INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

Exponential Sums and L-Functions over Finite Fields

by

Francis Castro

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree Doctor of Philosophy, The City University of New York

1997

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

5/27/97 — Carlos J. Moreno

Date — Chair of Examining Committee

5/27/97 — I. Chavel (ATV)

Date — Executive Officer

Carlos J. Moreno
Professor Carlos J. Moreno

Raymond Hoobler
Professor Raymond Hoobler

Melvyn B. Nathanson
Professor Melvyn B. Nathanson

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Acknowledgments

I am particularly grateful to my advisor and Chairman of the dissertation committee, Dr. Carlos J. Moreno for his patience in directing this thesis, for his enthusiasm and encouragement during these years.

I want to thank Dr. Raymond Hoobler for his valuable suggestions and for being part of the dissertation committee. I am also thankful to Dr. Melvyn B. Nathanson for being part of the dissertation committee.

I want to thank Aaron Wan and Weichin Yao for their help and friendship.

I am grateful to my parents for teaching me the importance of education and for their moral support.

I would like to thank Dr. Oscar Moreno for his influence and help in my decision to undertake my PhD.

None of this would have been possible without the support and help of my wife, Zahideé. Her constant encouragement, helped me to go through the difficult moments of this journey.

Contents

Introduction

In this thesis we study several problems related to algebraic curves over finite fields and exponential sums in one and several variables. The following three topics are discussed:

(A.) In **Chapter 1** we make an analysis of the ramification groups of the composite field of an Artin-Schreier extension and a cyclic extension of degree p^i for $i = 1, 2$. This provides an effective method to calculate the conductor of the L-functions associated to such an extension. As a consequence of this calculation we are able to estimate certain mixed exponential sums constructed by multiplying an additive and a multiplicative character.

(B.) In **Chapter 2** we study algebraic curves with singularities and introduce a new definition of L-function associated to an abelian covering of the projective line. The main result we prove (Theorem 2.5) shows that our definition is compatible with that of the zeta function defined by Stöhr. We have calculated several examples and one (Example 2) is particularly interesting because it shows that the L-function may not be a rational function. The

main application we give of these results is to the definition of exponential sums over singular curves (Definition 2.8). In Theorem 2.9 we give estimates for such sums.

(C.) Chapter 3 deals mainly with exponential sums in several variables. We make a detailed study of the Kloosterman sum in seven variables. For this sum we determine its L-function (Theorem 3.12). As an application of this result we obtain a Weyl-type distribution for the signs of the Kloosterman sum (Theorem 3.17).

We have included an introductory section (**Chapter 0**) that serves to set down the notation and basic definitions in the classical theory of exponential sums.

Exponential Sums in One Variable: A Survey

The main purpose of this chapter is to introduce the basic definitions and to set down the notation which will be used in the rest of the thesis. We briefly survey some of the results in the classical theory of exponential sums and their associated zeta and L-functions.

0.1 On Exponential Sums

In this introduction we want to present in an elementary way, the theory of exponential sums in one variable. This presentation is based on [26], [1] and [11].

Let $\mathbf{F}_q$ be a finite field of q elements and let $\mathbf{F}_{q^n}$ be a finite extension of $\mathbf{F}_q$ of degree n. We consider the field $\mathbf{F}_q(T)$ of rational functions in one transcendental T, with coefficients in $\mathbf{F}_q$, geometrically, this is the function field, over the ground field $\mathbf{F}_q$, of the projective line. We consider finite divisor on the projective line $\mathbf{P}^1$, i.e., a divisor of $\mathbf{F}_q(T)$ is an element of the free abelian group generated by the set closed points of $\mathbf{P}^1$. We say a divisor

is finite, if it does not contain the point at infinity with a non-zero coefficient. A non-zero divisor is positive if all the coeficients are greater than or equal to 0. We have one to one correspondence between finite positive divisors on $\mathbf{P}^1$ and ideals of $\mathbf{F}_q[T]$. For every positive finite divisor D, we attach the polynomial $P_D(T) = T^n + \cdots + a_n$ which generates the corresponding ideal, i.e., whose zeros are the points in D, with multiplicities respectively equal to their coefficients in D. An arbitrary finite divisor D can be expressed as a difference of two positive divisors $D = D_0 - D_\infty$; under the correspondence of $D_0 \leftrightarrow I_0$ and $D_\infty \leftrightarrow I_\infty$, we can associate D to the rational function

