ASYMPTOTICS OF CLASS NUMBER AND GENUS FOR ABELIAN EXTENSIONS OF AN ALGEBRAIC FUNCTION FIELD

By

KENNETH WARD

Bachelor of Arts in Mathematics
University of Chicago
Chicago, Illinois, U.S.A.
2004

Master of Science in Pure Mathematics
Oklahoma State University
Stillwater, Oklahoma, U.S.A.
2009

Submitted to the Faculty of the
Graduate College of
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
DOCTOR OF PHILOSOPHY
May, 2012

ASYMPTOTICS OF CLASS NUMBER AND GENUS FOR ABELIAN EXTENSIONS OF AN ALGEBRAIC FUNCTION FIELD

Dissertation Approved:

David Wright

Dissertation Advisor

Amit Ghosh

Anthony Kable

Satyanarayan Nandi

Sheryl Tucker

Dean of the Graduate College

TABLE OF CONTENTS

Chapter	Page
1 INTRODUCTION	**1**
2 THE LOWER BOUND	**5**
3 THE UPPER BOUND	**11**
4 CONCLUSIONS	**30**
BIBLIOGRAPHY	**33**

CHAPTER 1

INTRODUCTION

The topic of this thesis lies at the intersection of algebraic geometry and number theory; what immediately follows is a brief summary of mathematical work in these subjects relevant to the proof of the main result of this thesis.

The first study on the genus of a surface is attributed to B. Riemann. In his 1857 work on abelian functions, he established what is known as Riemann's inequality: that, for any finite integral linear combination D of points on a Riemann surface $\mathcal{S}$, it holds that

$$l(-D) \geq \deg(D) - g_{\mathcal{S}} + 1;$$

with $l(-D)$ the dimension over the complex numbers $\mathbb{C}$ of the meromorphic functions of $\mathcal{S}$ of degree at least that of the coefficient of $-D$ at each point of $\mathcal{S}$, $\deg(D)$ the sum of the coefficients that appear in D, and $g_{\mathcal{S}}$ the non-negative integer known today as the genus of $\mathcal{S}$ [29]. Later, G. Roch is credited with establishment in 1865 of what is known as the Riemann-Roch theorem, which, with the previous notation, states that

$$l(-D) = \deg(D) - g_{\mathcal{S}} - 1 + l(D - \mathcal{W}),$$

with $\mathcal{W}$ a finite integral linear combination of points on $\mathcal{S}$ that is attached to a special type of function, called a differential of $\mathcal{S}$ [30].

In 1882, R. Dedekind and H. Weber developed the ideal theory on Riemann surfaces, which permitted a purely algebraic interpretation of the theorem of Riemann and Roch. In place of the meromorphic functions on a Riemann surface was a finite extension of the field $\mathbb{C}(X)$ of algebraic functions [8]. In 1936, H.K. Schmidt extended the Riemann-Roch theorem to an arbitrary field in place of $\mathbb{C}$ [33].

Zeta functions were essential to the early study of algebraic geometry and number theory. E. Artin is credited with the invention in 1921 of the zeta function of a curve over a finite field and, in certain cases, proof of what is called the "Riemann hypothesis" for curves over finite fields, which states that each zero of the zeta function of a curve over a finite field must have real part equal to one-half [1]. In 1934, H. Hasse established the Riemann hypothesis for curves over finite fields with genus equal to one [13]. A. Weil is credited with noting in 1940, and later proving, the validity of the Riemann hypothesis for all curves over finite fields [39, 40]. Based upon a method of S.A. Stepanov [35], a concise proof of Weil's claim was established by E. Bombieri in 1973 [4].

Part of the early development of modern number theory appears in class field theory, which has its roots in the theorem of L. Kronecker and H. Weber, first stated in 1853: that any abelian extension of the rational numbers is contained in a cyclotomic extension of the rational numbers [20]. The first proof of the Kronecker-Weber theorem is credited to D. Hilbert in 1897 [16]. In 1900, D. Hilbert published a list of 23 fundamental problems in mathematics, the ninth of which called for the establishment of a reciprocity law for number fields that would later become the foundation of class field theory [17]. The early developments of the reciprocity law, which applied to number fields, are credited to E. Artin [2], T. Takagi [36], and H. Hasse [12], in the years from 1920 to 1927. Later, between the years 1931 and 1935, the reciprocity law was developed for curves over finite fields by F.K. Schmidt [32], H. Hasse [14], and E. Witt [41].

Let us introduce some definitions and notation. Let $\mathbb{F}_q$ be a finite field. Let x be an element that is transcendental over $\mathbb{F}_q$. A finite extension of the field of rational functions $\mathbb{F}_q(x)$ is called a *congruence function field*. Let K denote a congruence function field. Let $\mathbb{F}_K$ denote the field of constants of K. Let g_K denote the genus of

K. Let h_K denote the class number of K.

This thesis is devoted to establishment of the following result. *Let F be a fixed choice of congruence function field. Let K be a finite abelian extension of F. It holds that*

$$\lim_{g_K \to \infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_K|} = 1.$$

The proof of this result is divided into three sections. In Chapter 2, a lower bound is established as Theorem 1:

Theorem 1. *Let K be a congruence function field. It holds that*

$$\liminf_{g_K \to \infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_K|} \geq 1.$$

The proof of Theorem 1 employs analytic methods to count divisors. In Chapter 3, an upper bound is established as Theorem 2:

Theorem 2. *Let F be a fixed choice of congruence function field. Let K be a finite abelian extension of F. It holds that*

$$\limsup_{g_K \to \infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_K|} \leq 1.$$

The proof of Theorem 2 employs properties of zeta functions in conjunction with ramification theory. In Chapter 4, the main result of this work is stated as a corollary of Theorems 1 and 2, and a simple example is provided that demonstrates why the arguments of Chapter 3 do not extend in general beyond the abelian case.

Work on this problem dates to a result of E. Inaba [18], which established, for a fixed choice of natural number m, that among congruence function fields K with a fixed choice of constant field $\mathbb{F}_q$ and an element x of K that satisfies $[K : \mathbb{F}_q(x)] \leq m$,

$$\lim_{g_K \to \infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_q|} = 1. \tag{1.1}$$

Furthermore, Inaba showed that among congruence fields K with a fixed choice of constant field $\mathbb{F}_q$,

$$\liminf_{g_K \to \infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_q|} \geq 1. \tag{1.2}$$

The work of Inaba depends upon an estimate for the number of integral divisors of degree equal to $2g_K$ and a bound for the value of the zeta function of K near one. M. Madan and D. Madden [24] extended the work of Inaba by proving, for congruence function fields K with a fixed choice of constant field $\mathbb{F}_q$ and an element x of K, that

$$\lim_{\frac{[K:\mathbb{F}_q(x)]}{g_K}\to 0} \frac{\ln h_K}{g_K \ln |\mathbb{F}_q|} = 1.$$

The result of Madan and Madden employs the basic mechanics of Inaba's proof. S. Gogia and I. Luthar [23] established a result similar to the equality (1.1) of Inaba. Also, using methods similar to those of Inaba, M. Tsfasman [37] independently established (1.2).

By use of an explicit formula for the genus obtained by D. Hayes [15], P. Lam-Estrada and G. D. Villa-Salvador [21] established that the cyclotomic extensions K of a fixed choice of rational congruence function field $\mathbb{F}_q(T)$ satisfy the relation

$$\lim_{g_K\to\infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_q|} = 1.$$

The work of Lam-Estrada and Villa-Salvador employed a lower bound for the degree of the different of a cyclotomic extension of a rational congruence function field. Each cyclotomic extension of $\mathbb{F}_q(T)$ is geometric, meaning that the field of constants of such an extension is equal to $\mathbb{F}_q$ [38].

By use of a result in class field theory that employs the idèlic topology [3], G. Frey, M. Perret, and H. Stichtenoth [10] obtained a lower bound for the degree of the different of a finite, geometric, and abelian extension of a congruence function field. As shown in the proof of Theorem 2, a much more simple proof is possible: one only needs the density theorem of Čebotarev for totally split places in a Galois extension of a congruence function field [38] and the result from global class field theory that the Artin map of a finite, unramified, and abelian extension of a congruence function field is trivial for principal divisors [19].

CHAPTER 2

THE LOWER BOUND

In this section is given the proof of Theorem 1. The proof proceeds as follows:

1. Count the number of monic and irreducible polynomials of a given degree with coefficients in a finite field via Möbius inversion [25];

2. Estimate the number of places of a given degree for a congruence function field via Möbius inversion and Riemann's hypothesis [4];

3. Obtain a lower bound for the number of integral divisors of degree $2g_K$ via the Riemann-Roch theorem [30].

Henceforth, let K be a congruence function field.

Lemma 1. *Let $x \in K \backslash \mathbb{F}_K$. For each $m \in \mathbb{N}$, let $\psi(m)$ be the number of monic irreducible elements of $\mathbb{F}_K[x]$ of degree in x equal to m. Let μ be the Möbius function [26]. It holds for each $m \in \mathbb{N}$ that*

$$\psi(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) |\mathbb{F}_K|^d .$$

Proof. Let $|\mathbb{F}_K| = q$. Let $m \in \mathbb{N}$. For each $f \in \mathbb{F}_K[x]$, let $d_x(f)$ denote the degree of f in x. One has the identity of polynomials

$$x^{q^m} - x = \prod_{d|m} \prod_{\substack{f \in \mathbb{F}_K[x] \\ f \text{ monic} \\ f \text{ irreducible} \\ d_x(f)=d}} f(x).$$

By equation of degrees in x, one obtains that

$$q^m = \sum_{d|m} d\psi(d).$$

By Möbius inversion [25], it follows that

$$\psi(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d.$$

□

Definition. Let $\mathbb{P}_K$ be the collection of places of K [38]. Let $\mathfrak{P} \in \mathbb{P}_K$ with associated valuation $v_{\mathfrak{P}}$, valuation ring $\vartheta_{\mathfrak{P}}$, and maximal ideal $\mathfrak{P}$. The *degree* of $\mathfrak{P}$ in K is defined as $d_K(\mathfrak{P}) = [\vartheta_{\mathfrak{P}}/\mathfrak{P} : \mathbb{F}_K]$.

Definition. Let $\mathfrak{A}$ be a divisor of K, written as

$$\mathfrak{A} = \prod_{\mathfrak{P}\in\mathbb{P}_K} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{A})}.$$

The *degree* in K of $\mathfrak{A}$ is defined as

$$d_K(\mathfrak{A}) = \sum_{\mathfrak{P}\in\mathbb{P}_K} v_{\mathfrak{P}}(\mathfrak{A}) d_K(\mathfrak{P}).$$

Definition. Let $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. For each non-negative integer n, let A_n denote the number of integral divisors of K of degree in K equal to n. The *zeta function* of K is defined as

$$\zeta_K(s) = \sum_{n=0}^{\infty} \frac{A_n}{|\mathbb{F}_K|^s}.$$

Lemma 2. *Let $x \in K \backslash \mathbb{F}_K$. Let $\mathbb{P}_0$ denote the collection of places of $\mathbb{F}_K(x)$; let d_0 denote the degree function for the divisors of $\mathbb{F}_K(x)$. For each $m \in \mathbb{N}$, let*

$$n_m = |\{\mathfrak{p} \in \mathbb{P}_0 \mid d_0(\mathfrak{p}) = m\}| \;\; \textit{and} \;\; N_m = |\{\mathfrak{P} \in \mathbb{P}_K \mid d_K(\mathfrak{P}) = m\}|.$$

It holds for each $m \in \mathbb{N}$ that $|N_m - n_m| \leq 4g_K|\mathbb{F}_K|^{\frac{m}{2}}$.

Proof. Let $|\mathbb{F}_K| = q$. Let $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. Let $u = q^{-s}$. One may write

$$\zeta_K(s) = \prod_{\mathfrak{P}\in\mathbb{P}_K} \left(1 - \frac{1}{q^{d_K(\mathfrak{P})s}}\right)^{-1} = \prod_{k=1}^{\infty} \left(1 - u^k\right)^{-N_k}.$$

Application of the logarithmic derivative yields

$$\frac{\zeta_K'(s)}{\zeta_K(s)} = \frac{d}{ds}\left(\ln \zeta_K(s)\right) = \frac{d}{ds}\left[\sum_{k=1}^{\infty} -N_k \left(\ln\left(1-u^k\right)\right)\right] = -\ln q \sum_{m=1}^{\infty}\left(\sum_{d|m} dN_d\right) u^m.$$

Let $\zeta_0(s)$ denote the zeta function of $\mathbb{F}_K(x)$. One has similarly

$$\frac{\zeta_0'(s)}{\zeta_0(s)} = -\ln q \sum_{m=1}^{\infty}\left(\sum_{d|m} dn_d\right) u^m.$$

Thus

$$\frac{\zeta_K'(s)}{\zeta_K(s)} - \frac{\zeta_0'(s)}{\zeta_0(s)} = -\ln q \sum_{m=1}^{\infty}\left(\sum_{d|m} d\left(N_d - n_d\right)\right) u^m.$$

Let $P_K(s) = (1-u)(1-qu)\zeta_K(s)$. It is well-known [9] that there exist $\omega_1, ..., \omega_{2g_K} \in \mathbb{C}$ with

$$P_K(s) = \prod_{i=1}^{2g_K}\left(1-\omega_i u\right).$$

Let $\mathfrak{p}_\infty \in \mathbb{P}_0$ be chosen with associated valuation $v_{\mathfrak{p}_\infty}$ defined for each $f, g \in \mathbb{F}_K[x]$ as

$$v_{\mathfrak{p}_\infty}\left(\frac{f}{g}\right) = d_x(g) - d_x(f).$$

One obtains that

$$\begin{aligned}\zeta_0(s) &= \prod_{\mathfrak{p}\in\mathbb{P}_0}\left(1-\frac{1}{q^{d_0(\mathfrak{p})s}}\right)^{-1} = \left(1-\frac{1}{q^{d_0(\mathfrak{p}_\infty)s}}\right)^{-1}\prod_{\substack{\mathfrak{p}\in\mathbb{P}_0\\ \mathfrak{p}\neq\mathfrak{p}_\infty}}\left(1-\frac{1}{q^{d_0(\mathfrak{p})s}}\right)^{-1}\\ &= \left(\frac{1}{1-u}\right)\left(\frac{1}{1-qu}\right).\end{aligned}$$

