)(1, \tau^n) = (1, 1)$. So, $\text{ord}(\sigma\tau) \leq n$.

On the other hand, let $k \in \mathbb{N} - \{0\}$ with $k < n$.

If $(\sigma\tau)^k = 1$, then $\sigma^k = (\tau^{-1})^k$. So $(\tau^{-1})^k \in \langle \sigma \rangle$. Since $\tau^{-1} \in G$, and $\langle \sigma \rangle \cap G = \{1\}$, $(\tau^{-1})^k = 1$. That is $\sigma^k = 1$. That implies $\text{ord}(\sigma) \leq k < n$. This is impossible.

Thus $(\sigma\tau)^k \neq 1$ and hence $\text{ord}(\sigma\tau) = n$. That proves Claim 1. \square

Claim 2:

(i) $\langle \sigma\tau \rangle \cap G = \{1\}$.

(ii) If $\tau' \in G$ such that $\tau' \neq \tau$, then $\langle \sigma\tau \rangle \neq \langle \sigma\tau' \rangle$.

Proof of Claim 2.

Proof. (i) Let $\alpha \in \langle \sigma\tau \rangle \cap G$. Then we can find $i \in \{0, \dots, n-1\}$ such that $\alpha = \sigma^i \tau^i$, because $\alpha \in \langle \sigma\tau \rangle$ and $\text{ord}(\sigma\tau) = n$ by Claim 1.

It follows that $\alpha\tau^{-i} = \sigma^i$. As $\alpha \in G$, $\tau^{-i} \in G$, $\sigma^i \in \langle \sigma \rangle$, and $\langle \sigma \rangle \cap G = \{1\}$, then $\sigma^i = 1$.

But $i \in \{0, \dots, n-1\}$, and $\text{ord}(\sigma) = n$, then $i = 0$.

Thus $\alpha = 1$. Hence $\langle \sigma\tau \rangle \cap G = \{1\}$.

(ii) Let $\tau' \in G$ such that $\tau' \neq \tau$.

Suppose $\langle \sigma\tau \rangle = \langle \sigma\tau' \rangle$. Then $\sigma\tau = (\sigma\tau')^k$, for some $k \in \{0, \dots, n-1\}$. As $\tau' \in G$, then $\sigma\tau' = \tau'\sigma$. Hence $\sigma\tau = \sigma^k(\tau')^k$.

Case 1: If $k \neq 0$.

Then we obtain that $\sigma^{k-1} = (\tau')^{-k}\tau$. Since $\sigma^{k-1} \in \langle \sigma \rangle$, $(\tau')^{-k}\tau \in G$, and $\langle \sigma \rangle \cap G = \{1\}$, $\sigma^{k-1} = 1$. As $\text{ord}(\sigma) = n$, and $0 \leq k-1 < n$, then $k = 1$. Hence $\tau = \tau'$.

Case 2: If $k = 0$.

Then $\sigma\tau = 1$, which contradicts $|\langle \sigma\tau \rangle| = n$.

□

We now return to the proof of the Lemma 4.2.11.

Since $\text{ord}(G) = m$, then $G = \{\tau_1, \dots, \tau_m\}$, with $\tau_i \neq \tau_j$ if $i \neq j$.

From Claim 2, we deduce that $\langle \sigma\tau_1 \rangle, \langle \sigma\tau_2 \rangle, \dots, \langle \sigma\tau_m \rangle$ are pairwise distinct cyclic groups of order n , with $\langle \sigma\tau_i \rangle \cap G = \{1\}$ for any $i \in \{1, \dots, m\}$.

Thus we have found $m = \text{ord}(G)$ distinct subgroups of G' , $U_1 = \langle \sigma\tau_1 \rangle, \dots, U_m = \langle \sigma\tau_m \rangle$ such that for any $i \in \{1, \dots, m\}$, $U_i \cap G = \{1\}$, and $\text{ord}(U_i) = n$. Two more lemmas are needed in order to achieve the proof of Lemma 4.2.11.

Lemma 4.2.12. (i) G is a normal subgroup of G' .

(ii) $H/(H \cap G) \simeq \langle \sigma \rangle$.

Proof. (i) The homomorphism of groups $\varphi : G \times \langle \sigma \rangle \rightarrow \langle \sigma \rangle$, $(\tau, \beta) \mapsto \beta$, satisfies $\ker(\varphi) \simeq G$, so G is a normal subgroup of G' .

(ii) From (i) we obtain $H/(H \cap G) \simeq HG/G$.

Since $\text{ord}(H \cap G) = e$, $\text{ord}(G) = m$, and $\text{ord}(H) = ne$, $\text{ord}(HG) = nm$.

But $G' \simeq \langle \sigma \rangle \times G$, $\text{ord}(\sigma) = n$, and HG is a subgroup of G' , then $HG = G'$.

It follows that $HG/G \simeq \langle \sigma \rangle$.

□

Lemma 4.2.13. There exists $\tau_0 \in G$, such that if $H \cap G = \{\gamma_1, \dots, \gamma_e\}$, then,

(i) for any $j \in \{1, \dots, e\}$, $U_j = \langle \sigma\tau_0\gamma_j \rangle$ is cyclic of order n , and $U_j \cap G = \{1\}$.

(ii) U_1, \dots, U_e are pairwise distinct, and are the only cyclic subgroups of H which has order n .

Proof. From Lemma 4.2.12, (ii), there exists $\lambda_0 \in H$ such that $\text{ord}(\lambda_0 H \cap G) = n$. As $G' = \langle \sigma \rangle \times G$, then $\lambda_0 = \sigma^a \tau'$, for some $a \in \mathbb{Z}$, and for $\tau' \in G$.

Claim 3: There exists $(u, v) \in \mathbb{Z}^2$, such that $au + vn = 1$.

Proof of Claim 3.

Proof. We show that $\text{gcd}(a, n) = 1$.

Suppose there exists $d \in \{1, \dots, n-1\}$ such that $d|n$, $d|a$, and $d > 1$, then $n = dl$, $a = dl_1$, with $(l, l_1) \in \mathbb{Z}^2$, and $l \in \{1, \dots, n-1\}$.

It follows that $al = nl_1$, and thus $\sigma^{al} = 1$. So $\lambda_0^l = (\tau')^l$. From this, we get $(\tau')^l \in H \cap G$. Since $l \in \{1, \dots, n-1\}$, $\text{ord}(\lambda_0 H \cap G) < n$. This gives us a contradiction to $\text{ord}(\lambda_0 H \cap G) = n$. \square

By Claim 3, there exists $(u, v) \in \mathbb{Z}^2$, such that $au + vn = 1$. This implies that $\lambda_0^u = \sigma(\tau')^u$.

Setting $\lambda = \lambda_0^u$, and $\tau_0 = (\tau')^u$, we get $\lambda = \sigma\tau_0$, for some $\tau_0 \in G$. In particular $\sigma\tau_0 \in H$.