$$f_D(T) = \frac{P_{I_0}(T)}{P_{I_\infty}(T)}.$$

Let $D = \sum_v m_v P_v$ be a finite divisor of $\mathbf{P}^1$ and let f be a rational function in $\mathbf{F}_q(T)$ such that $supp(D) \bigcap supp(f) = \emptyset$. The value of f at D is defined by the expression

$$f(D) = \prod_v f(P_v)^{m_v},$$

where for a closed point P of degree d, $f(P) = N_{\mathbf{F}_{q^d}/\mathbf{F}_q}(\xi)$ and ξ is an element in $\mathbf{F}_{q^d}$ corresponding to P. Equivalently, if P corresponds to the polynomial $T^d + \cdots + a_d = \prod_{i=1}^{d}(T - \xi_i)$, then

$$f(P) = \prod_{i=1}^{d} f(\xi_i).$$

Let χ be a multiplicative character of $\mathbf{F}_q^*$. We fix a finite positive divisor $\mathcal{F}_0 = \sum_v a_v P_v$ and we assume that no a_n is a multiple of the order of χ.

Let $\omega : \mathbf{F}_q((T))^* \longrightarrow \mathbf{C}$ be a multiplicative character of $\mathbf{F}_q((T))$, where $\mathbf{F}_q((T))$ is the field of formal power series. We assume that $\omega(aT) = 1$ for every $a \in \mathbf{F}_q^*$. Note that $\mathbf{F}_q((T)) = \mathbf{F}_q((\frac{1}{T}))$ and $\mathbf{F}_q((\frac{1}{T}))$ is the completion of $\mathbf{F}_q(T)$ at infinity. Note that ω can ramify only at infinity. We have that $\mathbf{F}_q((T)) \cong \{T^{\mathbf{Z}}\} \times U$ where $\{T^{\mathbf{Z}}\}$ is the cyclic group generated by T and U is the subgroup of invertible power series in $\frac{1}{T}$, i.e.,

$$U = \{f \in \mathbf{F}_q((\frac{1}{T})) \mid f = a_0 + \frac{a_1}{T} + \cdots \text{ where } a_0 \neq 0\}.$$

We define $U_n = \{f \in U \mid f \equiv 1 \bmod \frac{1}{T^n}\}$. Therefore, we have the following filtration:

$$U \supseteq U_1 \supseteq \cdots U_n \supseteq \cdots \supseteq 1.$$

The family $\{U_n\}_{n \in \mathbf{N}}$ forms a complete system of neighborhood of 1 and U is a compact group under the induced topology. Now we can talk about continuous characters. We assume that $\omega : \mathbf{F}_q((T))^* \simeq \mathbf{F}_q^* \times \{T^{\mathbf{Z}}\} \times U_1 \longrightarrow \mathbf{C}$ is a continuous character. Therefore, by continuity, we have that $\omega(U_n) = 1$ for some n.

Definition 0.1. *Let* $\mathbf{L/K}$ *be a finite Galois extension with Galois group* G *and let* $\mathbf{K}$ *be a local field. Let* χ *be a character of a representation of* G*. The conductor of* χ *is defined by :*

$$\mathcal{F}(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0}(\chi(1) - \chi(G_i)),$$

where g_i is the order of the i-th ramification group G_i of G and $\chi(G_i) = \frac{1}{g_i}\sum_{s\in G_i}\chi(s)$.