It follows that

$$P_K(s) = \frac{\zeta_K(s)}{\zeta_0(s)}.$$

Thus

$$\begin{aligned}\frac{\zeta_K'(s)}{\zeta_K(s)} - \frac{\zeta_0'(s)}{\zeta_0(s)} &= \frac{d}{ds}\left[\ln\left(\frac{\zeta_K(s)}{\zeta_0(s)}\right)\right] = \frac{d}{ds}\left[\ln\left(P_K(s)\right)\right] = \frac{d}{ds}\left[\sum_{i=1}^{2g_K}\ln\left(1-\omega_i u\right)\right]\\ &= \ln q\sum_{i=1}^{2g_K}\frac{\omega_i u}{1-\omega_i u} = \ln q\sum_{i=1}^{2g_K}\sum_{m=1}^{\infty}\omega_i^m u^m = \ln q\sum_{m=1}^{\infty}\left(\sum_{i=1}^{2g_K}\omega_i^m\right)u^m.\end{aligned}$$

Therefore

$$-\ln q \sum_{m=1}^{\infty}\left(\sum_{d|m} d\left(N_d-n_d\right)\right) u^m=\ln q \sum_{m=1}^{\infty}\left(\sum_{i=1}^{2g_K} \omega_i^m\right) u^m .$$

As this holds for all such s, it follows for each $m \in \mathbb{N}$ that

$$\sum_{d|m} d(N_d-n_d)=-\sum_{i=1}^{2g_K} \omega_i^m .$$

Let $m \in \mathbb{N}$. By Möbius inversion [25], it follows that

$$N_m-n_m=-\frac{1}{m} \sum_{d|m}\left[\mu\left(\frac{m}{d}\right) \sum_{i=1}^{2g_K} \omega_i^d\right] .$$

Thus

$$|N_m-n_m| \leq \frac{1}{m} \sum_{d|m}\left|\mu\left(\frac{m}{d}\right) \sum_{i=1}^{2g_K} \omega_i^d\right| \leq \frac{1}{m} \sum_{d|m} \sum_{i=1}^{2g_K}|\omega_i|^d \leq \frac{1}{m} \sum_{d=1}^{m} \sum_{i=1}^{2g_K}|\omega_i|^d .$$

By Riemann's hypothesis, it follows for each $i=1,...,2g_K$ that $|\omega_i|=q^{\frac{1}{2}}$ [4]. Therefore

$$\frac{1}{m} \sum_{d=1}^{m} \sum_{i=1}^{2g_K}|\omega_i|^d=\frac{1}{m} \sum_{d=1}^{m} \sum_{i=1}^{2g_K} q^{\frac{d}{2}}=\frac{2g_K q^{\frac{1}{2}}}{m}\left(\frac{q^{\frac{m}{2}}-1}{q^{\frac{1}{2}}-1}\right) \leq 4g_K q^{\frac{m}{2}} .$$

The result follows. □

Definition. Let C_K denote the group of divisor classes of K. Let $C \in C_K$. Let $\mathfrak{A} \in C$. Let $\mathfrak{A}_1,...,\mathfrak{A}_n$ be divisors that also lie in the class C. For each $i=1,...,n$, let $x_i \in K^*$ satisfy $(x_i)_K=\mathfrak{A}_i\mathfrak{A}^{-1}$. The divisors $\mathfrak{A}_1,...,\mathfrak{A}_n$ are called *linearly independent* if the elements $x_1,...,x_n$ are linearly independent over $\mathbb{F}_K$.

Definition. Let D_K denote the group of divisors of K. For each $\mathfrak{A} \in D_K$, let

$$L_K(\mathfrak{A})=\left\{x \in K \mid v_{\mathfrak{P}}(x) \geq v_{\mathfrak{P}}(\mathfrak{A}) \text{ for all } \mathfrak{P} \in \mathbb{P}_K\right\} .$$

Let $l_K(\mathfrak{A})=\dim_{\mathbb{F}_K} L_K(\mathfrak{A})$.

Lemma 3. *Let $C \in C_K$. Let $N_K(C)$ denote the maximal number of linearly independent integral divisors of C. Let $\mathfrak{A} \in C$. It holds that $N_K(C)=l_K(\mathfrak{A}^{-1})$.*

Proof. Let $\mathfrak{A}_1, ..., \mathfrak{A}_n \in C$ be linearly independent and integral. Let $\mathfrak{A} \in C$. For each $i = 1, ..., n$, let $\mathfrak{A}_i\mathfrak{A}^{-1} = (x_i)_K$. Thus the elements $x_1, ..., x_n$ are linearly independent over $\mathbb{F}_K$. As the divisor $\mathfrak{A}_i$ is integral for each $i = 1, ..., n$, it follows that the elements $x_1, ..., x_n$ lie in $L_K(\mathfrak{A}^{-1})$. Thus $n \le l_K(\mathfrak{A}^{-1})$.

Conversely, let $m = l_K(\mathfrak{A}^{-1})$. Let $y_1, ..., y_m$ be a basis of $L_K(\mathfrak{A}^{-1})$ over $\mathbb{F}_K$. Thus for each $i = 1, ..., m$ there exists an integral $\mathfrak{B}_i \in D_K$ with $(y_i)_K = \mathfrak{B}_i\mathfrak{A}^{-1}$. It follows that the divisors $\mathfrak{B}_1, ..., \mathfrak{B}_m$ lie in C and are linearly independent. □

Lemma 4. *Let $C \in C_K$. The number of integral divisors in C is equal to $\frac{|\mathbb{F}_K|^{N_K(C)}-1}{|\mathbb{F}_K|-1}$.*

Proof. Let $\mathfrak{A} \in C$. Let $\mathfrak{B} \in C$ be integral. As $\mathfrak{A}, \mathfrak{B} \in C$, it follows that $\mathfrak{B} = (\alpha)_K\mathfrak{A}$ for some $\alpha \in K^*$. As $\mathfrak{B}$ is integral, it follows that $\alpha \in L_K(\mathfrak{A}^{-1})$. Let $|\mathbb{F}_K| = q$. By the definition of $l_K(\mathfrak{A}^{-1})$, the number of non-zero elements of $L_K(\mathfrak{A}^{-1})$ is equal to $q^{l_K(\mathfrak{A}^{-1})} - 1$. Furthermore, two elements $\alpha, \beta \in K^*$ satisfy $(\alpha)_K = (\beta)_K$ if, and only if, $\alpha = a\beta$ for some $a \in \mathbb{F}_K^*$. It follows that the number of integral divisors in C is equal to $\frac{q^{l_K(\mathfrak{A}^{-1})}-1}{q-1}$. By Lemma 3, the result follows. □

Theorem 1. *Let K be a congruence function field. It holds that*

$$\liminf_{g_K\to\infty} \frac{\ln h_K}{g_K \ln|\mathbb{F}_K|} \ge 1.$$

Proof. Let $|\mathbb{F}_K| = q$. Let $C \in C_K$. Let W_K denote the canonical class. By the Riemann-Roch theorem [30], it holds that

$$N_K(C) = d_K(C) - g_K + 1 + N_K(W_KC^{-1}).$$

Suppose that $d_K(C) = 2g_K$. Once again by the Riemann-Roch theorem, it holds that

$$d_K(CW_K^{-1}) = d_K(C) - d_K(W_K) = 2g_K - (2g_K - 2) = 2.$$

Let $\mathfrak{A} \in C$. Let ω be a non-zero Weil differential of K. Let $(\omega)_K$ be the divisor associated with ω. Each principal divisor of K is of degree zero [9]. By Lemma 3, it follows that

$$N_K(W_KC^{-1}) = l_K(\mathfrak{A}(\omega)_K^{-1}) = \dim_{\mathbb{F}_K} L_K(\mathfrak{A}(\omega)_K^{-1}) = \dim_{\mathbb{F}_K}\{0\} = 0.$$

Thus

$$d_K(C) - g_K + 1 + N_K(W_K C^{-1}) = d_K(C) - g_K + 1 + 0 = 2g_K - g_K + 1 = g_K + 1.$$

By Lemma 4, the number of integral divisors in C is equal to $\frac{q^{N_K(C)}-1}{q-1}$. Thus the number of integral divisors of K of degree in K equal to $2g_K$ is equal to $h_K\left(\frac{q^{g_K+1}-1}{q-1}\right)$.

The place $\mathfrak{p}_\infty$ is the only place of $\mathbb{F}_K(x)$ that is not associated with a valuation determined by degree in an irreducible element of $\mathbb{F}_K[x]$. As $d_0(\mathfrak{p}_\infty) = 1$, it follows for each integer $m > 2$ that $n_m = \psi(m)$. It may be assumed that $g_K \geq 1$. Thus $n_{2g_K} = \psi(2g_K)$. By Lemmas 1 and 2, it follows that

$$\begin{aligned}
h_K\left(\frac{q^{g_K+1}-1}{q-1}\right) &\geq N_{2g_K} \geq n_{2g_K} - 4g_K q^{g_K} = \psi(2g_K) - 4g_K q^{g_K} \\
&\geq \frac{q^{2g_K}}{2g_K} - \left|\frac{1}{2g_K}\sum_{\substack{d|2g_K \\ d<2g_K}} \mu\left(\frac{2g_K}{d}\right) q^d\right| - 4g_K q^{g_K} \\
&\geq \frac{q^{2g_K}}{2g_K} - \sum_{\substack{d|2g_K \\ d<2g_K}} q^d - 4g_K q^{g_K} \\
&\geq \frac{q^{2g_K}}{2g_K} - \sum_{d=1}^{g_K} q^d - 4g_K q^{g_K} \\
&\geq \frac{q^{2g_K}}{2g_K} - (4g_K + 2)q^{g_K}.
\end{aligned}$$

Thus

$$h_K \geq \left(\frac{q-1}{q^{g_K+1}-1}\right)\left(\frac{q^{2g_K}}{2g_K} - (4g_K+2)q^{g_K}\right).$$

By basic calculus, if g_K is large enough it holds for any prime power q that

$$h_K \geq \frac{(q-1)q^{g_K-1}}{4g_K}.$$

As $g_K \geq 1$ and $q \geq 2$, it follows that

$$\begin{aligned}
\frac{\ln h_K}{g_K \ln q} &\geq \frac{\ln(q-1)}{g_K \ln q} + 1 - \frac{1}{g_K} - \frac{\ln 4g_K}{g_K \ln q} \geq \frac{\ln q - 1}{g_K \ln q} + 1 - \frac{1}{g_K} - \frac{\ln 4g_K}{g_K \ln q} \\
&= 1 - \frac{1 + \ln 4g_K}{g_K \ln q} \geq 1 - \frac{1 + \ln 4g_K}{g_K \ln 2}.
\end{aligned}$$

□

CHAPTER 3

THE UPPER BOUND

In this section is given the proof of Theorem 2. The proof proceeds as follows:

1. Establish the upper bound of Theorem 2 for those congruence function fields with a condition on the growth of the genus via ramification theory [38] and Riemann's inequality [29];

2. Obtain an upper bound for the degree of a finite, abelian, geometric, and unramified extension of a congruence function field via ramification theory [38], Čebotarev's density theorem [38] and global class field theory [19];

3. Obtain a lower bound for the degree of the different of a finite and abelian extension of a congruence function field via higher ramification theory [38] and the Hasse-Arf theorem [28];

4. Derive a contradiction for a sequence that violates the statement of Theorem 2 via the Riemann-Roch theorem [30], Riemann's hypothesis [4], and the Riemann-Hurwitz formula [38].

Definition. Let F be a congruence function field. Let $\mathfrak{p} \in \mathbb{P}_F$. Let K be a finite extension of F. Let $\{K|\mathfrak{p}\}$ denote the collection of places of K that lie above $\mathfrak{p}$. Let $n(K|\mathfrak{p}) = |\{K|\mathfrak{p}\}|$.

Henceforth, let F be a congruence function field, and let K be a finite extension of F.

Definition. The *ramification index* of $\mathfrak{P}|\mathfrak{p}$ is defined as $e(\mathfrak{P}|\mathfrak{p}) = |v_{\mathfrak{P}}(K^*)/v_{\mathfrak{P}}(F^*)|$. The *relative degree* of $\mathfrak{P}|\mathfrak{p}$ is defined as $f(\mathfrak{P}|\mathfrak{p}) = [\vartheta_{\mathfrak{P}}/\mathfrak{P} : \vartheta_{\mathfrak{p}}/\mathfrak{p}]$.

Henceforth, unless otherwise noted, let $\mathfrak{p} \in \mathbb{P}_F$, and $\mathfrak{P} \in \{K|\mathfrak{p}\}$.