Now consider $U_j = \langle \sigma\tau_0\gamma_j \rangle$, for any $j \in \{1, \dots, e\}$. Then for all $j \in \{1, \dots, e\}$, $U_j \subseteq H$.

We also get the following.

Claim 4:

- (i) For all $j \in \{1, \dots, e\}$, U_j is cyclic of order n and $U_j \cap G = \{1\}$.
- (ii) If $(i, j) \in \{1, \dots, e\}^2$, with $i \neq j$, then $U_i \neq U_j$.

Proof of Claim 4.

Proof. (i) Let $j \in \{1, \dots, e\}$. Since we have seen that $\langle \lambda_0(H \cap G) \rangle$ is cyclic of order n , and from Claim 3, $\text{gcd}(u, n) = 1$, then $\langle \lambda_0^u(H \cap G) \rangle$ is cyclic of order n . That means that $\langle \sigma\tau_0(H \cap G) \rangle$ is cyclic of order n . Then, we get a surjective homomorphism $U_j \rightarrow \langle \sigma\tau_0(H \cap G) \rangle$, $(\sigma\tau_0\gamma_j)^k \mapsto (\sigma\tau_0)^k(H \cap G)$. It follows that $n = \text{ord}(\langle \sigma\tau_0(H \cap G) \rangle) \leq \text{ord}(U_j)$.

On the other hand, since $m|n$, $(\sigma\tau_0\gamma_j)^n = \sigma^n(\tau_0\gamma_j)^n = 1$. Then $\text{ord}(U_j) \leq n$. Hence U_j is cyclic of order n .

From Claim 2, (i), since $\tau_0\gamma_j \in G$, we obtain $U_j \cap G = \{1\}$.

- (ii) Let $(i, j) \in \{1, \dots, e\}^2$, with $i \neq j$.

As $\gamma_i \neq \gamma_j$, and $\tau_0 \in G$, then, by Claim 2, (ii), $\langle \sigma\tau_0\gamma_i \rangle \neq \langle \sigma\tau_0\gamma_j \rangle$. \square

By Claim 4, we obtain Lemma 4.2.13, (i), and the first assertion of Lemma 4.2.13, (ii). \square

In order to prove the second assertion of Lemma (4.2.13), (ii), we need the following claim.

Claim 5: If U is a cyclic subgroup of H such that $\text{ord}(U) = n$, and $U \cap G = \{1\}$, then there exists $j_0 \in \{1, \dots, e\}$ such that $U = U_{j_0}$, where U_{j_0} is defined in Claim 4.

Proof of Claim 5.

Proof. By assumption, we can find $\delta_0 \in H$ such that $\langle \delta_0 \rangle = U$, and $\text{ord}(\delta_0) = n$. As $G' = \langle \sigma \rangle \times G$, then there exist $a_1 \in \mathbb{Z}$, and $\tau' \in G$ such that $\delta_0 = \sigma^{a_1} \tau'$. We have the following.

Claim 6: There exist $(u_1, v_1) \in \mathbb{Z}^2$, such that $a_1 u_1 + v_1 n = 1$.

Proof of the claim.

Proof. Suppose there exists $d \in \{1, \dots, n-1\}$ such that $d|n$, $d|a_1$, and $d > 1$, then $n = dl$, $a_1 = dl_1$, with $(l, l_1) \in \mathbb{Z}^2$, and $l \in \{1, \dots, n-1\}$.

It follows that $a_1 l = nl_1$, and thus $\sigma^{a_1 l} = 1$. So $\delta_0^l = (\tau')^l$. From this, we get $(\tau')^l \in U \cap G$. Since $l \in \{1, \dots, n-1\}$, $H \cap G = \{1\}$, $\text{ord}(\delta_0) < n$. This gives us a contradiction to $\text{ord}(\delta_0) = n$. \square

From Claim 6, and the fact that $\text{ord}(\sigma) = n$, we deduce that $\delta_0^{u_1} = \sigma(\tau')^{u_1}$. Since $(u_1, n) = 1$, $\langle \delta_0 \rangle = U$, and $\text{ord}(\delta_0) = n$, then $\langle \delta_0^{u_1} \rangle = U$. That means that $U = \langle \sigma \tau_1 \rangle$, where $\tau_1 \in G$.

As $U \subseteq H$, then $\sigma \tau_1 \in H$.

On the other hand, since $\lambda_0 \in H$, then $\sigma \tau_0 \in H$. Thus $\tau_0^{-1} \sigma^{-1} \sigma \tau_1 = \tau_0^{-1} \tau_1 \in H \cap G$. It follows that $U = \langle \sigma \tau_0 \gamma_j \rangle$, for some $j \in \{1, \dots, e\}$.

That shows that U_1, \dots, U_e are the only cyclic subgroups of H which have order n . That prove Lemma 4.2.13. \square

From Lemma 4.2.13, we deduce that there exist exactly e subgroups U_1, \dots, U_e of H such that for all $i \in \{1, \dots, e\}$, U_i is cyclic of order n , and $U_i \cap G = \{1\}$. Thus, we obtain Lemma 4.2.11. \square

4.3 Constant Field Extensions

The second part of the proof is to use the main result, which is Theorem 4.2.7, of the previous section for the finite extension of constant field extensions of K .

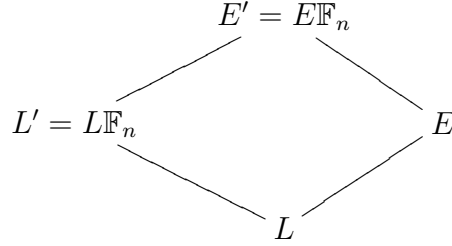
Lemma 4.3.1. Let E/L be a Galois extension of global function fields with $[E : L] = m$. Assume that \mathbb{F} is the full constant field of both E , and L . Let $n \in \mathbb{N} - \{0\}$ with $m|n$, and let us set $E' = E\mathbb{F}_n$, $L' = L\mathbb{F}_n$.

Then,

- (i) E'/L' is Galois.

- (ii) $\text{Gal}(E'/L) \simeq \langle \sigma_{E'/E} \rangle \times \text{Gal}(E'/L')$, where $\sigma_{E'/E}$ is the Frobenius automorphism of E'/E , which is defined by, for any $z \in E$, $\sigma_{E'/E}(z) = z$, and for any $\alpha \in \mathbb{F}_n$, $\sigma_{E'/E}(\alpha) = \alpha^q$.

Proof. (i) Let us show that E'/L is separable.



Since E/L is a Galois extension, E/L is separable. As \mathbb{F}_n/\mathbb{F} is a Galois extension, $E\mathbb{F}_n/L\mathbb{F}$ is separable, that is E'/L is separable.

Let us show that E'/L is a normal extension.