Definition 0.2. *The ideal $(\frac{1}{T^n})$ in $\mathbf{F}_q[\frac{1}{T}]$ is called the conductor of ω if $\omega(f) = 1$ for every $f \in U_n$ and n is the smallest integer with that property. The integer n is called the exponential conductor of ω.*

The class field theory gives the equivalence of the two definitions above. In our case we have $ker(\omega) = \mathbf{F}_q \times \{T^{\mathbf{Z}}\} \times U_n$, therefore

$$\mathbf{F}_q((T))^*/ker(\omega) \cong U_1/U_n.$$

We can conclude that the values of ω are p^s-roots of unity for some positive integer s. Recall

$$G_i/G_{i+1} \hookrightarrow U_i/U_{i+1} \cong P^i/P^{i+1},$$

where P is the maximal ideal of $\mathbf{F}_q((T))$.

Let $\lambda(a) = \omega(\frac{1}{T} - a)$ for every $a \in \mathbf{F}_q$. Given a function $f \in \mathbf{F}_q((T))^* = \mathbf{F}_q((\frac{1}{T}))$, we expand it in terms of the local uniformizing parameter at infinity and denoted by $f(\frac{1}{T})$. For every finite divisor D whose support is disjoint from $\mathcal{F}_0$, we define a function

$$\Lambda(D) = \omega(f_D(\frac{1}{T}))\chi(f_D(\mathcal{F}_0)).$$

Note that Λ satisfies $\Lambda(D + D') = \Lambda(D)\Lambda(D')$.

Let n be the exponential conductor of ω. Abusing the notation we set

$\mathcal{F} = \mathcal{F}_0 + nP_\infty$. We define two subgroups of group of divisors $Div(\mathbf{P}^1)$:

$$Div(\mathcal{F}) = \{D \in Div(\mathbf{P}^1) \,|\, supp(D) \bigcap \mathcal{F} = \emptyset\}$$

and

$$Div_0(\mathcal{F}) = \{D = (f) \,|\, f \in \mathbf{F}_q(T)^*, f(\frac{1}{T}) \equiv 1 \bmod \frac{1}{T^n}, f(P_v) = 1 \text{ for every } P_v \in supp(\mathcal{F})\}.$$

Let $Cl_{\mathcal{F}}(\mathbf{P}^1) = Div(\mathcal{F})/Div_0(\mathcal{F})$. $Cl_{\mathcal{F}}(\mathbf{P}^1)$ is a finite group. Λ defines a character

$$\Lambda : Cl_{\mathcal{F}}(\mathbf{P}^1) \longrightarrow \mathbf{C},$$

since Λ is trivial on $Div_0(\mathcal{F})$. Note that the multiplicities a_v in the divisor $\mathcal{F}_0$ do not enter in the definition of $Cl_{\mathcal{F}}(\mathbf{P}^1)$.

Definition 0.3. *The L-function of the projective line $\mathbf{P}^1/\mathbf{F}_q$ corresponding to the character $\Lambda : Cl_{\mathcal{F}}(\mathbf{P}^1) \longrightarrow \mathbf{C}$ is defined by*

$$L(t, \Lambda, \mathbf{P}^1) = \sum_D \Lambda(D) t^{deg(D)} = \prod_P (1 - \Lambda(P) t^{deg(P)})^{-1},$$

where the summation is taken over all finite positive divisors D with $supp(D) \bigcap \mathcal{F} = \emptyset$ and the product is taken over all closed points $P \notin supp(\mathcal{F})$.

In general, the definition of the L-function and the zeta function of a non-singular curve X are given as follows.

Definition 0.4. *Let χ be a character of $Div(X)$, then the L-function asso-*

ciated to the character χ is defined by the Euler product

$$L(t, X, \chi) = \prod_P (1 - \chi(P) t^{deg(D)})^{-1},$$

where the product runs over all closed points $P \in Div(X)$ whose support is disjoint of the conductor of χ.

Definition 0.5. *The Zeta function of the non-singular curve $X/\mathbf{F}_q$ is defined by*

$$Z(t, X) = \sum_D t^{deg(D)},$$

where the sum is taken over all positive divisors D in $Div(X)$.

Some Remarks about L-functions and Zeta functions.

1. The L-function associated to χ can be represented by a polynomial of degree $2g - 2 + \mathcal{F}(\chi)$ where g is the genus of X and $\mathcal{F}(\chi)$ is the degree of the conductor of χ.