Lemma 5. *It holds that $n(K|\mathfrak{p}) \leq [K : F]$.*

Proof. By Riemann's inequality [29], one has that

$$l_F(\mathfrak{p}^{-(g_F+1)}) \geq d_F(\mathfrak{p}^{g_F+1}) - g_F + 1 = (g_F+1)d_F(\mathfrak{p}) - g_F + 1 \geq g_F + 1 - g_F + 1 = 2.$$

By Lemma 3, there exists $\alpha \in F\backslash\mathbb{F}_F$ and an integral $\mathfrak{A} \in D_F$ with $(\alpha)_F = \mathfrak{p}^{g_F+1}\mathfrak{A}^{-1}$ and $\mathfrak{A}$ relatively prime to $\mathfrak{p}$. Let $\mathfrak{B} \in D_K$ be integral with $(\alpha)_K = \mathfrak{P}_1^{a_1}\cdots\mathfrak{P}_r^{a_r}\mathfrak{B}^{-1}$, each of $a_1, ..., a_r$ positive, and $\mathfrak{B}$ relatively prime to each of $\mathfrak{P}_1, ..., \mathfrak{P}_r$. For $\mathfrak{P} \in \{K|\mathfrak{p}\}$, one has that $v_{\mathfrak{p}}(\alpha) > 0$ if, and only if, $v_{\mathfrak{P}}(\alpha) > 0$. It follows that $\{\mathfrak{P}_1, ..., \mathfrak{P}_r\} = \{K|\mathfrak{p}\}$ and $r = n(K|\mathfrak{p})$. Also, one has for each $i = 1, ..., n(K|\mathfrak{p})$ that $a_i = (g_F+1)e(\mathfrak{P}_i|\mathfrak{p})$. By basic function field theory [9], this yields that

$$\begin{aligned}[K : \mathbb{F}_K(\alpha)] &= d_K(\mathfrak{P}_1^{a_1}\cdots\mathfrak{P}_{n(K|\mathfrak{p})}^{a_{n(K|\mathfrak{p})}}) = \sum_{i=1}^{n(K|\mathfrak{p})} a_i d_K(\mathfrak{P}_i)\\ &= (g_F+1)\sum_{i=1}^{n(K|\mathfrak{p})} e(\mathfrak{P}_i|\mathfrak{p})d_K(\mathfrak{P}_i) = (g_F+1)\sum_{i=1}^{n(K|\mathfrak{p})} e(\mathfrak{P}_i|\mathfrak{p})\frac{f(\mathfrak{P}_i|\mathfrak{p})d_F(\mathfrak{p})}{[\mathbb{F}_K : \mathbb{F}_F]}\\ &= \frac{(g_F+1)d_F(\mathfrak{p})}{[\mathbb{F}_K : \mathbb{F}_F]}\sum_{i=1}^{n(K|\mathfrak{p})} e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p}).\end{aligned}$$

Likewise, one obtains that $[F : \mathbb{F}_F(\alpha)] = d_F(\mathfrak{p}^{g_F+1}) = (g_F+1)d_F(\mathfrak{p})$, Thus

$$\begin{aligned}(g_F+1)d_F(\mathfrak{p})\sum_{i=1}^{n(K|\mathfrak{p})} e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p}) &= [K : \mathbb{F}_K(\alpha)][\mathbb{F}_K : \mathbb{F}_F]\\ &= [K : \mathbb{F}_K(\alpha)][\mathbb{F}_K(\alpha) : \mathbb{F}_F(\alpha)] = [K : \mathbb{F}_F(\alpha)]\\ &= [K : F][F : \mathbb{F}_F(\alpha)] = [K : F](g_F+1)d_F(\mathfrak{p}).\end{aligned}$$

Therefore

$$\sum_{i=1}^{n(K|\mathfrak{p})} e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p}) = [K : F].$$

In particular, it follows that $n(K|\mathfrak{p}) \leq [K : F]$. □

Lemma 6. *Let $x \in K \backslash \mathbb{F}_K$. It holds that*

$$\limsup_{\frac{[K:\mathbb{F}_K(x)]}{g_K} \to 0} \frac{\ln h_K}{g_K \ln |\mathbb{F}_K|} \leq 1.$$

Proof. Let $|\mathbb{F}_K| = q$. Let $C \in C_K$. By Riemann's inequality [29], one obtains that

$$N_K(C) \geq d_K(C) - g_K + 1.$$

Suppose that $d_K(C) = n \geq 0$. Thus

$$\frac{q^{N_K(C)} - 1}{q-1} \geq \frac{q^{d_K(C) - g_K + 1} - 1}{q-1} = \frac{q^{n-g_K+1} - 1}{q-1}.$$

By Lemma 4,

$$A_n \geq h_K \frac{q^{n-g_K+1} - 1}{q-1}.$$

Let $s \in \mathbb{R}$ with $s > 1$. One has

$$\begin{aligned}
\zeta_K(s) &= \sum_{n=0}^{\infty} \frac{A_n}{q^{ns}} \geq \sum_{n=g_K}^{\infty} \frac{A_n}{q^{ns}} \geq \sum_{n=g_K}^{\infty} h_K \frac{q^{n-g_K+1} - 1}{q-1} \frac{1}{q^{ns}} \\
&= \frac{h_K}{q^{g_K s}} \sum_{n=g_K}^{\infty} \frac{q^{n-g_K+1} - 1}{q-1} \frac{1}{q^{(n-g_K)s}} = \frac{h_K}{q^{g_K s}} \sum_{n=0}^{\infty} \frac{q^{n+1} - 1}{q-1} \frac{1}{q^{ns}} = \frac{h_K}{q^{g_K s}} \zeta_0(s).
\end{aligned}$$

Let $\mathfrak{p}$ be a place of $\mathbb{F}_K(x)$. Let $\mathfrak{P} \in \{K|\mathfrak{p}\}$. The relative degree $f(\mathfrak{P}|\mathfrak{p})$ satisfies $d_K(\mathfrak{P}) = f(\mathfrak{P}|\mathfrak{p}) d_0(\mathfrak{p})$. Thus

$$1 - \frac{1}{q^{d_K(\mathfrak{P})s}} = 1 - \frac{1}{q^{f(\mathfrak{P}|\mathfrak{p}) d_0(\mathfrak{p}) s}} \geq 1 - \frac{1}{q^{d_0(\mathfrak{p})s}}.$$

By Lemma 5, the set $\{K|\mathfrak{p}\}$ is finite. Let $\{K|\mathfrak{p}\} = \{\mathfrak{P}_1, ..., \mathfrak{P}_{n(K|\mathfrak{p})}\}$. Also by Lemma 5, it holds that $n(K|\mathfrak{p}) \leq [K : \mathbb{F}_K(x)]$. This yields that

$$\begin{aligned}
\prod_{i=1}^{n(K|\mathfrak{p})} \left(1 - \frac{1}{q^{d_K(\mathfrak{P}_i)s}}\right) &= \prod_{i=1}^{n(K|\mathfrak{p})} \left(1 - \frac{1}{q^{f(\mathfrak{P}_i|\mathfrak{p}) d_0(\mathfrak{p}) s}}\right) \geq \left(1 - \frac{1}{q^{d_0(\mathfrak{p})s}}\right)^{n(K|\mathfrak{p})} \\
&\geq \left(1 - \frac{1}{q^{d_0(\mathfrak{p})s}}\right)^{[K:\mathbb{F}_K(x)]}.
\end{aligned}$$

Therefore

$$\zeta_K(s) = \prod_{\mathfrak{P} \in \mathbb{P}_K} \left(1 - \frac{1}{q^{d_K(\mathfrak{P})s}}\right)^{-1} \leq \prod_{\mathfrak{p} \in \mathbb{P}_0} \left(1 - \frac{1}{q^{d_0(\mathfrak{p})s}}\right)^{-[K:\mathbb{F}_K(x)]} = \zeta_0(s)^{[K:\mathbb{F}_K(x)]}.$$

It follows that

$$\frac{h_K}{q^{g_K s}}\zeta_0(s) \le \zeta_K(s) \le \zeta_0(s)^{[K:\mathbb{F}_K(x)]}.$$

In particular, one has that $\frac{h_K}{q^{g_K s}} \le \zeta_0(s)^{[K:\mathbb{F}_K(x)]-1}$. Application of the logarithm yields that

$$\ln h_K - g_K s \ln q \le ([K:\mathbb{F}_K(x)]-1)\ln \zeta_0(s).$$

Also, let T be transcendental over $\mathbb{F}_2$. As $s > 1$ and $q \ge 2$, it holds that

$$\zeta_0(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})} \le \frac{1}{(1-2^{-s})(1-2^{1-s})} = \zeta_{\mathbb{F}_2(T)}(s).$$

As $q \ge 2$, it follows that

$$\frac{\ln h_K}{g_K \ln q} \le s + \frac{([K:\mathbb{F}_K(x)]-1)\ln \zeta_0(s)}{g_K \ln q} \le s + \frac{([K:\mathbb{F}_K(x)]-1)\ln \zeta_{\mathbb{F}_2(T)}(s)}{g_K \ln 2}.$$

Let $\varepsilon \in \mathbb{R}$ with $\varepsilon > 0$. Let $s = 1 + \frac{\varepsilon}{2}$. Let the quantity $\frac{[K:\mathbb{F}_K(x)]}{g_K}$ be chosen small enough that

$$\frac{([K:\mathbb{F}_K(x)]-1)\ln \zeta_{\mathbb{F}_2(T)}(s)}{g_K \ln 2} < \frac{\varepsilon}{2}.$$

Therefore

$$\frac{\ln h_K}{g_K \ln q} \le 1 + \frac{\varepsilon}{2} + \frac{([K:\mathbb{F}_K(x)]-1)\ln \zeta_{\mathbb{F}_2(T)}(s)}{g_K \ln 2} < 1 + \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = 1 + \varepsilon.$$

□

Henceforth, let K be a finite and Galois extension of F.

Definition. Let $\sigma \in \mathrm{Gal}(K|F)$. Let $\sigma(\mathfrak{P}) \in \mathbb{P}_K$ be defined, for each $\alpha \in K$, as $v_{\sigma(\mathfrak{P})}(\alpha) = v_{\mathfrak{P}}(\sigma^{-1}(\alpha))$.

Lemma 7. *Each of the quantities $e(\mathfrak{P}|\mathfrak{p})$ and $f(\mathfrak{P}|\mathfrak{p})$ is independent of the choice of $\mathfrak{P} \in \{K|\mathfrak{p}\}$.*

Proof. Let $\mathfrak{P}' \in \{K|\mathfrak{p}\}$. Suppose that $\sigma(\mathfrak{P}) \ne \mathfrak{P}'$ for all $\sigma \in \mathrm{Gal}(K|F)$. By Artin's approximation theorem [28], there exists $\alpha \in K$ with $v_{\mathfrak{P}'}(\alpha) > 0$ and, for each

$\sigma \in \mathrm{Gal}(K|F)$, $v_{\mathfrak{P}'}(\sigma(\alpha)) \geq 0$ and $v_{\mathfrak{P}}(\sigma(\alpha)) = 0$. Thus

$$v_{\mathfrak{p}}(N_{K|F}\alpha) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{P}}(N_{K|F}\alpha) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{P}}\left(\prod_{\sigma\in\mathrm{Gal}(K|F)} \sigma(\alpha)\right)$$
$$= e(\mathfrak{P}|\mathfrak{p}) \sum_{\sigma\in\mathrm{Gal}(K|F)} v_{\mathfrak{P}}(\sigma(\alpha)) = 0.$$

Also,

$$v_{\mathfrak{p}}(N_{K|F}\alpha) = e(\mathfrak{P}'|\mathfrak{p})v_{\mathfrak{P}'}(N_{K|F}\alpha) = e(\mathfrak{P}'|\mathfrak{p})v_{\mathfrak{P}'}\left(\prod_{\sigma\in\mathrm{Gal}(K|F)} \sigma(\alpha)\right)$$
$$= e(\mathfrak{P}'|\mathfrak{p}) \sum_{\sigma\in\mathrm{Gal}(K|F)} v_{\mathfrak{P}'}(\sigma(\alpha)) \geq e(\mathfrak{P}'|\mathfrak{p})v_{\mathfrak{P}'}(\alpha) > 0.$$

This is a contradiction. Thus there exists $\sigma \in \mathrm{Gal}(K|F)$ with $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Let $\alpha \in F^*$ with $v_{\mathfrak{p}}(\alpha) \neq 0$. Thus

$$e(\mathfrak{P}'|\mathfrak{p})v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{P}'}(\alpha) = v_{\sigma(\mathfrak{P})}(\alpha) = v_{\mathfrak{P}}(\sigma^{-1}(\alpha)) = v_{\mathfrak{P}}(\alpha) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(\alpha).$$

It follows that $e(\mathfrak{P}'|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p})$. Furthermore, as $\sigma(\mathfrak{P}) = \mathfrak{P}'$, it holds that $\sigma(\vartheta_{\mathfrak{P}}) = \vartheta_{\mathfrak{P}'}$. Thus σ induces an isomorphism of $\vartheta_{\mathfrak{P}}/\mathfrak{P}$ with $\vartheta_{\mathfrak{P}'}/\mathfrak{P}'$ over $\vartheta_{\mathfrak{p}}/\mathfrak{p}$. Therefore

$$f(\mathfrak{P}|\mathfrak{p}) = [\vartheta_{\mathfrak{P}}/\mathfrak{P} : \vartheta_{\mathfrak{p}}/\mathfrak{p}] = [\vartheta_{\mathfrak{P}'}/\mathfrak{P}' : \vartheta_{\mathfrak{p}}/\mathfrak{p}] = f(\mathfrak{P}'|\mathfrak{p}).$$

□

Lemma 8. *It holds that* $[K : F] = n(K|\mathfrak{p})e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$.

Proof. By Lemma 5, the set $\{K|\mathfrak{p}\}$ is finite. Let $\{K|\mathfrak{p}\} = \{\mathfrak{P}_1, ..., \mathfrak{P}_{n(K|\mathfrak{p})}\}$. By Lemma 7, it holds for each $i = 1, ..., n(K|\mathfrak{p})$ that $e(\mathfrak{P}_i|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p})$ and $f(\mathfrak{P}_i|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p})$. By the proof of Lemma 5, it follows that

$$[K : F] = \sum_{i=1}^{n(K|\mathfrak{p})} e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p}) = n(K|\mathfrak{p})e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p}).$$

□

Definition. The *decomposition group* of $\mathfrak{P}|\mathfrak{p}$ is defined as

$$D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K|F) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Lemma 9. *It holds that* $|D(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$.

Proof. The group $D(\mathfrak{P}|\mathfrak{p})$ is by definition the stabiliser of $\mathfrak{P}$ for the action of $\mathrm{Gal}(K|F)$ on $\{K|\mathfrak{p}\}$. By the proof of Lemma 7, $\mathrm{Gal}(K|F)$ acts transitively on $\{K|\mathfrak{p}\}$. Thus

$$|D(\mathfrak{P}|\mathfrak{p})| = \frac{[K:F]}{n(K|\mathfrak{p})}.$$

By Lemma 8, the result follows. □

Definition. The *inertia group* of $\mathfrak{P}|\mathfrak{p}$ is defined as

$$I(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K|F) \mid \text{for each } \alpha \in K,\ \sigma(\alpha) = \alpha \bmod \mathfrak{P}\}.$$

Lemma 10. *It holds that* $|I(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})$.