Let $\tau : E' \rightarrow \bar{E}$ be an L -homomorphism of fields, where \bar{E} is an algebraically closed field which contains E' .

We need to show that $\tau(E') \subseteq E'$.

Let $y \in E'$. Then $y = \sum_{i=1}^s x_i z_i$, with $s \in \mathbb{N}$, for any $i \in \{1, \dots, s\}$, $x_i \in E$, and $z_i \in \mathbb{F}_n$.

Since τ is an L -homomorphism, $\tau(y) = \sum_{i=1}^s \tau(x_i)\tau(z_i)$.

As $\tau|_E$ is an L -homomorphism, and E/L is Galois, $\tau|_E(E) \subseteq E$. Thus for any $i \in \{1, \dots, s\}$, $\tau(x_i) \in E$.

On the other hand, since \mathbb{F}_n/\mathbb{F} is Galois, and $\tau|_{\mathbb{F}_n}$ is an \mathbb{F} -homomorphism, then for all $i \in \{1, \dots, s\}$, $\tau(z_i) \in \mathbb{F}_n$. It follows that $\tau(y) \in E'$. So, $\tau(E') \subseteq E'$.

That shows that for any L -homomorphism $\tau : E' \rightarrow \bar{E}$, we get $\tau(E') \subseteq E'$, which means E'/L is a normal extension.

So, E'/L is a Galois extension.

- (ii) First of all let us set $G' = \text{Gal}(E'/L)$, and $G = \text{Gal}(E'/L')$, and $\sigma = \sigma_{E'/E}$.

From the assumption $E' = E\mathbb{F}_n$, and $L' = L\mathbb{F}_n$, then $G \simeq \text{Gal}(E/L)$.

Let $i \in \mathbb{N}$, and let $\tau \in G$. Let us show that $\sigma^i \tau \in G'$.

It is clear that $\sigma^i \tau \in \text{Aut}(E')$, where $\text{Aut}(E')$ is the set of automorphisms of E' .

Let $x \in L$. As τ is an L' -automorphism of E' , σ is an E -automorphism of E' , and $L \subseteq E$, then $\sigma^i \tau(x) = x$.

Thus $\sigma^i \tau \in G'$. Hence $\langle \sigma \rangle G \subseteq G'$.

Now, let us prove that $\langle \sigma \rangle \cap G = \{1\}$.

Let $\tau \in \langle \sigma \rangle \cap G$, then there exists $i \in \mathbb{N}$, such that $\tau = \sigma^i$.

Let $x \in E'$. Then there exists $t \in \mathbb{N}$ such that $x = \sum_{j=1}^t x_j y_j$, where for any $j \in \{1, \dots, t\}$, $x_j \in E$, and $y_j \in \mathbb{F}_n$. It follows that $\sigma^i(x) =$

$\sum_{j=1}^t \sigma^i(x_j)\tau(y_j)$. Since $\mathbb{F}_n \subseteq L'$, $\sigma \in \text{Gal}(E'/E)$, and $\tau \in G$, then $\sigma^i(x) = \sum_{j=1}^t x_j y_j = x$. Therefore $\tau(x) = x$. Hence $\tau = 1$.

These prove that $\langle \sigma \rangle \text{Gal}(E'/L')$ is a direct product.

Suppose that $|\langle \sigma \rangle G| = |G'|$, then $G' \simeq \langle \sigma \rangle \times G$.

We need to show that $|\langle \sigma \rangle G| = |G'|$.

As $\langle \sigma \rangle G$ is a direct product, then $\langle \sigma \rangle G \simeq \langle \sigma \rangle \times G$.

Let us show that $|\langle \sigma \rangle| = n$.

Let $\alpha \in \mathbb{F}_n$. Then $\sigma^n(\alpha) = \sigma^{n-1}(\alpha^q) = \dots = \sigma(\alpha^{q^{n-1}}) = \alpha^{q^n} = \alpha$, because \mathbb{F}_n is a field of cardinality q^n .

Since $\sigma^n(\alpha) = \alpha$, for all $\alpha \in E$, then $\sigma^n = 1$.

Suppose that there exists $k_0 \in \mathbb{N}$ such that $k_0 < n$, and $\sigma^{k_0} = 1$.

Then, for all $\alpha \in \mathbb{F}_n$, $\alpha^{q^{k_0}} = \alpha$. Therefore $\mathbb{F}_n \subseteq \mathbb{F}_{k_0}$. That means $n|k_0$.

That contradicts to $k_0 < n$. It follows that $|\langle \sigma \rangle| = n$.

Since $G \simeq \text{Gal}(E/L)$, and $|\text{Gal}(E/L)| = [E : L] = m$, then $|G| = m$.

Hence $|\langle \sigma \rangle G| = mn$.

Let us show that $|G'| = mn$.

On one hand, we have $|G'| = [E' : L] = [E' : L'][L' : L] = m[L' : L]$.

On the other hand we obtain $[L' : L] = [L\mathbb{F}_n : L\mathbb{F}] = [\mathbb{F}_n : \mathbb{F}] = n$. Thus $|G'| = nm$.

We deduce the result. □

Corollary 4.3.2. Let E/L be a Galois extension of global function fields with $[E : L] = m$. Assume that \mathbb{F} is the full constant field of both E , and L .

Let $n \in \mathbb{N} - \{0\}$ with $m|n$, and let us set $E' = E\mathbb{F}_n$, $L' = L\mathbb{F}_n$.

Then $\text{Gal}(E'/L)$ contains exactly m cyclic subgroups $U_1 = \langle \sigma_{E'/E} \rangle, \dots, U_m$ such that for all $j \in \{1, \dots, m\}$, $\text{ord}(U_j) = n$, and $U_j \cap \text{Gal}(E'/L') = \{1\}$.

Proof. From Lemma 4.3.1, (ii), we have $\text{Gal}(E'/L) \simeq \langle \sigma_{E'/E} \rangle \times \text{Gal}(E'/L')$. Since $\langle \sigma_{E'/E} \rangle$ is a cyclic subgroup of $\text{Gal}(E'/L)$, $\text{Gal}(E'/L')$ is a subgroup of $\text{Gal}(E'/L)$, $\text{ord}(\text{Gal}(E'/L')) = m$, $\text{ord}(\sigma_{E'/E}) = n$, $m|n$, and $\text{ord}(\text{Gal}(E'/L) \cap \text{Gal}(E'/L')) = m$.

Then, by Lemma 4.2.11, there exist exactly m subgroups U_1, \dots, U_m of $\text{Gal}(E'/L)$ such that for all $i \in \{1, \dots, m\}$, U_i is cyclic of order n , and $U_i \cap \text{Gal}(E'/L') = \{1\}$.