2. Let X be a complete non-singular curve defined over $\mathbf{F}_q$ with function field $\mathbf{K}$ and suppose that $\mathbf{F}_q$ is the field of constants of $\mathbf{K}$. We denote the genus of the curve X by g. We have the following results:

A. The degree map induces an exact sequence

$$0 \longrightarrow Cl_0(X) \longrightarrow Cl(X) \xrightarrow{deg} \mathbf{Z} \longrightarrow 0$$

where $Cl(X)$ is the group of divisor classes of X and $Cl_0(X)$ is group of divisor classes of degree 0 of X.

B. The zeta function of X can be represented in the form

$$Z(t,X) = \frac{L(t)}{(1-t)(1-qt)},$$

where $L(t)$ is a polynomial in $\mathbf{Z}[t]$ of degree $2g$ with $L(0) = 1$ satisfying

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

C. The residue of $Z(t,X)$ at $t = 1$ is $h(X) = L(1)$ where $h(X)$ is the number of divisor classes of X of degree 0.

D. (Riemann Hypothesis) The reciprocal roots $\alpha_1, \cdots, \alpha_{2g}$ of the numerator of

$$Z(t,X) = \frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-qt)}$$

all satisfy $|\alpha_i| = q^{1/2}$ for $1 \leq i \leq 2g$.

The proof of the above remarks about L-functions and zeta functions can be found in [11, chapter 3].

By class field theory, there is an abelian covering $X \longmapsto \mathbf{P}^1$ of the projective line, i.e., there is a finite separable extension $\mathbf{K}$ of $\mathbf{F}_q(T)$ with Galois group isomorphic to $Cl_{\mathcal{F}}(\mathbf{P}^1)$ having the curve X as a model. That gives us the following equality:

$$Z(t,X) = Z(t,\mathbf{P}^1)\prod_{\Lambda_i} L(t,\Lambda_i,\mathbf{P}^1), \tag{0.1}$$

where the product is taken over all non-trivial characters of $G(X/\mathbf{P}^1)$, one of which is the original character Λ. Since the genus of $\mathbf{P}^1$ is 0, then

$$deg(Z(t,\mathbf{P}^1)) = deg(\prod_{\Lambda_i} L(t,\Lambda_i,\mathbf{P}^1)) = \sum_{\Lambda_i}(\mathcal{F}(\Lambda_i)-2),$$

where the $\mathcal{F}(\Lambda_i)$ is the degree of the conductor of Λ_i. Using the property (1) of remarks about of L-functions and zeta functions we have

$$deg(L(t,\Lambda,\mathbf{P}^1)) = 2(0)+\mathcal{F}(\Lambda)-2 = \mathcal{F}(\Lambda)-2 = d+n-2,$$

where d is the number of distinct closed points of $\mathcal{F}_0$. From (0.1) and the Riemann hypothesis, we get that

$$L(t,\Lambda,\mathbf{P}^1) = \sum_D \Lambda(D)t^{deg(D)} = \prod_{i=1}^{d+n-2}(1-\alpha_i t),$$

where $|\alpha_i| = q^{1/2}$. Therefore we obtain

$$\sum_{deg(D)=1}\Lambda(D) = -\sum_{i=1}^{d+n-2}\alpha_i$$

where the sum is taken over all divisors D defined over $\mathbf{F}_q$ of degree 1 and $D \notin supp(\mathcal{F})$. But we have one to one correspondence between finite positive divisors D defined over $\mathbf{F}_q$ of degree 1 and polynomials of degree one $P_D(T) = T-a$ for some $a \in \mathbf{F}_q$. We have

$$f_D(\frac{1}{T}) = P_D(\frac{1}{T}) = (\frac{1}{T}-a)$$

then

$$\lambda(a) = \omega(\frac{1}{T}-a) = \omega(f_D).$$

We also have

$$f_D(\mathcal{F}_0) = \prod_v (\xi_v - a)^{a_v} = (-1)^m f_{\mathcal{F}_0}(a)$$

where $m = \sum_v a_v$, therefore we obtain

$$\begin{aligned}\sum_{deg(D)=1} \Lambda(D) &= \sum_{deg(D)} \omega(f_D(\frac{1}{T}))\chi(f_D(\mathcal{F}_0)) \\ &= \sum_{a\in\mathcal{F}}{}' \lambda(a)\chi((-1)^m f_{\mathbf{F}_0}(a)) \\ &= -\chi(-1)^m\Big(\sum_{i=1}^{d+n-2} \alpha_i\Big),\end{aligned}$$