Proof. For $\alpha \in \vartheta_{\mathfrak{P}}$, let $\overline{\alpha} := \alpha \bmod \mathfrak{P}$. The field $\vartheta_{\mathfrak{P}}/\mathfrak{P}$ is a finite and Galois extension of $\vartheta_{\mathfrak{p}}/\mathfrak{p}$ [7]. In particular, there exists $\alpha \in \vartheta_{\mathfrak{P}}$ with $\vartheta_{\mathfrak{P}}/\mathfrak{P} = \vartheta_{\mathfrak{p}}/\mathfrak{p}(\overline{\alpha})$. An element of $\mathrm{Gal}(\vartheta_{\mathfrak{P}}/\mathfrak{P}|\vartheta_{\mathfrak{p}}/\mathfrak{p})$ is completely determined by its action on $\overline{\alpha}$. By Artin's approximation theorem [28], there exists $\alpha' \in K$ so that $v_{\mathfrak{P}}(\alpha' - \alpha) > 0$ and, for each $\mathfrak{P}' \in \{K|\mathfrak{p}\}$ with $\mathfrak{P}' \neq \mathfrak{P}$, $v_{\mathfrak{P}'}(\alpha') > 0$. In particular, it follows that $\alpha' \in \vartheta_{\mathfrak{P}}$ and $\overline{\alpha'} = \overline{\alpha}$. Let

$$f(T) = \prod_{\sigma \in \mathrm{Gal}(K|F)} (T - \sigma(\alpha')).$$

By the definition of α', it follows that $f(T) \in \vartheta_{\mathfrak{p}}[T]$. Furthermore, if an element $\sigma \in \mathrm{Gal}(K|F)$ is not contained in $D(\mathfrak{P}|\mathfrak{p})$, it follows that $\sigma^{-1}(\mathfrak{P}) \neq \mathfrak{P}$. Also by the definition of α', it holds for such σ that $v_{\mathfrak{P}}(\sigma(\alpha')) = v_{\sigma^{-1}(\mathfrak{P})}(\alpha') > 0$. Let $\overline{f}(T) := f(T) \bmod \mathfrak{p}$. It follows for some non-negative integer n that

$$\overline{f}(T) = T^n \prod_{\sigma \in D(\mathfrak{P}|\mathfrak{p})} (T - \overline{\sigma(\alpha')}).$$

Let $\phi : D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(\vartheta_{\mathfrak{P}}/\mathfrak{P}|\vartheta_{\mathfrak{p}}/\mathfrak{p})$ be defined for each $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ and $\beta \in \vartheta_{\mathfrak{P}}$ as $\overline{\sigma}(\beta) = \overline{\sigma(\beta)}$. By the previous argument, each Galois conjugate of $\overline{\alpha'}$ over $\vartheta_{\mathfrak{p}}/\mathfrak{p}$ is of the form $\overline{\sigma(\alpha')}$ for some $\sigma \in D(\mathfrak{P}|\mathfrak{p})$. Thus ϕ is surjective. Also, by the definition of $I(\mathfrak{P}|\mathfrak{p})$, one obtains that the kernel of ϕ is equal to $I(\mathfrak{P}|\mathfrak{p})$. By Lemma 9, it follows that

$$\begin{aligned}|I(\mathfrak{P}|\mathfrak{p})| &= \frac{|D(\mathfrak{P}|\mathfrak{p})|}{|\mathrm{Gal}(\vartheta_{\mathfrak{P}}/\mathfrak{P}|\vartheta_{\mathfrak{p}}/\mathfrak{p})|} = \frac{e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})}{|\mathrm{Gal}(\vartheta_{\mathfrak{P}}/\mathfrak{P}|\vartheta_{\mathfrak{p}}/\mathfrak{p})|} = \frac{e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})}{[\vartheta_{\mathfrak{P}}/\mathfrak{P} : \vartheta_{\mathfrak{p}}/\mathfrak{p}]} \\ &= \frac{e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})}{f(\mathfrak{P}|\mathfrak{p})} = e(\mathfrak{P}|\mathfrak{p}).\end{aligned}$$

□

Lemma 11. *Let $\mathbb{E}$ be a finite field that contains $\mathbb{F}_F$. It holds that*

$$n(\mathbb{E}F|\mathfrak{p}) = ([\mathbb{E} : \mathbb{F}_F], d_F(\mathfrak{p})).$$

Proof. Let $\mathfrak{P} \in \mathbb{P}_{\mathbb{E}F}$ with $\mathfrak{P}|\mathfrak{p}$. As $\vartheta_{\mathfrak{p}}/\mathfrak{p} \subset \vartheta_{\mathfrak{P}}/\mathfrak{P}$ and $\mathbb{E} \subset \vartheta_{\mathfrak{P}}/\mathfrak{P}$, it follows that $(\vartheta_{\mathfrak{p}}/\mathfrak{p})\mathbb{E} \subset \vartheta_{\mathfrak{P}}/\mathfrak{P}$.

For the converse, let $y \in \vartheta_{\mathfrak{P}}$. By Artin's approximation theorem [28], there exists $y' \in \mathbb{E}F$ with $v_{\mathfrak{P}}(y' - y) > 0$ and, for each $\mathfrak{P}' \in \{\mathbb{E}F|\mathfrak{p}\}$ with $\mathfrak{P}' \neq \mathfrak{P}$, $v_{\mathfrak{P}'}(y') \geq 0$. Let $\xi \in \mathbb{E}$ with $\mathbb{E} = \mathbb{F}_F(\xi)$. Let $m = [\mathbb{E} : \mathbb{F}_F]$. One may write

$$y' = \sum_{i=0}^{m} a_i \xi^i$$

with $a_1, ..., a_m \in F$. Also, $\mathbb{E}F$ is a finite and Galois extension of F [7]. Let $y'^{(1)} = y', y'^{(2)}, ..., y'^{(m)}$ be the Galois conjugates of y' over F. By Cramer's rule [22], it follows for each $i = 1, ..., m$ that

$$a_i = \sum_{j=1}^{m} t_{i,j} y'^{(j)}$$

with $t_{i,1}, ..., t_{i,m} \in \mathbb{E}$. Let $\sigma \in I(\mathfrak{P}|\mathfrak{p})$. By the definition of $I(\mathfrak{P}|\mathfrak{p})$, it holds that $v_{\mathfrak{P}}(\sigma(\xi) - \xi) > 0$. As $\xi \in \mathbb{E}$ and $v_{\mathfrak{P}}$ is trivial on $\mathbb{E}$, it follows that $\sigma(\xi) = \xi$. By Lemma 10, this yields that $e(\mathfrak{P}|\mathfrak{p}) = |I(\mathfrak{P}|\mathfrak{p})| = 1$. Furthermore, by the definition of y', it follows for each $j = 1, ..., m$ that $y'^{(j)} \in \vartheta_{\mathfrak{P}}$. Thus one obtains for each $i = 1, ..., m$ that

$$v_{\mathfrak{p}}(a_i) = v_{\mathfrak{P}}(a_i) = v_{\mathfrak{P}}\left(\sum_{j=1}^{n} t_{i,j} y'^{(j)}\right) \geq \min_{1 \leq j \leq n} \{v_{\mathfrak{P}}(y'^{(j)})\} \geq 0.$$

Therefore $\vartheta_{\mathfrak{P}}/\mathfrak{P} = (\vartheta_{\mathfrak{p}}/\mathfrak{p})\mathbb{E}$. Let $q = |\mathbb{F}_F|$. Let $r = d_F(\mathfrak{p})$, $s = d_{\mathbb{E}F}(\mathfrak{P})$, and $t = f(\mathfrak{P}|\mathfrak{p})$. Thus $\mathbb{F}_{q^{sn}} = \mathbb{F}_{q^r}\mathbb{F}_{q^n} = \mathbb{F}_{q^{[r,n]}}$. Therefore $d_{\mathbb{E}F}(\mathfrak{P})[\mathbb{E} : \mathbb{F}_F] = [d_F(\mathfrak{p}), [\mathbb{E} : \mathbb{F}_F]]$. As $\mathbb{E}F$ is a finite and Galois extension of F, it follows by Lemma 8 that

$$n(\mathbb{E}F|\mathfrak{p}) = \frac{[\mathbb{E}F : F]}{e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})} = \frac{[\mathbb{E} : \mathbb{F}_F]}{e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})} = \frac{[\mathbb{E} : \mathbb{F}_F]}{f(\mathfrak{P}|\mathfrak{p})} = \frac{d_F(\mathfrak{p})}{d_{\mathbb{E}F}(\mathfrak{P})} = (d_F(\mathfrak{p}), [\mathbb{E} : \mathbb{F}_F]).$$

□

Definition. The place $\mathfrak{p}$ is said to *split totally* in K if $e(\mathfrak{P}|\mathfrak{p}) = 1$ and $f(\mathfrak{P}|\mathfrak{p}) = 1$. The collection of places of F that split totally in K is denoted by $\mathcal{S}(K|F)$.

Definition. K is called a *geometric* extension of F if $\mathbb{F}_K = \mathbb{F}_F$.

Lemma 12. *Let H be a finite, Galois, and geometric extension of F. Let $\mathfrak{d}(H|F) = \gcd\{d_F(\mathfrak{p}) \mid \mathfrak{p} \in \mathcal{S}(H|F)\}$. It holds that $\mathfrak{d}(H|F) = 1$.*

Proof. Let $\mathbb{E}$ be the extension of $\mathbb{F}_F$ that satisfies $[\mathbb{E} : \mathbb{F}_F] = \mathfrak{d}(H|F)$. Let $\mathfrak{p} \in \mathcal{S}(H|F)$. By the definition of $\mathfrak{d}(H|F)$, it follows that $[\mathbb{E} : \mathbb{F}_F] \mid d_F(\mathfrak{p})$. Let $\mathfrak{P} \in \{\mathbb{E}F|\mathfrak{p}\}$. By Lemma 11, one obtains that

$$n(\mathbb{E}F|\mathfrak{p}) = ([\mathbb{E} : \mathbb{F}_F], d_F(\mathfrak{p})) = [\mathbb{E} : \mathbb{F}_F].$$

The field $\mathbb{E}F$ is a finite and Galois extension of F [7]. By Lemma 8, it holds that

$$n(\mathbb{E}F|\mathfrak{p}) = \frac{[\mathbb{E}F : F]}{e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})}$$

As $[\mathbb{E}F : F] = [\mathbb{E} : \mathbb{F}_F]$, it follows that $\mathfrak{p} \in \mathcal{S}(\mathbb{E}F|F)$.

Let $\mathfrak{Q} \in \{\mathbb{E}H|\mathfrak{P}\}$. Let $\mathfrak{R} \in \mathbb{P}_H$ so that $\mathfrak{Q} \in \{\mathbb{E}H|\mathfrak{R}\}$. As each of $\mathbb{E}F$ and H is a finite and Galois extension of F, it follows by basic Galois theory that $\mathbb{E}H$ is a finite and Galois extension of F, and that the decomposition group $D(\mathfrak{Q}|\mathfrak{p})$ restricts injectively onto the product of $D(\mathfrak{P}|\mathfrak{p})$ with $D(\mathfrak{R}|\mathfrak{p})$ [7]. By Lemma 9, it holds that $|D(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$ and $|D(\mathfrak{R}|\mathfrak{p})| = e(\mathfrak{R}|\mathfrak{p})f(\mathfrak{R}|\mathfrak{p})$. As $\mathfrak{p}$ lies in both $\mathcal{S}(H|F)$ and $\mathcal{S}(\mathbb{E}F|F)$, it follows that each of the groups $D(\mathfrak{P}|\mathfrak{p})$ and $D(\mathfrak{R}|\mathfrak{p})$ is trivial. Thus the group $D(\mathfrak{Q}|\mathfrak{p})$ is trivial. Once again by Lemma 9, one obtains that $e(\mathfrak{Q}|\mathfrak{p}) = 1$ and $f(\mathfrak{Q}|\mathfrak{p}) = 1$. Therefore $\mathfrak{p} \in \mathcal{S}(\mathbb{E}H|F)$.

Conversely, suppose that $\mathfrak{p} \in \mathcal{S}(\mathbb{E}H|F)$. By Lemma 9, it follows that $e(\mathfrak{Q}|\mathfrak{p}) = 1$ and $f(\mathfrak{Q}|\mathfrak{p}) = 1$. With the previous notation, the definitions of ramification index and relative degree yield that $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{R})e(\mathfrak{R}|\mathfrak{p})$ and $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{R})f(\mathfrak{R}|\mathfrak{p})$. Thus $e(\mathfrak{R}|\mathfrak{p}) = 1$ and $f(\mathfrak{R}|\mathfrak{p}) = 1$. Therefore $\mathfrak{p} \in \mathcal{S}(H|F)$.

By the previous argument, it follows that $\mathcal{S}(\mathbb{E}H|F) = \mathcal{S}(H|F)$. Let δ denote Dirichlet density. By Čebotarev's density theorem, one obtains that $\delta(\mathcal{S}(H|F)) = [H : F]^{-1}$ and $\delta(\mathcal{S}(\mathbb{E}H|F)) = [\mathbb{E}H : F]^{-1}$ [38]. Thus $\mathbb{E}H = H$. As H is a geometric extension of F, it follows that $\mathbb{E} = \mathbb{F}_F$. Therefore $\mathfrak{d}(H|F) = [\mathbb{E} : \mathbb{F}_F] = 1$. □

Lemma 13. *Let H be a finite, abelian, geometric, and unramified extension of F. It holds that $[H : F] \leq h_F$.*

Proof. Let M be the fixed field of the image of the Artin map of $H|F$ in $\mathrm{Gal}(H|F)$ [28]. By the definition of M, it holds that $\mathcal{S}(M|F) = \mathbb{P}_F$. By Čebotarev's density theorem, one obtains that $\delta(\mathcal{S}(M|F)) = [M : F]^{-1}$ and $\delta(\mathbb{P}_F) = 1$ [38]. Thus $M = F$. By the Galois correspondence, the Artin map of $H|F$ surjects onto $\mathrm{Gal}(H|F)$ [7].