Moreover, since $\langle \sigma_{E'/E} \rangle$ is cyclic of order n , and $\langle \sigma_{E'/E} \rangle \cap \text{Gal}(E'/L') = \{1\}$, then we may assume that $U_1 = \langle \sigma_{E'/E} \rangle$. □

Definition 4.3.3. Let E/L be a Galois extension of global function fields with $[E : L] = m$, and let $j \in \{1, \dots, m\}$, and let us set $E' = E\mathbb{F}_n$, where $n \in \mathbb{N} - \{0\}$.

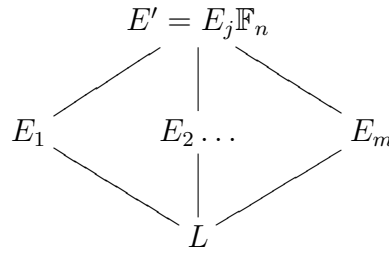
(i) The set $E_j = (E')^{U_j}$ is called the fixed field of U_j .

- (ii) g_{E_j} is the genus of E_j .
- (iii) $N(E_j)$ (respectively $N(L)$) is the number of places of degree 1 of E_j (respectively L).

Proposition 4.3.4. With the same notations as in Definition 4.3.3

- (i) For any $j \in \{1, \dots, m\}$, \mathbb{F} is the full constant field of E_j .
- (ii) For any $j \in \{1, \dots, m\}$, $E' = E_j\mathbb{F}_n$ and $g_{E_j} = g_E$.
- (iii) $mN(L) = \sum_{j=1}^m N(E_j)$.

Proof.



- (i) Let $j \in \{1, \dots, m\}$. As $U_j = \text{Gal}(E'/E_j)$, $\text{Gal}(E'/L) \cap U_j = \{1\}$, by Corollary 4.3.2, then, from Galois theory, $\text{Gal}(E'/E_jL) = \{1\}$. Therefore $E' = E_jL'$.
So, $E' = E_jL\mathbb{F}_n = E_j\mathbb{F}_n$.
Now, let F_j be the full constant field of E_j . Since $L \subseteq E_j$, and \mathbb{F} is the full constant field of L , then F_j/\mathbb{F} is finite.
Since $E' = E\mathbb{F}_n$ is the constant field extension of $E\mathbb{F}$, \mathbb{F}_n is the constant field of E' .
But $E_j \subseteq E'$, then $F_j \subseteq \mathbb{F}_n$. It follows that $[\mathbb{F}_n : \mathbb{F}] = [\mathbb{F}_n : F_j][F_j : \mathbb{F}] = n$.
On the other hand, we get $[E' : E_j] = [E_j\mathbb{F}_n : E_jF_j] = [\mathbb{F}_n : F_j] = |U_j| = n$. Therefore $[F_j : \mathbb{F}] = 1$. That means $F_j = \mathbb{F}$.
- (ii) Let $j \in \{1, \dots, m\}$. Since E'/E_j is a constant field extension and E'/E is a constant field extension, then, from Theorem 2.3.12, (iii), we obtain $g_{E_j} = g_{E'} = g_E$.
- (iii) Let us set $X = \{P \in \mathcal{M}_L : \deg_L(P) = 1\}$, and for any $j \in \{1, \dots, m\}$, let us set $X_j = \{Q \in \mathcal{M}_{E_j} : \deg_{E_j}(Q) = 1\}$.
In order to prove this assertion, we need some lemmas.

Lemma 4.3.5. Let $j \in \{1, \dots, m\}$, and let $P \in X$. For all $Q \in X_j$ such that $Q|P$, there exists a unique $Q' \in \mathcal{M}_{E'}$ which lies above Q .

Proof. Let $Q \in X_j$, such that $Q|P$. Since E'/E_j and E_j/L are finite extension of global function fields, there exists $Q' \in \mathcal{M}_{E'}$, such that $Q'|Q$. We want to show that Q' is unique.

Claim 7: Let $Q' \in \mathcal{M}_{E'}$ such that $Q'|Q$. Then $f(Q'|Q) = n$.

Proof of Claim 7.

Proof.

$$\begin{array}{ccc} E' & & Q' \\ | & & | \\ E_j & & Q_j \\ | & & | \\ L & & P \end{array}$$

As $E' = E_j\mathbb{F}_n$ is the constant field extension of E/\mathbb{F} , which is finite and the full constant field of E' is \mathbb{F}_n , then, by Theorem 2.3.12, (v), we get $E'_{Q'} = (E_j)_Q\mathbb{F}_n$. So, $f(Q'|Q) = [(E')_{Q'} : (E_j)_Q] = [(E_j)_Q\mathbb{F}_n : (E_j)_Q\mathbb{F}] = [\mathbb{F}_n : \mathbb{F}] = n$.

□

We now return to the proof of Lemma 4.3.5.

Let us prove that

$$f(Q'|Q) = [E' : E_j]. \quad (4.3.1)$$

From Claim 7, we have $f(Q'|Q) = n$, because $Q' \in \mathcal{M}_{E'}$ such that $Q'|Q$. Since $Q \in X_j$, and $P \in X$, then $\deg_{E_j}(Q) = [(E_j)_Q : \mathbb{F}] = f(Q|P) \deg_L(P) = f(Q|P) = 1$. Therefore $f(Q'|P) = n = f(Q'|Q)$.

But $E_j = (E')^{U_j}$, so, by Galois theory, E'/E_j is a Galois extension and $[E' : E_j] = |U_j| = n$. It follows $f(Q'|Q) = [E' : E_j]$.

Let us denote by r_j the number of places of E' above Q .

Again, using the fact that E'/E_j is a Galois extension, we obtain, From Proposition 2.4.3, $e(Q'|Q)f(Q'|Q)r_j = [E' : E_j]$.

Thus, by (4.3.1), $e(Q'|Q) = r_j = 1$. We conclude that Q' is unique. □

We also need a proposition.

Proposition 4.3.6. For all $Q' \in \mathcal{M}_{E'}$, such that $Q'|P$, there are exactly $e = e(Q'|P)$ distinct places $Q_1, \dots, Q_e \in \bigcup_{i=1}^m X_i$ such that for any $i \in \{1, \dots, e\}$, $Q'|Q_i$.

Proof. Let $Q' \in \mathcal{M}_{E'}$ with $Q'|P$. Let H be the decomposition group of Q' over P , $Z = (E')^H$ be the fixed field of H , and $P_Z = Q' \cap Z$.

Then, by [1, Theorem 3.8.2, (a)], $|H| = e(Q'|P)f(Q'|P)$.
 From [1, Theorem 3.8.2, (c)], we get $f(P_Z|P) = 1$.

Claim 9: \mathbb{F} is the full constant field of Z .

Proof of Claim 9.

Proof. Let K_1 be the constant field of Z . Since $L \subseteq Z \subseteq E'$, and, by assumption, \mathbb{F} is the constant field of L , then $\mathbb{F} \subseteq K_1$.