Let the Artin map of $H|F$ be written for each $\mathfrak{a} \in D_F$ as $(\mathfrak{A}, H|F)$. Let $\sigma \in \mathrm{Gal}(H|F)$. By the previous argument, there exists $\mathfrak{a} \in D_F$ with $(\mathfrak{a}, H|F) = \sigma$. By Lemma 12, there exist $\mathfrak{p}_1, ..., \mathfrak{p}_m \in \mathcal{S}(H|F)$ and integers $a_1, ..., a_m$ with

$$\sum_{i=1}^{m} a_i d_F(\mathfrak{p}_i) = 1.$$

Let $n = d_F(\mathfrak{a})$. Let $\mathfrak{b} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_m^{a_m}$. Thus $(\mathfrak{b}, H|F)$ is trivial and $d_F(\mathfrak{b}) = 1$. Therefore $(\mathfrak{a}\mathfrak{b}^{-n}, H|F) = (\mathfrak{a}, H|F)$ and $d_F(\mathfrak{a}\mathfrak{b}^{-n}) = 0$. Let $D_{F,0}$ denote the group of divisors of F of degree equal to zero. By the previous argument, it follows that the Artin map of $H|F$ for $D_{F,0}$ surjects onto $\mathrm{Gal}(H|F)$. Let P_F denote the group of principal divisors of F. By global class field theory, the Artin map of $H|F$ is trivial for P_F [19]. Therefore

$$[H : F] = |\mathrm{Gal}(H|F)| \leq |D_{F,0}/P_F| = h_F.$$

□

Let $F_\mathfrak{p}$ denote the completion of F for $\mathfrak{p}$. Let $\mathfrak{p}$ be identified with its unique extension fo $F_\mathfrak{p}$ [28].

Lemma 14. *Let V be a finite extension of $F_\mathfrak{p}$. Let $\mathfrak{P} \in \{V|\mathfrak{p}\}$. It holds that $\{V|\mathfrak{p}\} = \mathfrak{P}$. Furthermore, V is complete for the place $\mathfrak{P}$.*

Proof. Let $n = \dim_{F_\mathfrak{p}} V$. If $n = 1$, the result is immediate. Let $n \in \mathbb{N}$ with $n > 1$. Let $\{\alpha_1, ..., \alpha_n\}$ denote a basis of V over $F_\mathfrak{p}$. For each $m \in \mathbb{N}$, let

$$x_m = \sum_{i=1}^{n} a_{i,m}\alpha_i$$

with $a_{1,m}, ..., a_{n,m} \in F_\mathfrak{p}$. One has, for each element $m \in \mathbb{N}$, that

$$\begin{aligned} v_\mathfrak{P}(x_m) &= v_\mathfrak{P}(\sum_{i=1}^{n} a_{i,m}\alpha_i) \geq \min_{1\leq i\leq n}\{v_\mathfrak{P}(a_{i,m}\alpha_i)\} = \min_{1\leq i\leq n}\{v_\mathfrak{P}(a_{i,m}) + v_\mathfrak{P}(\alpha_i)\} \\ &\geq \min_{1\leq i\leq n}\{v_\mathfrak{P}(a_{i,m})\} + \min_{1\leq i\leq n}\{v_\mathfrak{P}(\alpha_i)\} = \min_{1\leq i\leq n}\{e(\mathfrak{P}|\mathfrak{p})v_\mathfrak{p}(a_{i,m})\} + \min_{1\leq i\leq n}\{v_\mathfrak{P}(\alpha_i)\} \\ &= e(\mathfrak{P}|\mathfrak{p})\min_{1\leq i\leq n}\{v_\mathfrak{p}(a_{i,m})\} + \min_{1\leq i\leq n}\{v_\mathfrak{P}(\alpha_i)\}. \end{aligned}$$

Thus if $\lim^\mathfrak{p}_{m\to\infty} a_{i,m} = 0$ for each $i = 1, ..., n$, then $\lim^\mathfrak{P}_{m\to\infty} x_m = 0$.

Conversely, suppose that there exists $i \in \{1, ..., n\}$ so that $\{a_{i,m}\}_{m\in\mathbb{N}}$ is not convergent to zero for $\mathfrak{p}$. Thus it may be assumed that there exists $N \in \mathbb{N}$ so that, for each $m \in \mathbb{N}$, $v_\mathfrak{p}(a_{i,m}) \leq N$. It follows for each $m \in \mathbb{N}$ that

$$v_\mathfrak{P}\left(\frac{x_m}{a_{i,m}}\right) = v_\mathfrak{P}(x_m) - v_\mathfrak{P}(a_{i,m}) = v_\mathfrak{P}(x_m) - e(\mathfrak{P}|\mathfrak{p})v_\mathfrak{p}(a_{i,m}) \geq v_\mathfrak{P}(x_m) - e(\mathfrak{P}|\mathfrak{p})N.$$

Thus $\lim^{\mathfrak{P}}_{m\to\infty} \frac{x_m}{a_{i,m}} = 0$. It follows that the sequence $\left\{\sum_{j\neq i} \frac{a_{j,m}}{a_{i,m}}\alpha_j\right\}_{m\in\mathbb{N}}$ is convergent for $\mathfrak{P}$. By induction, for each $j \in \{1, ..., n\}$ with $j \neq i$, there exists $a_j \in F_{\mathfrak{p}}$ so that $\lim^{\mathfrak{p}}_{m\to\infty} \frac{a_{j,m}}{a_{i,m}} = a_j$. Therefore

$$\alpha_i = \sum_{j\neq i} -a_i\alpha_j.$$

This is a contradiction. The result follows. □

Let $K_{\mathfrak{P}}$ denote the completion of K for $\mathfrak{P}$. Let $\mathfrak{P}$ be identified with its unique extension to $K_{\mathfrak{P}}$.

Lemma 15. *The field $K_{\mathfrak{P}}$ is a finite and Galois extension of $F_{\mathfrak{p}}$.*

Proof. Let K be identified with its image in $K_{\mathfrak{P}}$. As K is a finite and Galois extension of F, it follows from basic Galois theory that $KF_{\mathfrak{p}}$ is a finite and Galois extension of $F_{\mathfrak{p}}$ [7]. By Lemma 14, one obtains that $KF_{\mathfrak{p}}$ is complete for the place $\mathfrak{P}$. Also, one has that $K \subset KF_{\mathfrak{p}} \subset K_{\mathfrak{P}}$. It follows that $KF_{\mathfrak{p}} = K_{\mathfrak{P}}$. □

Definition. For each non-negative integer n, the *nth ramification group* of $\mathfrak{P}|\mathfrak{p}$ is defined as

$$G_n(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K_{\mathfrak{P}}|F_{\mathfrak{p}}) \mid \text{for each } \alpha \in \vartheta_{\mathfrak{P}},\ v_{\mathfrak{P}}(\sigma(\alpha) - \alpha) \geq n + 1\}.$$

Lemma 16. *It holds that $|G_0(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})$.*

Proof. By Lemma 10, it suffices to show that $|G_0(\mathfrak{P}|\mathfrak{p})| = |I(\mathfrak{P}|\mathfrak{p})|$. By the definition of the inertia group, it holds that $I(\mathfrak{P}|\mathfrak{p}) \subset D(\mathfrak{P}|\mathfrak{p})$. By the proof of Lemma 14, it follows that each $\sigma \in I(\mathfrak{P}|\mathfrak{p})$ extends continuously to an element $\hat{\sigma} \in \mathrm{Gal}(K_{\mathfrak{P}}|F_{\mathfrak{p}})$. Let $\alpha \in K_{\mathfrak{P}}$. Let $\{\alpha_n\}_{n\in\mathbb{N}} \subset K$ with $\lim^{\mathfrak{P}}_{n\to\infty} \alpha_n = \alpha$. This yields that

$$\hat{\sigma}(\alpha) = \lim^{\mathfrak{P}}_{n\to\infty} \sigma(\alpha_n) \equiv \lim^{\mathfrak{P}}_{n\to\infty} \alpha_n \bmod \mathfrak{P} \equiv \alpha \bmod \mathfrak{P}.$$

Thus $\hat{\sigma} \in G_0(\mathfrak{P}|\mathfrak{p})$.

Conversely, let $\eta \in G_0(\mathfrak{P}|\mathfrak{p})$. By the definition of $G_0(\mathfrak{P}|\mathfrak{p})$, it holds that $\eta|_K \in I(\mathfrak{P}|\mathfrak{p})$. Therefore the elements of $I(\mathfrak{P}|\mathfrak{p})$ and $G_0(\mathfrak{P}|\mathfrak{p})$ are in one-to-one correspondence. □

Definition. A *jump* in the ramification of $\mathfrak{P}|\mathfrak{p}$ is a non-negative integer n so that $G_n(\mathfrak{P}|\mathfrak{p}) \neq G_{n+1}(\mathfrak{P}|\mathfrak{p})$. Let $k(\mathfrak{P}|\mathfrak{p})$ be the number of jumps in the ramification of $\mathfrak{P}|\mathfrak{p}$. Let $\alpha_{\mathfrak{P}|\mathfrak{p}}$ be the differential exponent for $\mathfrak{P}|\mathfrak{p}$ [38].

Henceforth, let each $\eta \in \mathrm{Gal}(K_{\mathfrak{P}}|F_{\mathfrak{p}})$ be identified with $\eta|_K$.

Lemma 17. *Each of the quantities $k(\mathfrak{P}|\mathfrak{p})$ and $\alpha_{\mathfrak{P}|\mathfrak{p}}$ is independent of the choice of $\mathfrak{P} \in \{K|\mathfrak{p}\}$.*

Proof. Let n be a non-negative integer. Let $\sigma \in \mathrm{Gal}(K|F)$. Let $\eta \in G_n(\sigma(\mathfrak{P})|\mathfrak{p})$. Let $\beta \in \vartheta_{\mathfrak{P}}$. As $\sigma(\vartheta_{\mathfrak{P}}) = \vartheta_{\sigma(\mathfrak{P})}$, it holds that $\sigma(\beta) \in \vartheta_{\sigma(\mathfrak{P})}$. Thus

$$v_{\mathfrak{P}}(\sigma^{-1}\eta\sigma(\beta) - \beta) = v_{\mathfrak{P}}(\sigma^{-1}\eta\sigma(\beta) - \sigma^{-1}\sigma(\beta)) = v_{\sigma(\mathfrak{P})}(\eta\sigma(\beta) - \sigma(\beta)) \geq n + 1.$$

This implies that $G_n(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma G_n(\mathfrak{P}|\mathfrak{p})\sigma^{-1}$. In particular, one obtains that $|G_n(\sigma(\mathfrak{P})|\mathfrak{p})| = |\sigma G_n(\mathfrak{P}|\mathfrak{p})\sigma^{-1}| = |G_n(\mathfrak{P}|\mathfrak{p})|$. It follows that the jumps in the ramification of $\mathfrak{P}|\mathfrak{p}$ are the same as the those in the ramification of $\sigma(\mathfrak{P})|\mathfrak{p}$. By the proof of Lemma 7, $\mathrm{Gal}(K|F)$ acts transitively on $\{K|\mathfrak{p}\}$. It follows that $|G_n(\mathfrak{P}|\mathfrak{p})|$ is independent of the choice of $\mathfrak{P} \in \{K|\mathfrak{p}\}$. This establishes the result for $k(\mathfrak{P}|\mathfrak{p})$.

By ramification theory [38], it holds that

$$\alpha_{\mathfrak{P}|\mathfrak{p}} = \sum_{i=0}^{\infty}(|G_i(\mathfrak{P}|\mathfrak{p})| - 1).$$

By the previous argument, the result also follows for $\alpha_{\mathfrak{P}|\mathfrak{p}}$. □

Henceforth, let K be a finite and abelian extension of F.

Lemma 18. *It holds that $K_{\mathfrak{P}}|F_{\mathfrak{p}}$ is finite and abelian.*

Proof. As $\mathrm{Gal}(K|F)$ is abelian, so must $D(\mathfrak{P}|\mathfrak{p})$ also be abelian. By Lemma 15, one has that $K_{\mathfrak{P}}$ is a finite and Galois extension of $F_{\mathfrak{p}}$. Also, by the proof of Lemma 14, $\mathrm{Gal}(K_{\mathfrak{P}}|F_{\mathfrak{p}})$ is isomorphic to $D(\mathfrak{P}|\mathfrak{p})$. The result follows. □

Lemma 19. *The group $G_0(\mathfrak{P}|\mathfrak{p})$ is independent of the choice of $\mathfrak{P} \in \{K|\mathfrak{p}\}$.*

Proof. By the proof of Lemma 17, one has for each $\sigma \in \mathrm{Gal}(K|F)$ that $G_0(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma G_0(\mathfrak{P}|\mathfrak{p})\sigma^{-1}$. As $\mathrm{Gal}(K|F)$ is abelian, it follows that $\sigma G_0(\mathfrak{P}|\mathfrak{p})\sigma^{-1} = G_0(\mathfrak{P}|\mathfrak{p})$. By the proof of Lemma 7, $\mathrm{Gal}(K|F)$ acts transitively on $\{K|\mathfrak{p}\}$. The result follows. □

Lemma 20. *It holds that* $\alpha_{\mathfrak{P}|\mathfrak{p}} \geq \frac{1}{2}k(\mathfrak{P}|\mathfrak{p})e(\mathfrak{P}|\mathfrak{p})$.