On the other hand, we have seen that $f(P_Z|P) = [Z_{P_Z} : L_P] = 1$. Since $[L_P : \mathbb{F}] = \deg_L(P) = 1$, $[Z_{P_Z} : \mathbb{F}] = 1$. Thus $Z_{P_Z} = \mathbb{F}$.

As we have an embedding of fields $K_1 \hookrightarrow Z_{P_Z}$, then $K_1 \subseteq \mathbb{F}$. We conclude that $K_1 = \mathbb{F}$. □

Claim 10: $[E' : ZL'] = e(Q'|P)$.

Proof of Claim 10.

Proof. From Galois theory, we have $(E')^{H \cap \text{Gal}(E'/L')} = ZL'$. As $L \subseteq Z$, $ZL' = ZL\mathbb{F}_n = Z\mathbb{F}_n$.

By Claim 9, we get \mathbb{F} is the full constant field of Z . So $Z\mathbb{F}_n/Z\mathbb{F}$ is a constant field extension of degree n , then $[Z\mathbb{F}_n : Z] = n$.

On the other hand, we know that $[E' : Z] = [E' : ZL'] [ZL' : Z]$, so $[E' : Z] = \frac{[E' : ZL']}{[ZL' : Z]} = \frac{|H|}{[ZL' : Z]} = \frac{e(Q'|P)f(Q'|P)}{n}$.

From Claim 7, we obtain $f(Q'|P) = n$. Hence $[E' : ZL'] = e(Q'|P)$. □

Lemma 4.3.7.

$$ZL' = T(Q'|P), \tag{4.3.2}$$

where $T(Q'|P)$ is the inertia field of $Q'|P$.

Proof of Lemma 4.3.7.

Proof. Let us show $ZL' \subseteq T(Q'|P)$.

As E'/L is a Galois extension of algebraic global function field, $P \in \mathcal{M}_L$, $Q' \in \mathcal{M}_{E'}$ such that $Q'|P$, $L \subseteq ZL' \subseteq E'$, and $P_{ZL'} = Q' \cap ZL'$, then, from [1, Theorem 3.8.3, (c)], $ZL' \subseteq T(Q'|P)$ if and only if $e(P_{ZL'}|P) = 1$. So, it is sufficient to show that $e(P_{ZL'}|P) = 1$.

Since $P_Z = Q' \cap Z = Q' \cap (Z \cap ZL')$, $P_Z = (Q' \cap ZL') \cap Z = P_{ZL'} \cap Z$. Therefore $P_{ZL'}|P_Z$. As $ZL' = Z\mathbb{F}_n$, then $ZL'/Z\mathbb{F}$ is a constant field extension. It follows that P_Z is unramified in ZL' , and thus $e(P_{ZL'}|P_Z) = 1$. But, from [1, Theorem 3.8.2, (c)], $e(P_Z|P) = 1$, so, by Proposition 2.3.8,

(ii), we get $e(P_{ZL'}|P) = 1$.

Let us show $T(Q'|P) \subseteq ZL'$.

It is clear that $Q'|P_{ZL'}$.

Since we have seen that $e(P_{ZL'}|P) = 1$, then $e(Q'|P) = e(Q'|P_{ZL'})$.

On the other hand, from Claim 10, we have $e(Q'|P) = [E' : ZL']$. Therefore $e(Q'|P_{ZL'}) = [E' : ZL']$.

We have shown that we can find $Q' \in \mathcal{M}_{E'}$ such that $Q'|P_{ZL'}$ and $e(Q'|P_{ZL'}) = [E' : ZL']$. That means, by [1, Theorem 3.8.3], $P_{ZL'}$ is totally ramified in E'/ZL' . But E'/L is a Galois extension of algebraic function fields, then this is equivalent to $ZL' \supseteq T(Q'|P)$.

We thus conclude that $ZL' = T(Q'|P)$. \square

Corollary 4.3.8. $I(Q'|P) = H \cap \text{Gal}(E'/L)$, where $I(Q'|P)$ is the inertia group of $Q'|P$.

Proof. Since $(E')^{H \cap \text{Gal}(E'/L)} = T(Q'|P)$, and by Lemma 4.3.7, $ZL' = T(Q'|P)$. Thus $I(Q'|P) = H \cap \text{Gal}(E'/L)$. \square

We now return to the proof of the Proposition 4.3.6.

Since we know that $\text{Gal}(E'/L) \simeq \langle \sigma_{E'/E} \rangle \times \text{Gal}(E'/L)$, H subgroup of $\text{Gal}(E'/L)$ with $|H| = en$, and $|H \cap \text{Gal}(E'/L)| = n$, then, by Lemma 4.2.11, there are exactly e subgroups V_1, \dots, V_e of H such that for any $i \in \{1, \dots, e\}$, V_i is cyclic of order n , and $V_i \cap \text{Gal}(E'/L) = \{1\}$.

But $\text{Gal}(E'/L)$ has exactly m cyclic subgroups U_1, \dots, U_m with $U_i \cap \text{Gal}(E'/L) = \{1\}$, and $|U_i| = n$ for any $i \in \{1, \dots, m\}$.

It follows that $V_1 = U_{i_1}, \dots, V_e = U_{i_e}$ where $i_j \in \{1, \dots, m\}$, for any $j \in \{1, \dots, e\}$.

Let $j \in \{1, \dots, e\}$, and let us set $Q_{i_j} = Q' \cap E_{i_j}$.

Claim 11: Q' is the only place of E' which lies over Q_{i_j} , and

$$f(Q'|Q_{i_j}) = n \quad (4.3.3)$$

Proof of the Claim 11.

Proof. Since $U_{i_j} \subseteq H$, then, by the fundamental theorem of Galois theory, we obtain $E_{i_j} \supseteq Z = Z(Q'|P)$.

As E'/L is a Galois extension of algebraic function fields, $P \in \mathcal{M}_L$, $Q' \in \mathcal{M}_{E'}$, with $Q'|P$, $L \subseteq Z \subseteq E_{i_j} \subseteq E'$, and $Q_{i_j} = Q' \cap E_{i_j}$, then, by [1, Theorem 3.8.3, (b)], Q' is the only place of E' with $Q'|Q_{i_j}$. That prove the first assertion of the Claim 11.

On the other hand, $e(Q'|Q_{i_j}) = 1$.

Indeed, from Proposition 4.3.4, (ii), $E' = E_{i_j}\mathbb{F}_n$, that is $(E'/\mathbb{F}_n) / (E_{i_j}/\mathbb{F})$

is a constant field extension. So we get the result from [1, Theorem 3.6.3 (a)].

As E'/E_{i_j} is a finite Galois extension, and Q' is the only place of E' lying above Q_{i_j} , then by the fundamental equality, we have $f(Q'|Q_{i_j})e(Q'|Q_{i_j}) = [E' : E_{i_j}] = |U_{i_j}| = n$. Thus $f(Q'|Q_{i_j}) = n$. \square

Claim 12: $f(Q_{i_j}|P_Z) = 1$.