Proof. Let the jumps in the ramification of $\mathfrak{P}|\mathfrak{p}$ be denoted by $r_1(\mathfrak{P}|\mathfrak{p}), ..., r_{k(\mathfrak{P}|\mathfrak{p})}(\mathfrak{P}|\mathfrak{p})$. Let $n_1(\mathfrak{P}|\mathfrak{p}) = r_1(\mathfrak{P}|\mathfrak{p}) + 1$. Also, for each $m = 2, ..., k(\mathfrak{P}|\mathfrak{p})$, let $n_m(\mathfrak{P}|\mathfrak{p}) = r_m(\mathfrak{P}|\mathfrak{p}) - r_{m-1}(\mathfrak{P}|\mathfrak{p})$. By Lemma 18, it holds that $K_\mathfrak{P}$ is a finite and abelian extension of $F_\mathfrak{p}$. By the Hasse-Arf theorem [28], it follows for each $m = 1, ..., k(\mathfrak{P}|\mathfrak{p})$ that $|G_0(\mathfrak{P}|\mathfrak{p})| \,\Big|\, n_m(\mathfrak{P}|\mathfrak{p})|G_{(r_m(\mathfrak{P}|\mathfrak{p}))}(\mathfrak{P}|\mathfrak{p})|$. By ramification theory [38], it follows that

$$\begin{aligned}
\alpha_{\mathfrak{P}|\mathfrak{p}} &= \sum_{m=1}^{k(\mathfrak{P}|\mathfrak{p})} n_m(\mathfrak{P}|\mathfrak{p}) \left(|G_{(r_m(\mathfrak{P}|\mathfrak{p}))}(\mathfrak{P}|\mathfrak{p})| - 1\right) \\
&= \sum_{m=1}^{k(\mathfrak{P}|\mathfrak{p})} n_m(\mathfrak{P}|\mathfrak{p})|G_{(r_m(\mathfrak{P}|\mathfrak{p}))}(\mathfrak{P}|\mathfrak{p})| \left(1 - |G_{(r_m(\mathfrak{P}|\mathfrak{p}))}(\mathfrak{P}|\mathfrak{p})|^{-1}\right) \\
&\geq \frac{1}{2} \sum_{m=1}^{k(\mathfrak{P}|\mathfrak{p})} n_m(\mathfrak{P}|\mathfrak{p})|G_{(r_m(\mathfrak{P}|\mathfrak{p}))}(\mathfrak{P}|\mathfrak{p})| \\
&\geq \frac{1}{2} k(\mathfrak{P}|\mathfrak{p})|G_0(\mathfrak{P}|\mathfrak{p})|.
\end{aligned}$$

By Lemma 16, the result follows. □

Lemma 21. *It holds that* $e(\mathfrak{P}|\mathfrak{p}) \leq |\vartheta_\mathfrak{p}/\mathfrak{p}|^{k(\mathfrak{P}|\mathfrak{p})}$.

Proof. By Lemma 15, it holds that $K_\mathfrak{P}$ is a finite and Galois extension of $F_\mathfrak{p}$. Let $\eta \in \mathrm{Gal}(K_\mathfrak{P}|F_\mathfrak{p})$. The field $\vartheta_\mathfrak{P}/\mathfrak{P}$ is a finite and Galois extension of $\vartheta_\mathfrak{p}/\mathfrak{p}$ [7]. Let $\tilde{\eta}_0 \in \mathrm{Gal}(\vartheta_\mathfrak{P}/\mathfrak{P}|\vartheta_\mathfrak{p}/\mathfrak{p})$ be defined for each $\alpha \in \vartheta_\mathfrak{P}$ as $\tilde{\eta}_0(\alpha \bmod \mathfrak{P}) = \eta(\alpha) \bmod \mathfrak{P}$. Let $\pi_\mathfrak{P}$ be prime for $\mathfrak{P}$. Let ψ_0 be defined for each $\sigma \in G_0(\mathfrak{P}|\mathfrak{p})$ as $\psi_0(\sigma) = \frac{\sigma(\pi_\mathfrak{P})}{\pi_\mathfrak{P}}$. By ramification theory, the map ψ_0 induces an injection of $G_0(\mathfrak{P}|\mathfrak{p})/G_1(\mathfrak{P}|\mathfrak{p})$ into $(\vartheta_\mathfrak{P}/\mathfrak{P})^*$ [38]. Let $\tau \in \mathrm{Gal}(\vartheta_\mathfrak{P}/\mathfrak{P}|\vartheta_\mathfrak{p}/\mathfrak{p})$. By the proof of Lemma 10, there exists $\eta \in \mathrm{Gal}(K_\mathfrak{P}|F_\mathfrak{p})$ so that $\tilde{\eta}_0 = \tau$. Let $\sigma \in G_0(\mathfrak{P}|\mathfrak{p})$. By Lemma 18, it holds that $K_\mathfrak{P}$ is an abelian extension of $F_{\mathfrak{p}}$. Thus one obtains that

$$\tau(\psi_0(\sigma) \bmod \mathfrak{P}) = \tilde{\eta}_0\left(\frac{\sigma(\pi_{\mathfrak{P}})}{\pi_{\mathfrak{P}}} \bmod \mathfrak{P}\right) = \frac{\eta(\sigma(\pi_{\mathfrak{P}}))}{\eta(\pi_{\mathfrak{P}})} \bmod \mathfrak{P} = \frac{\sigma(\eta(\pi_{\mathfrak{P}}))}{\eta(\pi_{\mathfrak{P}})} \bmod \mathfrak{P}.$$

By Lemma 14, it holds that $\mathfrak{P} = \{K_{\mathfrak{P}}|\mathfrak{p}\}$. It follows that the element $\eta(\pi_{\mathfrak{P}})$ is prime for $\mathfrak{P}$. Also by ramification theory, the map ψ_0 is independent of the choice of prime element for $\mathfrak{P}$ [38]. This yields that $\tau(\psi_0(\sigma) \bmod \mathfrak{P}) = \psi_0(\sigma) \bmod \mathfrak{P}$. By the Galois correspondence [7], it follows that the image of ψ_0 lies in $(\vartheta_{\mathfrak{p}}/\mathfrak{p})^*$. Thus $|G_0(\mathfrak{P}|\mathfrak{p})/G_1(\mathfrak{P}|\mathfrak{p})| \leq |(\vartheta_{\mathfrak{p}}/\mathfrak{p})^*| \leq |\vartheta_{\mathfrak{p}}/\mathfrak{p}|$.

Let n be a positive integer. Once again, let $\eta \in \mathrm{Gal}(K_{\mathfrak{P}}|F_{\mathfrak{p}})$. Let $\tilde{\eta}_n$ be defined for each $\alpha \in \mathfrak{P}^n$ as $\tilde{\eta}_n(\alpha \bmod \mathfrak{P}^{n+1}) = \eta(\alpha) \bmod \mathfrak{P}^{n+1}$. As before, let $\pi_{\mathfrak{P}}$ be prime for $\mathfrak{P}$. Let ψ_n be defined for each $\sigma \in G_n(\mathfrak{P}|\mathfrak{p})$ as $\psi_n(\sigma) = \frac{\sigma(\pi_{\mathfrak{P}})}{\pi_{\mathfrak{P}}} - 1$. By ramification theory, ψ_n induces an injection of $G_n(\mathfrak{P}|\mathfrak{p})/G_{n+1}(\mathfrak{P}|\mathfrak{p})$ into $\mathfrak{P}^n/\mathfrak{P}^{n+1}$ [38]. Let $\eta \in \mathrm{Gal}(K_{\mathfrak{P}}|F_{\mathfrak{p}})$. Let $\sigma \in G_n(\mathfrak{P}|\mathfrak{p})$. As in the previous argument, one obtains that $\tilde{\eta}_n(\psi_n(\sigma) \bmod \mathfrak{P}^{n+1}) = \psi_n(\sigma) \bmod \mathfrak{P}^{n+1}$. By the Galois correspondence [7], it follows that the dimension over $\vartheta_{\mathfrak{p}}/\mathfrak{p}$ of the image of ψ_n is at most one. Thus $|G_n(\mathfrak{P}|\mathfrak{p})/G_{n+1}(\mathfrak{P}|\mathfrak{p})| \leq |\vartheta_{\mathfrak{p}}/\mathfrak{p}|$. Therefore

$$\begin{aligned}|G_0(\mathfrak{P}|\mathfrak{p})| &= \prod_{i=0}^{r_{k(\mathfrak{P}|\mathfrak{p})}} |G_i(\mathfrak{P}|\mathfrak{p})/G_{i+1}(\mathfrak{P}|\mathfrak{p})| \\ &= \prod_{m=1}^{k(\mathfrak{P}|\mathfrak{p})} |G_{(r_m(\mathfrak{P}|\mathfrak{p}))}(\mathfrak{P}|\mathfrak{p})/G_{(r_m(\mathfrak{P}|\mathfrak{p}))+1}(\mathfrak{P}|\mathfrak{p})| \\ &\leq |\vartheta_{\mathfrak{p}}/\mathfrak{p}|^{k(\mathfrak{P}|\mathfrak{p})}.\end{aligned}$$

By Lemma 16, the result follows. □

Lemma 22. *Let $\mathfrak{D}_{K|F}$ denote the different of K over F. Let $H_{K|F}$ denote the maximal unramified extension of F in K. It holds that*

$$d_K(\mathfrak{D}_{K|F}) \geq \frac{[K:F]}{2\ln|\mathbb{F}_F|}\left(\ln[K:F] - \ln\left[H_{K|F}:F\right]\right).$$

Proof. By Lemmas 7 and 17, each of the quantities $e(\mathfrak{P}|\mathfrak{p})$, $f(\mathfrak{P}|\mathfrak{p})$, $k(\mathfrak{P}|\mathfrak{p})$, and $\alpha_{\mathfrak{P}|\mathfrak{p}}$ is independent of the choice of $\mathfrak{P} \in \{K|\mathfrak{p}\}$, for each $\mathfrak{p} \in \mathbb{P}_F$. Thus one may write

$e(\mathfrak{P}|\mathfrak{p}) = e(K|\mathfrak{p})$, $f(\mathfrak{P}|\mathfrak{p}) = f(K|\mathfrak{p})$, $k(\mathfrak{P}|\mathfrak{p}) = k(K|\mathfrak{p})$, and $\alpha_{\mathfrak{P}|\mathfrak{p}} = \alpha_{K|\mathfrak{p}}$. Let the collection of places of F that ramify in K be denoted by $\mathcal{R}(K|F)$. By Lemmas 8, 20, 21, and the definition of the degree of a place, it follows that

$$\begin{aligned} d_K(\mathfrak{D}_{K|F}) = \sum_{\mathfrak{p}\in R(K|F)} \sum_{\mathfrak{P}\in\{K|\mathfrak{p}\}} \alpha_{K|\mathfrak{p}} d_K(\mathfrak{P}) &= \sum_{\mathfrak{p}\in R(K|F)} \sum_{\mathfrak{P}\in\{K|\mathfrak{p}\}} \alpha_{K|\mathfrak{p}} f(K|\mathfrak{p}) d_F(\mathfrak{p}) \\ &= \sum_{\mathfrak{p}\in R(K|F)} n(K|\mathfrak{p})\alpha_{K|\mathfrak{p}} f(K|\mathfrak{p}) d_F(\mathfrak{p}) \\ &\geq \frac{1}{2} \sum_{\mathfrak{p}\in R(K|F)} n(K|\mathfrak{p})k(K|\mathfrak{p})e(K|\mathfrak{p})f(K|\mathfrak{p})d_F(\mathfrak{p}) \\ &= \frac{[K:F]}{2} \sum_{\mathfrak{p}\in R(K|F)} k(K|\mathfrak{p})d_F(\mathfrak{p}) \\ &= \frac{[K:F]}{2\ln|\mathbb{F}_F|} \sum_{\mathfrak{p}\in R(K|F)} k(K|\mathfrak{p}) \ln|\vartheta_{\mathfrak{p}}/\mathfrak{p}| \\ &\geq \frac{[K:F]}{2\ln|\mathbb{F}_F|} \sum_{\mathfrak{p}\in R(K|F)} \ln e(K|\mathfrak{p}). \end{aligned}$$

By Lemma 19, the group $G_0(\mathfrak{P}|\mathfrak{p})$ is independent of the choice of $\mathfrak{P} \in \{K|\mathfrak{p}\}$, for each $\mathfrak{p} \in \mathbb{P}_F$. Thus one may write $G_0(\mathfrak{P}|\mathfrak{p}) = G_0(K|\mathfrak{p})$. Let

$$G_{\mathcal{R}(K|F)} = \prod_{\mathfrak{p}\in\mathbb{P}_F} G_0(K|\mathfrak{p}).$$

By ramification theory [38], the fixed field of $G_{R(K|F)}$ is equal to $H_{K|F}$. By Lemma 16 and the Galois correspondence [7], it follows that

$$\begin{aligned} \sum_{\mathfrak{p}\in R(K|F)} \ln e(K|\mathfrak{p}) = \sum_{\mathfrak{p}\in\mathbb{P}_F} \ln|G_0(K|\mathfrak{p})| = \ln\left(\prod_{\mathfrak{p}\in\mathbb{P}_F} |G_0(K|\mathfrak{p})|\right) \geq \ln\left|\prod_{\mathfrak{p}\in\mathbb{P}_F} G_0(K|\mathfrak{p})\right| \\ = \ln\left|G_{\mathcal{R}(K|F)}\right| = \ln\left[K : H_{K|F}\right] = \ln[K:F] - \ln\left[H_{K|F} : F\right]. \end{aligned}$$

The result follows. □

Lemma 23. *Let $\mathfrak{a} \in D_K$. Let $\mathfrak{a}$ be identified with its image in $D_{\mathbb{E}K}$. It holds that $d_{\mathbb{E}K}(\mathfrak{a}) = d_K(\mathfrak{a})$.*

Proof. By the definition of the degree function, it suffices to prove the claim for each $\mathfrak{p} \in \mathbb{P}_K$. By Lemma 5, it holds that the set $\{\mathbb{E}K|\mathfrak{p}\}$ is finite. Let $\{\mathbb{E}K|\mathfrak{p}\} =$

$\{\mathfrak{P}_1, ..., \mathfrak{P}_{n(\mathbb{E}K|\mathfrak{p})}\}$. Let $\mathfrak{p}$ be identified with its image in $D_{\mathbb{E}K}$. In $\mathbb{E}K$, one has the equality $\mathfrak{p} = \mathfrak{P}_1^{e(\mathfrak{P}_1|\mathfrak{p})} \cdots \mathfrak{P}_{n(\mathbb{E}K|\mathfrak{p})}^{e(\mathfrak{P}_{n(\mathbb{E}K|\mathfrak{p})}|\mathfrak{p})}$. By the proof of Lemma 5, it follows that

$$d_{\mathbb{E}K}(\mathfrak{p}) = d_{\mathbb{E}K}(\mathfrak{P}_1^{e(\mathfrak{P}_1|\mathfrak{p})} \cdots \mathfrak{P}_{n(\mathbb{E}K|\mathfrak{p})}^{e(\mathfrak{P}_{n(\mathbb{E}K|\mathfrak{p})}|\mathfrak{p})}) = \sum_{i=1}^{n} (\mathbb{E}K|\mathfrak{p}) e(\mathfrak{P}_i|\mathfrak{p}) d_{\mathbb{E}K}(\mathfrak{P}_i)$$
$$= \frac{d_K(\mathfrak{p})}{[\mathbb{E} : \mathbb{F}_K]} \sum_{i=1}^{r} e(\mathfrak{P}_i|\mathfrak{p}) d(\mathfrak{P}_i|\mathfrak{p}) = \frac{d_K(\mathfrak{p})}{[\mathbb{E} : \mathbb{F}_K]} [\mathbb{E}K : K] = d_K(\mathfrak{p}).$$