Proof of Claim 12.

Proof. From Claim 7, and the fact that $P \in X$, $Q \in X_j$, and $f(P_Z|P) = 1$, then we get $f(Q'|P) = f(Q'|Q_{i_j})f(Q_{i_j}|P_Z) = nf(Q_{i_j}|P_Z) = n$. So $f(Q_{i_j}|P_Z) = 1$. \square

Claim 13: $\deg_{E_{i_j}}(Q_{i_j}) = 1$.

Proof of claim 13.

Proof. On one hand, we have, $[E'_{Q'} : \mathbb{F}] = [E'_{Q'} : (E_{i_j})_{Q_{i_j}}][(E_{i_j})_{Q_{i_j}} : \mathbb{F}] = f(Q'|Q_{i_j}) \deg_{E_{i_j}}(Q_{i_j})$.

from Claim 11, we have $f(Q'|Q_{i_j}) = n$. It implies $[E'_{Q'} : \mathbb{F}] = n \deg_{E_{i_j}}(Q_{i_j})$.

On the other hand, we obtain $[E'_{Q'} : \mathbb{F}] = [E'_{Q'} : L_P][L_P : \mathbb{F}]$. As $[L_P : \mathbb{F}] = \deg_L(P) = 1$, and $[E'_{Q'} : L_P] = f(Q'|P) = n$, therefore $[E'_{Q'} : \mathbb{F}] = n$.

It follows that $\deg_{E_{i_j}}(Q_{i_j}) = 1$. \square

Now, we go back to the proof of Proposition 4.3.6.

From Claim 13, we deduce that $Q_{i_j} \in \bigcup_{i=1}^m X_i$.

Since for $(j, l) \in \{1, \dots, e\}^2$, $E_{i_j} \neq E_{i_l}$, then $Q_{i_j} \neq Q_{i_l}$.

It follows that there are e distinct places Q_{i_1}, \dots, Q_{i_e} which belong to $\bigcup_{i=1}^m X_i$. That proves the existence.

Now, we want to prove the uniqueness.

Let $Q \in X_i$, for some $i \in \{1, \dots, m\}$ such that $Q'|Q$. Then, from Claim 7, we have $f(Q'|Q) = n$.

Now, since E'/L is a Galois extension of algebraic function field, $P \in \mathcal{M}_L$, $Q'|\mathcal{M}_{E'}$ with $Q'|P$, $Q = Q' \cap E_i$, and $L \subseteq E_i \subseteq E'$, if Q' is the only place of E' lying over Q , then, from [1, Theorem 3.8.3, (b)], we deduce $E_i \supseteq Z(Q'|P) = Z$, that is, by the fundamental theorem of Galois, $U_i \subseteq H$. Since U_i is cyclic of order n , and $U_i \cap G = \{1\}$, then $U_i = U_{i_l}$ for some $l \in \{1, \dots, e\}$. That means $Q = Q' \cap E_{i_l} = Q_{i_l}$, for some $l \in \{1, \dots, e\}$.

Let us show that Q' is the only place of E' lying over Q .

Since E'/E_i is a finite Galois extension of function fields, and $Q \in \mathcal{M}_{E_i}$, then by the fundamental equality we have $\sum_{j=1}^s e(P_j|Q)f(P_j|Q) = [E' : E_i]$, where $s \in \mathbb{N} - \{0\}$, and $P_1 = Q', \dots, P_s$ are the places of E'/\mathbb{F}_n lying above Q .

As $[E' : E_i] = |\text{Gal}(E'/E_i)| = |U_i| = n$, and $f(Q'|Q) = f(P_1|Q) = n$, then $s = 1$. It follows that Q' is the only place of E' lying over Q .

That is the end of Proposition 4.3.6. \square

We now return to the proof of Proposition 4.3.4.

Claim 14 $|\bigcup_{j=1}^m X_j| = m|X|$.

Proof of the Claim 14.

Proof. Let $P \in X$.

Let $Q' \in \mathcal{M}_{E'}$ such that $Q'|P$.

From Proposition 4.3.6, we can find exactly $e = e(Q'|P) = e(P)$ distinct places $Q_{i_1, Q'}, \dots, Q_{i_e, Q'}$ in $\bigcup_{i=1}^m X_i$ such that for all $j \in \{1, \dots, e\}$, $Q'|Q_{i_j, Q'}$. Moreover if $Q'' \in \mathcal{M}_{E'}$ with $Q''|P$, and $Q'' \neq Q'$, then by Lemma 4.3.5, $\{Q_{i_1, Q'}, \dots, Q_{i_e, Q'}\} \cap \{Q_{i_1, Q''}, \dots, Q_{i_e, Q''}\} = \emptyset$.

Let us denote by r the number of places of E' which are above P . Then, there are exactly er elements of $\bigcup_{i=1}^m X_i$ which lay above P .

It follows that $re|X| = |\bigcup_{i=1}^m X_i|$.

Let us show that $re = m$.

Since E'/L is a finite Galois extension, $Q' \in \mathcal{M}_{E'}$ such that $Q'|P$, by the fundamental equality, we obtain $[E' : L] = ef(Q'|P)r$.

But $[E' : L] = [E' : E][E : L] = nm$, and from Claim 7 and the fact that $\deg_L(P) = 1$, we have $f(Q'|P) = n$. Thus $re = m$. Therefore $m|X| = |\bigcup_{i=1}^m X_i|$. \square

Returning to the proof of Proposition 4.3.4, (iii).

We claim that $X_i \cap X_j = \emptyset$ for $i \neq j$.

Indeed, if there exists $Q \in X_i \cap X_j$, then Q is a place of E_i , and Q is a place of E_j . So, $\text{Quot}(\mathcal{O}_Q) = E_i$, and $\text{Quot}(\mathcal{O}_Q) = E_j$. Therefore $E_i = E_j$. That is impossible.

It follows that $m|X| = \sum_{i=1}^m |X_i|$.

\square

4.4 End of the Proof of the Riemann Hypothesis for ζ_A

The main result of this section is to conclude the proof of Theorem 4.1.1. We start with an important lemma.

Lemma 4.4.1. There exists $t \in K$ such that $K/\mathbb{F}(t)$ is separable, and there exists a finite extension E/K which satisfies $E/\mathbb{F}(t)$ is a Galois extension.

Proof. See [1, Proposition 3.10.2] . \square

Claim 15: If \mathbb{F}_d is the constant field of E , where E is defined by Lemma 4.4.1, then E is a Galois extension of $\mathbb{F}(t)\mathbb{F}_d$, where $\mathbb{F}(t)$ is also defined by Lemma 4.4.1.

Proof of the Claim 15.

Proof. From Lemma 4.4.1, we get $E/\mathbb{F}(t)$ is a Galois extension of global function fields. Therefore $(E\mathbb{F}_d)/(\mathbb{F}(t)\mathbb{F}_d)$ is a Galois extension. By assumption \mathbb{F}_d is the constant field of E , so $E/(\mathbb{F}(t)\mathbb{F}_d)$ is a Galois extension. \square

Claim 16: The roots of the equation $L_{K\mathbb{F}_d}(q^{-z}) = 0$ all have real part $\frac{d}{2}$, if and only if the roots of the equation $L_K(q^{-z}) = 0$ all have real parts equal to $\frac{1}{2}$.

Proof. Since $K\mathbb{F}_d/K$ is a constant field extension of global function fields, then Claim 16 follows directly from Lemma 4.2.2. \square

From Claim 16, we may assume that \mathbb{F} is the constant field of E , q is a square and $q > (g_E + 1)^4$.

In the following, \mathbb{F} will be the constant field of E , q will be a square and $q > (g_E + 1)^4$.

Let us set $m = [E : K]$, and $n = [E : \mathbb{F}(t)]$. Let us also consider the constant field extensions $E' = E\mathbb{F}_n$, $K' = K\mathbb{F}_n$, and $K_0 = \mathbb{F}(t)\mathbb{F}_n$.

Claim 17: There are exactly m different cyclic subgroups V_1, \dots, V_m of $\text{Gal}(E'/K)$ such that for any $j \in \{1, \dots, m\}$, $|V_j| = n$ and $V_j \cap \text{Gal}(E'/K') = \{1\}$.

Proof of Claim 17.

Proof. Let us set $G' = \text{Gal}(E'/\mathbb{F}(t))$, and $G = \text{Gal}(E'/K_0)$.

Let us show that $G' \simeq \langle \sigma_{E'/E} \rangle \times G$.

Since $K_0 \supseteq \mathbb{F}(t)$ and, by Lemma 4.4.1, $E \supseteq \mathbb{F}(t)$, $\langle \sigma_{E'/E} \rangle \times G \subseteq G'$.

Claim 18: $\langle \sigma_{E'/E} \rangle \cap G = \{1\}$.

Proof of Claim 18.

Proof. Let $\tau \in \langle \sigma_{E'/E} \rangle \cap G$, then there is $l \in \mathbb{N}$, such that $\tau = \sigma_{E'/E}^l$.

Let $x \in E'$. Then there exists $s \in \mathbb{N} - \{0\}$, such that $x = \sum_{j=1}^s x_j y_j$, where for all $j \in \{1, \dots, s\}$, $x_j \in E$, and $y_j \in \mathbb{F}_n$.

As τ is an automorphism of fields, then $\sigma_{E'/E}^l(x) = \sum_{j=1}^s \sigma_{E'/E}^l(x_j) \sigma_{E'/E}^l(y_j)$.

That is $\sigma_{E'/E}^l(x) = \sum_{j=1}^s x_j \sigma_{E'/E}^l(y_j)$, because $\sigma_{E'/E}$ is the Frobenius automorphism of E'/E .

Since $\sigma_{E'/E}^l \in G$, and $K' \supseteq \mathbb{F}_n$, then $\sigma_{E'/E}^l(y_j) = y_j$, for all $j \in \{1, \dots, s\}$. Thus $\sigma_{E'/E}^l(x) = \sum_{j=1}^s x_j y_j = x$.

It follows that $\tau = 1$. Hence we get the result. \square

From Claim 18, we deduce that $\langle \sigma_{E'/E} \rangle G$ is a direct product.

To show that $G' \simeq \langle \sigma_{E'/E} \rangle \times G$, it is sufficient to show that $|G'| = |\langle \sigma_{E'/E} \rangle| |G|$.

Since $n = [E : \mathbb{F}(t)]$, and $\sigma_{E'/E}$ is the Frobenius automorphism of E'/E , one can easily show that $|\langle \sigma_{E'/E} \rangle| = n$.

It is clear that $|G| = n$.

On the other hand, we have $|G'| = [E' : \mathbb{F}(t)] = [E\mathbb{F}_n : E][E : \mathbb{F}(t)] = n[E\mathbb{F}_n : E\mathbb{F}] = n[\mathbb{F}_n : \mathbb{F}]$. So, $|G'| = n^2$.

Therefore $|G'| = |\langle \sigma_{E'/E} \rangle| |G|$.

Now let us return to the proof of Claim 17.

Let us set $H = \text{Gal}(E'/K)$. As $[E : K] = m$, then $|H| = [E' : K] = [E' : E][E : K] = [E\mathbb{F}_n : E\mathbb{F}]m$.

Thus $|H| = nm$.

Claim 19: $H \cap G = \text{Gal}(E'/K')$.

Proof of Claim 19.

Proof. Let us show that $H \cap G \subseteq \text{Gal}(E'/K')$.

Let $\tau \in H \cap G$. Then τ is an K -automorphism of E' , and an K_0 -automorphism of E' . From the fact that $K' = K\mathbb{F}_n$, if $x \in K'$, then, one can show easily that $\tau(x) = x$.

So, $\tau \in \text{Gal}(E'/K')$. Hence $H \cap G \subseteq \text{Gal}(E'/K')$.

On the other hand, it is clear that $\text{Gal}(E'/K') \subseteq \text{Gal}(E'/K) \cap \text{Gal}(E'/K_0)$, that is $\text{Gal}(E'/K') \subseteq H \cap G$. \square

It follows from Claim 19, that $|H \cap G| = [E' : K'] = [E : K] = m$.

As $m|n$, by Lemma 4.2.11, there exist exactly m pairwise distinct cyclic subgroups V_1, \dots, V_m of H such that for all $j \in \{1, \dots, m\}$, $V_j \cap \text{Gal}(E'/K') = \{1\}$, and $|V_j| = n$.

As $\text{Gal}(E'/K') \subseteq \text{Gal}(E'/K_0)$, there are exactly m pairwise distinct cyclic subgroups V_1, \dots, V_m of $\text{Gal}(E'/K')$ such that for all $j \in \{1, \dots, m\}$, $V_j \cap G = \{1\}$, and $|V_j| = n$. \square

Claim 20: There exist n cyclic subgroups U_1, \dots, U_n of $\text{Gal}(E'/\mathbb{F}(t))$ which satisfy for all $j \in \{1, \dots, n\}$, $U_j \cap \text{Gal}(E'/K_0) = \{1\}$, and $|U_j| = n$.

Proof. We set $H = G'$, $G' = \text{Gal}(E'/\mathbb{F}(t))$, and $G = \text{Gal}(E'/K_0)$.