□

Lemma 24. *Let $\mathfrak{a} \in D_K$. Let $\mathfrak{a}$ be identified with its image in $D_{\mathbb{E}K}$. It holds that $l_{\mathbb{E}K}(\mathfrak{a}) = l_K(\mathfrak{a})$.*

Proof. Let $\mathbb{E}L_K(\mathfrak{a}) = \{\sum_{\text{finite}} a_i x_i \mid \text{for each } i,\ a_i \in \mathbb{E} \text{ and } x_i \in L_K(\mathfrak{a})\}$. Let $y \in \mathbb{E}L_K(\mathfrak{a})$. One may write

$$y = \sum_{i=1}^{n} a_i x_i$$

with $a_1, ..., a_n \in \mathbb{E}$ and $x_1, ..., x_n \in L_K(\mathfrak{a})$. Let $\mathfrak{p} \in \mathbb{P}_K$. Let $\mathfrak{P} \in \{\mathbb{E}K|\mathfrak{p}\}$. By the proof of Lemma 11, it holds that $e(\mathfrak{P}|\mathfrak{p}) = 1$. It follows that

$$v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}\left(\sum_{i=1}^{n} a_i x_i\right) \geq \min_{1\leq i\leq n}\{v_{\mathfrak{P}}(a_i x_i)\} = \min_{1\leq i\leq n}\{v_{\mathfrak{P}}(a_i) + v_{\mathfrak{P}}(x_i)\} = \min_{1\leq i\leq n}\{v_{\mathfrak{P}}(x_i)\}$$
$$= \min_{1\leq i\leq n}\{v_{\mathfrak{p}}(x_i)\} \geq v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{P}}(\mathfrak{a}).$$

Thus $\mathbb{E}L_K(\mathfrak{a}) \subset L_{\mathbb{E}K}(\mathfrak{a})$.

For the converse, let $y \in L_{\mathbb{E}K}(\mathfrak{a})$. Let $n = [\mathbb{E} : \mathbb{F}_K]$. Let $\xi \in \mathbb{E}$ with $\mathbb{E} = \mathbb{F}_K(\xi)$. One may write

$$y = \sum_{i=1}^{n} a_i \xi^i$$

with $a_1, ..., a_n \in \mathbb{E}$. Also, $\mathbb{E}K$ is a finite and Galois extension of K [7]. Let $y = y^{(1)}$, $y^{(2)}$,..., $y^{(n)}$ be the Galois conjugates of y over K. By Cramer's rule [22], one may write, for each $i = 1, ..., n$,

$$a_i = \sum_{j=1}^{n} t_{i,j} y^{(j)}$$

with $t_{i,1}, ..., t_{i,n} \in \mathbb{E}$. As $\mathfrak{a} \in D_K$, one obtains for each $j = 1, ..., n$ that $v_{\mathfrak{P}}(y^{(j)}) \geq v_{\mathfrak{P}}(\mathfrak{a})$. As $e(\mathfrak{P}|\mathfrak{p}) = 1$, it follows for each $i = 1, ..., n$ that

$$v_{\mathfrak{p}}(a_i) = v_{\mathfrak{p}}\left(\sum_{j=1}^{n} t_{i,j} y^{(j)}\right) = v_{\mathfrak{P}}\left(\sum_{j=1}^{n} t_{i,j} y^{(j)}\right) \geq \min_{1 \leq j \leq n}\{v_{\mathfrak{P}}(y^{(j)})\} \geq v_{\mathfrak{P}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{a}).$$

Thus $L_{\mathbb{E}K}(\mathfrak{a}) \subset \mathbb{E}L_K(\mathfrak{a})$.

By the previous argument, it follows that $L_{\mathbb{E}K}(\mathfrak{a}) = \mathbb{E}L_K(\mathfrak{a})$. By basic function field theory, the field of constants of $\mathbb{E}K$ is equal to $\mathbb{E}$ [38]. Therefore $l_{\mathbb{E}K}(\mathfrak{a}) = l_K(\mathfrak{a})$. □

Lemma 25. *Let $\mathbb{E}$ be a finite field that contains $\mathbb{F}_K$. It holds that $g_{\mathbb{E}K} = g_K$.*

Proof. Let $\mathfrak{a} \in D_K$ be chosen to satisfy $d_K(\mathfrak{a}) > \max\{2g_K - 2, 2g_{\mathbb{E}K} - 2\}$. Let $\mathfrak{a}$ be identified with its image in $D_{\mathbb{E}K}$. By the Riemann-Roch theorem [30], it follows that $l_{\mathbb{E}K}(\mathfrak{A}^{-1}) = d_{\mathbb{E}K}(\mathfrak{A}) - g_{\mathbb{E}K} + 1$ and $l_K(\mathfrak{A}^{-1}) = d_K(\mathfrak{A}) - g_K + 1$. By Lemmas 23 and 24, result follows. □

Theorem 2. *Let F be a fixed choice of congruence function field. Let K be a finite abelian extension of F. It holds that*

$$\limsup_{g_K \to \infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_K|} \leq 1.$$

Proof. Consider a sequence $\{K_n\}_{n \in \mathbb{N}}$ with K_n a finite and abelian extension of F for each $n \in \mathbb{N}$ and unbounded sequence of genera $\{g_{K_n}\}_{n \in \mathbb{N}}$. Furthermore, suppose that there exists $\delta \in \mathbb{R}$ with $\delta > 0$ and, for each $n \in \mathbb{N}$,

$$\frac{\ln h_{K_n}}{g_{K_n} \ln |\mathbb{F}_{K_n}|} \geq 1 + \delta.$$

Let $x \in F \backslash \mathbb{F}_F$. As $\mathbb{F}_F$ is algebraically closed in F, it follows that x is transcendental over $\mathbb{F}_F$. As $\mathbb{F}_K|\mathbb{F}_F$ is algebraic, it follows that x is transcendental over $\mathbb{F}_K$. In particular, one obtains that $x \in K \backslash \mathbb{F}_K$. By Lemma 6, there exists $\varepsilon \in \mathbb{R}$ with $\varepsilon > 0$ and, for each $n \in \mathbb{N}$,

$$\frac{[K_n : \mathbb{F}_{K_n}(x)]}{g_{K_n}} \geq \varepsilon.$$

Let $s \in \mathbb{C}$ and $n \in \mathbb{N}$. It is well-known [9] that there exist $\omega_1, ..., \omega_{2g_K} \in \mathbb{C}$ with

$$P_{K_n}(s) = \prod_{i=1}^{2g_{K_n}} (1 - \omega_i |\mathbb{F}_{K_n}|^{-s}).$$

By Riemann's hypothesis, one has for each $i = 1, ..., 2g_{K_n}$ that $|\omega_i| = |\mathbb{F}_{K_n}|^{\frac{1}{2}}$ [4]. Also, it is well-known that $P_{K_n}(0) = h_{K_n}$ [9]. Thus

$$\begin{aligned} h_{K_n} = P_{K_n}(0) = |P_{K_n}(0)| &= \left| \prod_{i=1}^{2g_{K_n}} (1 - \omega_i) \right| = \prod_{i=1}^{2g_{K_n}} |1 - \omega_i| \\ &\leq \prod_{i=1}^{2g_{K_n}} (1 + |\omega_i|) = \left(1 + |\mathbb{F}_{K_n}|^{\frac{1}{2}}\right)^{2g_{K_n}}. \end{aligned}$$

It may be assumed, for each $n \in \mathbb{N}$, that $g_{K_n} > 0$. Application of the logarithm yields that

$$\frac{\ln h_{K_n}}{g_{K_n} \ln |\mathbb{F}_{K_n}|} \leq \frac{2 \ln \left(1 + |\mathbb{F}_{K_n}|^{\frac{1}{2}}\right)}{\ln |\mathbb{F}_{K_n}|}.$$

It follows that the sequence $\{|\mathbb{F}_{K_n}|\}_{n \in \mathbb{N}}$ is bounded. Thus the field

$$\mathbb{E} = \prod_{n \in \mathbb{N}} \mathbb{F}_{K_n}$$

is finite.

Once again, let $n \in \mathbb{N}$. By basic function field theory [38], one obtains that $[\mathbb{E}K_n : \mathbb{E}(x)] = [K_n : \mathbb{F}_{K_n}(x)]$. By Lemma 25, it holds that $g_{\mathbb{E}K_n} = g_{K_n}$. Thus one obtains the inequality

$$\frac{[\mathbb{E}F : \mathbb{E}(x)]}{\varepsilon} \geq \frac{g_{\mathbb{E}K_n}}{[\mathbb{E}K_n : \mathbb{E}F]}.$$

As K_n is a finite and abelian extension of F, it follows by basic Galois theory that $\mathbb{E}K_n$ is a finite and abelian extension of $\mathbb{E}F$ [7]. In particular, it holds that $\mathbb{E}K_n$ is a finite and separable extension of $\mathbb{E}F$. Thus one may define the different of $\mathbb{E}K_n$ over $\mathbb{E}F$; let this be denoted by $\mathfrak{D}_{\mathbb{E}K_n|\mathbb{E}F}$. As $\mathbb{F}_F$ and $\mathbb{F}_{K_n}$ are contained in $\mathbb{E}$, it follows by basic function field theory that the field of constants of each of $\mathbb{E}F$ and $\mathbb{E}K_n$ is equal to $\mathbb{E}$ [38]. Thus $\mathbb{E}K_n$ is a geometric extension of $\mathbb{E}F$. Let $H_{\mathbb{E}K_n|\mathbb{E}F}$ denote the maximal unramified extension of $\mathbb{E}F$ in $\mathbb{E}K_n$. By the Riemann-Hurwitz formula [38] and Lemmas 13 and 22, one obtains that

$$\begin{aligned}
\frac{g_{\mathbb{E}K_n}}{[\mathbb{E}K_n : \mathbb{E}F]} &= \frac{1}{[\mathbb{E}K_n : \mathbb{E}F]} + g_{\mathbb{E}F} - 1 + \frac{1}{2\,[\mathbb{E}K_n : \mathbb{E}F]} d_{\mathbb{E}K_n}(\mathfrak{D}_{\mathbb{E}K_n|\mathbb{E}F}) \\
&\geq g_{\mathbb{E}F} - 1 + \frac{1}{2\,[\mathbb{E}K_n : \mathbb{E}F]} d_{\mathbb{E}K_n}(\mathfrak{D}_{\mathbb{E}K_n|\mathbb{E}F}) \\
&\geq g_{\mathbb{E}F} - 1 + \frac{1}{4\ln|\mathbb{E}|}(\ln\,[\mathbb{E}K_n : \mathbb{E}F] - \ln[H_{\mathbb{E}K_n|\mathbb{E}F} : \mathbb{E}F]) \\
&\geq g_{\mathbb{E}F} - 1 + \frac{1}{4\ln|\mathbb{E}|}(\ln\,[\mathbb{E}K_n : \mathbb{E}F] - \ln h_{\mathbb{E}F}).
\end{aligned}$$

It follows that the sequence $\{[\mathbb{E}K_n : \mathbb{E}F]\}_{n\in\mathbb{N}}$ is bounded. However, it also holds that

$$[\mathbb{E}K_n : \mathbb{E}F] \geq \frac{\varepsilon}{[\mathbb{E}F : \mathbb{E}(x)]} g_{K_n}.$$

As the sequence of genera $\{g_{K_n}\}_{n\in\mathbb{N}}$ is unbounded, this is a contradiction. The result follows. □

CHAPTER 4

CONCLUSIONS

One obtains as a corollary of Theorems 1 and 2 the main result of this work.

Corollary. *Let F be a fixed choice of congruence function field. Let K be a finite abelian extension of F. It holds that*

$$\lim_{g_K \to \infty} \frac{\ln h_K}{g_K \ln |\mathbb{F}_K|} = 1.$$

The following example demonstrates that Lemma 6 may not be applied to establish the previous Corollary in the case of a finite, tamely ramified [38], and geometric tower of extensions of a rational congruence function field so that each step in the tower is a Kummer extension [11].

Example. Let $p \in \mathbb{N}$ be a prime number. Let $q = p^2$. Let x_0 be an element transcendental over $\mathbb{F}_q$. For each $n \in \mathbb{N}$, let

$$x_n^{p+1} = (x_{n-1}+1)^{p+1} - 1 \text{ and } F_n = \mathbb{F}_q(x_0, x_1, ..., x_n).$$

Also, let $\mathbb{F}_q(x_0) = F_0$. Let $\mathfrak{p} \in \mathbb{P}_{F_0}$ be chosen with associated valuation $v_\mathfrak{p}$ defined for each $f, g \in \mathbb{F}_q[x_0]$ as

$$v_\mathfrak{p}\left(\frac{f}{g}\right) = d_{x_0}(f) - d_{x_0}(g).$$

One may write $x_1^{p+1} = x_0 f(x_0)$ with $f(x_0) \in \mathbb{F}_q[x_0]$. As f has constant term equal to one, it holds for a place $\mathfrak{P} \in \{F_1|\mathfrak{p}\}$ that

$$(p+1)v_\mathfrak{P}(x_1) = v_\mathfrak{P}(x_1^{p+1}) = v_\mathfrak{P}(x_0 f(x_0)) = v_\mathfrak{P}(x_0) + v_\mathfrak{P}(f(x_0)) = v_\mathfrak{P}(x_0) = e(\mathfrak{P}|\mathfrak{p}).$$

By Lemma 8, it follows that $e(\mathfrak{P}|\mathfrak{p}) = p + 1 = [F_1 : F_0]$. By basic function field theory, any constant extension of F_0 is unramified [38]. Futhermore, as $q = p^2$, the field $\mathbb{F}_q$ contains the $p+1$st roots of unity. Therefore F_1 is a finite, geometric and tamely ramified Kummer extension of F_0 [38]. Also, as $e(\mathfrak{P}|\mathfrak{p}) = p+1$, it follows that $v_{\mathfrak{P}}(x_1) = 1$. Thus one may repeat this argument inductively, which implies for each $n \in \mathbb{N}$ that F_n is a finite, tamely ramified, and geometric extension of F_0, as well as a Kummer extension of F_{n-1}. It is now shown that $\lim_{n\to\infty} g_{F_n} = \infty$ and $\liminf_{n\to\infty} \frac{[F_n:F_0]}{g_{F_n}} > 0$.

Let $\mathfrak{p}_\infty \in \mathbb{P}_{F_0}$ be chosen with associated valuation $v_{\mathfrak{p}_\infty}$ defined for each $f, g \in \mathbb{F}_q[x_0]$ as

$$v_{\mathfrak{p}_\infty}\left(\frac{f}{g}\right) = d_{x_0}(g) - d_{x_0}(f).$$

Let $n \in \mathbb{N}$. Let $y_n = \frac{x_n}{x_{n-1}}$. Let $\mathfrak{P} \in \{F_{n-1}|\mathfrak{p}_\infty\}$. Thus $y_n^{p+1} = \frac{f(x_{n-1})}{x_{n-1}^p} \in 1+\mathfrak{P}$. By Kummer's theorem [38], it follows that $\mathfrak{P}$ splits completely in F_n. Let $N_1(F_n)$ denote the collection of places of F_n of degree equal to one. By the previous argument, one obtains that $N_1(F_n) \geq [F_n : F_0]$. Also, by Riemann's hypothesis, one has that $|N_1(F_n) - (q+1)| \leq 2g_{F_n}q^{\frac{1}{2}}$ [4]. This yields that

$$g_{F_n} \geq \frac{N_1(F_n) - (q+1)}{2q^{\frac{1}{2}}} \geq \frac{[F_n : F_0] - (q+1)}{2q^{\frac{1}{2}}} = \frac{(p+1)^n - (q+1)}{2q^{\frac{1}{2}}}.$$

Thus $\liminf_{n\to\infty} g_{F_n} = \infty$.

Let $n \in \mathbb{N}$. Let $\mathfrak{p} \in \mathbb{P}_{F_0}$ be ramified in F_n. Let $\mathfrak{P} \in \{F_n|\mathfrak{p}\}$. For each $i = 0, ..., n-1$, let $\mathfrak{P}_i \in \mathbb{P}_{F_i}$ be chosen with $\mathfrak{P} \in \{F_n|\mathfrak{P}_i\}$. As $\mathfrak{p}$ is ramified in F_n, there exists $i \in \{0, ..., n-1\}$ so that $\mathfrak{P}_i$ is ramified in F_{i+1}. By Kummer theory [38], it follows that $x_i \in \mathfrak{P}_i$. Therefore $x_i \bmod \mathfrak{P}_i = 0 \in \mathbb{F}_q$. Thus $x_{i-1} \bmod \mathfrak{P}_{i-1} \in \mathbb{F}_q$. As $q = p^2$, it follows that $x_{i-1}^{p+1} \bmod \mathfrak{P}_{i-1} \in \mathbb{F}_p$. This yields that $x_{i-2} \bmod \mathfrak{P}_{i-2} \in \mathbb{F}_q$. By induction, one obtains that $x_0 \bmod \mathfrak{p} \in \mathbb{F}_q$. In particular, there exists $\alpha \in \mathbb{F}_q$ for which $\mathfrak{p}$ is associated with the valuation $v_{\mathfrak{p}}$ defined for each $f, g \in \mathbb{F}_q[x_0 - \alpha]$ as

$$v_{\mathfrak{p}_\infty}\left(\frac{f}{g}\right) = d_{(x_0-\alpha)}(f) - d_{(x_0-\alpha)}(g).$$

It follows that $d_{F_0}(\mathfrak{p}) = 1$, and that the number of places of F_0 that ramify in F_n cannot be greater than q. Also, as F_0 is a field of rational functions, it follows that

$g_{F_0} = 0$. Let $\mathcal{R}(F_n|F_0)$ denote the collection of places of F_0 that ramify in F_n. As F_n is a finite, separable and tamely ramified extension of F_0, it follows by ramification theory [38], the Riemann-Hurwitz formula [38] and the proof of Lemma 5 that

$$\begin{aligned}
g_{F_n} &= 1 + [F_n : F_0](g_{F_0} - 1) + \frac{1}{2} d_{F_n}(\mathfrak{D}_{F_n|F_0}) \\
&= 1 - [F_n : F_0] + \frac{1}{2} d_{F_n}(\mathfrak{D}_{F_n|F_0}) \\
&= 1 - [F_n : F_0] + \frac{1}{2} \sum_{\mathfrak{p} \in \mathcal{R}(F_n|F_0)} \sum_{\mathfrak{P} \in \{F_n|\mathfrak{p}\}} (e(\mathfrak{P}|\mathfrak{p}) - 1) d_{F_n}(\mathfrak{P}) \\
&\leq 1 - [F_n : F_0] + \frac{1}{2} \sum_{\mathfrak{p} \in \mathcal{R}(F_n|F_0)} \sum_{\mathfrak{P} \in \{F_n|\mathfrak{p}\}} e(\mathfrak{P}|\mathfrak{p}) d_{F_n}(\mathfrak{P}) \\
&= 1 - [F_n : F_0] + \frac{1}{2} \sum_{\mathfrak{p} \in \mathcal{R}(F_n|F_0)} \sum_{\mathfrak{P} \in \{F_n|\mathfrak{p}\}} e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p}) d_{F_0}(\mathfrak{p}) \\
&= 1 - [F_n : F_0] + \frac{[F_n : F_0]}{2} \sum_{\mathfrak{p} \in \mathcal{R}(F_n|F_0)} d_{F_0}(\mathfrak{p}) \\
&= 1 - [F_n : F_0] + \frac{[F_n : F_0]}{2} \sum_{\mathfrak{p} \in \mathcal{R}(F_n|F_0)} 1 \\
&\leq 1 + [F_n : F_0] \left(\frac{q}{2} - 1 \right).
\end{aligned}$$

Thus $\liminf_{n\to\infty} \frac{[F_n:F_0]}{g_{F_n}} > 0$. □

In general, the asymptotic relationship between class number and genus remains an open problem. It is worthy of note that the proof of the main result of this work is similar to the original proof of the classical Brauer-Siegel theorem [6], which states, for finite normal extensions K of $\mathbb{Q}$ with class number h_K, regulator R_K, and discriminant d_K, that

$$\lim_{\frac{[K:\mathbb{Q}]}{\ln |d_K|} \to 0} \frac{\ln (h_K R_K)}{\ln \sqrt{|d_K|}} = 1.$$

For example, one may notice that the lower bound of Theorem 1 is effective, whereas the upper bound of Theorem 2 is ineffective and established by uniqueness of a certain limit point using the value of a zeta function near one.

BIBLIOGRAPHY

[1] E. Artin. Quadratische körper im gebiete der höheren kongruenzen. II. *Mathematische Zeitschrift*, 19:207–246, 1924.

[2] E. Artin. Beweis des allgemeinen reziprozitätsgesetzes. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5:353–363, 1927.

[3] E. Artin and J. Tate. *Class Field Theory.* W.A. Benjamin, New York, 1967.

[4] E. Bombieri. Counting points on curves over finite fields. *Seminaire Bourbaki*, 430:234–241, 1973.

[5] R. Brauer. On the zeta functions of algebraic number fields. *American Journal of Mathematics*, 69(2):243–250, 1947.

[6] R. Brauer. On the zeta functions of algebraic number fields II. *American Journal of Mathematics*, 72(4):739–746, 1950.

[7] D. Cox. *Galois Theory.* John Wiley and Sons, Hoboken, 2004.

[8] R. Dedekind and H. Weber. Theorie der algebraischen functionen einer veränderlichen. *Journal für die reine und angewandte Mathematik*, 92:181–290, 1882.

[9] M. Deuring. *Lectures on the Theory of Algebraic Functions.* Springer, Berlin, 1973.

[10] G. Frey, M. Perret, and H. Stichtenoth. On the different of abelian extensions of global fields. *Coding Theory and Algebraic Geometry*, 1518:26–32, 1992.

[11] A. Garcia, H. Stichtenoth, and M. Thomas. On towers and composita of towers of function fields over finite fields. *Finite fields and their applications*, 3:257–274, 1997.

[12] H. Hasse. Bericht über neuere untersuchungen und probleme aus der theorie der algebraischen zahlkörper. I. Klassenkörpertheorie. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 35:1–55, 1926.

[13] H. Hasse. Abstrakte begründung der komplexen multiplication und Riemannsche vermutung in funktionenkörpern. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 10:325–348, 1934.

[14] H. Hasse. Explizite konstruktion zyklischer klassenkörper. *Mathematische Annalen*, 109(1):191–195, 1934.

[15] D. Hayes. Explicit class field theory for rational function fields. *Transactions of the American Mathematical Society*, 189:77–91, 1974.

[16] D. Hilbert. Zahlbericht. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 4:175–546, 1897.

[17] D. Hilbert. Mathematische probleme. *Nachrichten von der Königlich Gesellschaft der Wissenschaften zu Göttingen. Mathematische-physikalische Klasse*, pages 253–297, 1900.

[18] E. Inaba. Number of divisor classes in algebraic function fields. *Proceedings of the Japan Academy*, 28(7):1–4, 1950.

[19] S. Iyanaga. *The theory of numbers*. North-Holland, Amsterdam, 1975.

[20] L. Kronecker. Über die algebraisch auflösbaren gleichungen. *Bericht der Königlich Preušischen Akademie der Wissenschaften zu Berlin*, pages 365–374, 1853.

[21] P. Lam-Estrada and G. D. Villa-Salvador. Some remarks on the theory of cyclotomic function fields. *The Rocky Mountain Journal of Mathematics*, 31(2):483–502, 2001.

[22] S. Lang. *Algebra*. Springer, New York, 2002.

[23] I. Luthar and S. Gogia. The Brauer-Siegel theorem for algebraic function fields. *Journal für die reine und angewandte Mathematik*, 299-300:28–37, 1978.

[24] M. Madan and D. Madden. On the theory of congruence function fields. *Communications in Algebra*, 8(17):1687–1697, 1980.

[25] A. F. Möbius. Über eine besondere art von umkehrung der reihen. *Journal für die reine und angewandte Mathematik*, 9:105–123, 1832.

[26] M. Nathanson. *Elementary Methods in Number Theory*. Springer, Berlin, 2000.

[27] J. Neukirch. *Class Field Theory*. Springer, Berlin, 1986.

[28] J. Neukirch. *Algebraic Number Theory*. Springer, New York, 1999.

[29] B. Riemann. Theorie der Abel'schen functionen. *Journal für die reine und angewandte Mathematik*, 54:115–155, 1857.

[30] G. Roch. Ueber die anzahl der willkürlichen constanten in algebraischen functionen. *Journal für die reine und angewandte Mathematik*, 64:372–376, 1865.

[31] M. Rosen. *Number Theory in Function Fields*. Springer, New York, 2002.

[32] H.K. Schmidt. Analytische zahlentheorie in körpern der charakteristik p. *Mathematische Zeitschrift*, 33:1–32, 1931.

[33] H.K. Schmidt. Zur arithmetischen theorie der algebraischen funktionen. I. *Mathematische Zeitschrift*, 41(1):415–438, 1936.

[34] C.L. Siegel. Über die classenzahl quadratischer zahlkörper. *Acta Arithmetica*, 1:83–86, 1935.

[35] S. A. Stepanov. On the number of points of a hyperelliptic curve over a finite prime field. *Izv. Akad. Nauk SSSR*, 33:1103–1111, 1969.

[36] T. Takagi. Ueber eine theorie des relativ Abel'schen zahlkörpers. *Journal of the College of Science*, 41(9):1–133, 1920.

[37] M. Tsfasman. Some remarks on the asymptotic number of points. *Coding Theory and Algebraic Geometry*, 1518:178–192, 1992.

[38] G. D. Villa-Salvador. *Topics in the Theory of Algebraic Function Fields.* Birkhäuser, Boston, 2006.

[39] A. Weil. Sur les fonctions algébriques à corps de constantes finies. *Comptes rendus de l'Académie des sciences*, 210:592–594, 1940.

[40] A. Weil. *Courbes algébriques et variétés abéliennes. Sur les courbes algébriques et les variétés qui s'en deduisent.* Hermann, Paris, 1948.

[41] E. Witt. Der existenzsatz für Abelsche funktionenkörper. *Journal für die reine und angewandte Mathematik*, 1935(173):43–51, 1935.

VITA

Kenneth Ward

Candidate for the Degree of

Doctor of Philosophy

Dissertation: ASYMPTOTICS OF CLASS NUMBER AND GENUS FOR ABELIAN EXTENSIONS OF AN ALGEBRAIC FUNCTION FIELD

Major Field: Pure Mathematics

Biographical:

Personal Data: Born in Euclid, Ohio, U.S.A. on September 19, 1982

Education:

Received the degree of B.A. in Mathematics with Honours, the University of Chicago, Chicago, Illinois, U.S.A., 2004

Received the degree of M.S. in Pure Mathematics, Oklahoma State University, Stillwater, Oklahoma, U.S.A., 2009

Completed the requirements for the degree of Doctor of Philosophy in Pure Mathematics, Oklahoma State University, Stillwater, Oklahoma, U.S.A., May 2012

Name: Kenneth Ward Date of Degree: May, 2012

Institution: Oklahoma State University Location: Stillwater, Oklahoma

Title of Study: ASYMPTOTICS OF CLASS NUMBER AND GENUS FOR ABELIAN EXTENSIONS OF AN ALGEBRAIC FUNCTION FIELD

Pages in Study: 36 Candidate for the Degree of Doctor of Philosophy

Major Field: Pure Mathematics

Among abelian extensions of a congruence function field, an asymptotic relation of class number and genus is established. The proof is completely classical, employing well-known results from congruence function field theory.

ADVISOR'S APPROVAL: David Wright ____________________