We have seen from the proof of Claim 16 that $|H| = |G'| = n^2$. Since $H \cap G =$

G , and $|H \cap G| = [E' : K_0] = [E : \mathbb{F}(t)] = n$. So, by Lemma 4.2.11 again, there exist exactly n subgroups U_1, \dots, U_n of $G' = \text{Gal}(E'/\mathbb{F}(t))$ such that for all $j \in \{1, \dots, n\}$, $|U_j| = n$ and $U_j \cap G = \{1\}$. \square

Lemma 4.4.2. $\{V_1, \dots, V_m\} \subseteq \{U_1, \dots, U_n\}$, where for all $j \in \{1, \dots, m\}$, V_j is defined by Claim 17, and for all $j \in \{1, \dots, n\}$, U_j is defined by Claim 20.

Proof. Let $j \in \{1, \dots, m\}$. We have $(E')^{V_j} \subseteq E'$. Since $K_0 \subseteq E'$, $K_0(E')^{V_j} \subseteq E'$.

Claim 21: $[E' : K_0(E')^{V_j}] = 1$.

Proof of the Claim 21.

Proof. As $(E')^{V_j} \subseteq K_0(E')^{V_j} \subseteq E'$, then $[E' : K_0(E')^{V_j}] = \frac{[E' : (E')^{V_j}]}{[K_0(E')^{V_j} : (E')^{V_j}]}$.

On one hand, we have $E'/(E')^{V_j}$ is a Galois extension with $[E' : (E')^{V_j}] = |V_j| = n$.

On the other hand, as $V_j \subseteq \text{Gal}(E'/K)$, then any element of V_j fixes K .

But, from Lemma 4.4.1, we have $\mathbb{F}(t) \subseteq K$, then any element of V_j fixes $\mathbb{F}(t)$.

It follows that $\mathbb{F}(t) \subseteq (E')^{V_j}$. Hence $[K_0(E')^{V_j} : (E')^{V_j}] = [\mathbb{F}(t)(E')^{V_j} \mathbb{F}_n : (E')^{V_j} \mathbb{F}(t)]$, that is $[K_0(E')^{V_j} : (E')^{V_j}] = [\mathbb{F}(t) \mathbb{F}_n : \mathbb{F}(t) \mathbb{F}] = [\mathbb{F}_n : \mathbb{F}] = n$.

As $[E' : (E')^{V_j}] = |V_j| = n$, then $[E' : K_0(E')^{V_j}] = 1$. \square

From Claim 21, we deduce that $E' = K_0(E')^{V_j}$. By Galois theory, we have $V_j \cap \text{Gal}(E'/K_0) = \text{Gal}(E'/(E')^{V_j}) \cap \text{Gal}(E'/K_0) = \text{Gal}(E'/K_0(E')^{V_j}) = \{1\}$. Since V_j is a cyclic subgroup of $\text{Gal}(E'/K_0)$, $|V_j| = n$, and $V_j \cap \text{Gal}(E'/K_0) = \{1\}$, thus, from Lemma 4.2.11, $V_j = U_{i_j}$, for some $i_j \in \{1, \dots, n\}$. That implies that $\{V_1, \dots, V_m\} \subseteq \{U_1, \dots, U_n\}$. \square

Finally we arrive in the main result of this section.

Theorem 4.4.3. *There exists $c_2 > 0$ such that for any $r \in \mathbb{N} - \{0\}$, $N(K\mathbb{F}_r) \geq q^r + 1 - c_2 q^{r/2}$.*

Proof. For all $j \in \{1, \dots, n\}$, let us set $E_j = (E')^{U_j}$.

It is sufficient to show the result for the global function field K .

From Lemma 4.4.2 and Claim 20, we have for any $j \in \{1, \dots, m\}$, $(E')^{V_j} = (E')^{U_{i_j}}$ for some $i_j \in \{1, \dots, n\}$. Since E'/K is a Galois extension, by Proposition 4.3.4, (iii), we obtain

$$mN(K) = \sum_{j=1}^m N(E_{i_j}). \quad (4.4.1)$$

On the other hand, as $E/\mathbb{F}(t)$ is a Galois extension with $[E : \mathbb{F}(t)] = n$, and, from Claim 20, we have for any $j \in \{1, \dots, n\}$, $U_j \cap \text{Gal}(E'/K_0) = \{1\}$, and

$|U_j| = n$. So, by Proposition 4.3.4, (iii), we get

$$nN(\mathbb{F}(t)) = \sum_{l=1}^n N(E_l). \quad (4.4.2)$$

Let $j \in \{1, \dots, n\}$, we have, by Proposition 4.3.4, (ii), $g_{E_j} = g_E$. As q is a square and $q > (g_{E_j} + 1)^4$, then, from Theorem 4.2.7, we get

$$N(E_j) \leq q + 1 + (2g_E + 1)\sqrt{q}. \quad (4.4.3)$$

We also know from [1, Theorem 1.2.2], that $\{P_{t-\alpha} \in \mathcal{M}_{\mathbb{F}(t)} : \alpha \in \mathbb{F}\} \cup \{P_\infty\} = \{P \in \mathcal{M}_{\mathbb{F}(t)} : \deg_{\mathbb{F}(t)}(P) = 1\}$, then $N(\mathbb{F}(t)) = q + 1$.

It follows, from (4.4.1) and (4.4.2), that $mN(K) = n(q + 1) + \sum_{l=1}^m N(E_{i_l}) - \sum_{j=1}^n N(E_j)$. That is $mN(K) = n(q + 1) - \sum_{j=m+1}^n N(E_{i_j})$.

Therefore, from (4.4.3), we deduce that $mN(K) \geq n(q + 1) - (n - m)(q + 1 + (2g_E + 1)\sqrt{q})$. It implies that $N(K) \geq (q + 1) - \left(\frac{n - m}{m}\right)(2g_E + 1)\sqrt{q}$.

Setting $c_2 = \left(\frac{n - m}{m}\right)(2g_E + 1)$, then we get the result. \square

We now return to the proof of Theorem 4.1.1.

Proof. From Theorem 4.4.3, and Theorem 4.2.7, there exists $c = \max(2g_K + 1, c_2) > 0$, such that for any $r \in \mathbb{N} - \{0\}$,

$$|N_r - (q^r + 1)| \leq c\sqrt{q^r}.$$

Therefore, from Lemma 4.2.4, any reciprocal root α of L_K satisfies $|\alpha| = \sqrt{q}$. It follows that any non-trivial root of ζ_A has real part equal to $\frac{1}{2}$. \square

Bibliography

- [1] Stichtenoth, H.: *Algebraic Function Fields and Codes*. Springer, Berlin, 2008.
- [2] Rosen, M.: *Number Theory in Function Fields*. Springer, Berlin, 2002.
- [3] Janusz, G.: *Algebraic Number Fields*. Academic Press, New York, 1973.
- [4] Samuel-Zariski: *Commutative Algebra*. D. Van Nostrand Company, Toronto, 1958.
- [5] Sharma, J.N.: *Infinite Series and Products*. Krishna Prakashan Media, India, 1985.
- [6] Lang, S.: *Algebra*, vol. 211 of *Graduate Texts in Mathematics*. 3rd edn. Springer-Verlag, New York, 2002.