where the second sum of right side is taken over all closed points corresponding to the polynomials $T - a$ for $a \in \mathbf{F}_q$, except those, if any is contained in $supp(\mathcal{F}_0)$. We extend the sum to all closed points defined over $\mathbf{F}_q$ by setting $\chi(0) = \chi(\infty) = 0$.

Theorem 0.6. (Weil's Estimate) *With the above notation, we have*

$$|\sum_{a\in\mathcal{F}} \lambda(a)\chi(f_{\mathcal{F}_0}(a))| \leq (d+n-2)q^{1/2}.$$

Proof. Apply the Riemann hypothesis to the above discussion.

Example 1.

Let $\omega : U_1 \longmapsto \mathbf{C}^*$ be the character defined by :

$$\omega(1 + a_1T + a_2T^2 + \cdots) = -\psi(a_1),$$

where $\psi : \mathbf{F}_q^+ \longmapsto \mathbf{C}^*$ is an additive character of $\mathbf{F}_q$. Note that the conductor of ω is 2, therefore

$$|\sum_{a\in\mathbf{F}_q} \psi(a)\chi(f_{\mathbf{F}_0}(a))| \leq dq^{1/2}.$$

Example 2.

If $char(\mathbf{F}_q) \neq 2$, then we can take $f_{\mathcal{F}_0}(T) = T^2 - b$ with $b \in \mathbf{F}_q^*$. Then we obtain

$$|\sum_{a\in\mathbf{F}} \psi(a)\chi(a^2 - b)| \leq 2q^{1/2}$$

since $d = 2$.

Claim. If we take χ equal to the quadratic character of $\mathbf{F}_q^*$, then

$$\sum_{a\in\mathbf{F}_q} \psi(a)\chi(a^2 - b) = \sum_{a\in\mathbf{F}_q^*} \psi(ca + da^{-1}),$$

where $4cd = b$.

Proof. If $c = 0$ or $d = 0$, then the above equality is clear. For $cd \neq 0$ we can write

$$\sum_{a\in\mathbf{F}_q^*} \psi(ca + da^{-1}) = \sum_{r\in\mathbf{F}_q} \psi(r)N(r),$$

where $N(r)$ is the number of $a \in \mathbf{F}_q^*$ with $ca + da^{-1} = r$. This equation is equivalent to the quadratic equation $ca^2 - ra + d = 0$. Hence $N(r) = 2, 1$ or 0 depending on whether $\chi(r^2 - 4dc) = 1, 0$ or -1. That implies $N(r) = 1 + \chi(r^2 - 4dc)$. Then we have

$$\begin{aligned}\sum_{a\in\mathbf{F}_q^*}\psi(ca+da^{-1}) &= \sum_{r\in\mathbf{F}_q}\psi(r)N(r)\\ &= \sum_{r\in\mathbf{F}_q}(1+\chi(r^2-4dc))\psi(r)\\ &= \sum_{r\in\mathbf{F}_q}\psi(r)+\sum_{r\in\mathbf{F}_q}\psi(r)\chi(r^2-4dc)\\ &= 0+\sum_{r\in\mathbf{F}_q}\psi(r)\chi(r^2-b).\end{aligned}$$

This completes the proof of the claim.

Lemma 0.7. *Let $\psi : \mathbf{F}_q^+ \longmapsto \mathbf{C}^*$ be a non-trivial additive character. Let f be a polynomial in $\mathbf{F}_q[T]$ of degree d with $f(0) = 0$. Then, there exists at least one character $\omega : U_1 \longmapsto \mathbf{C}^*$ of order p , of conductor $(\frac{1}{T^n})$ for some $n \leq d+1$ such that*

$$\omega(1+\frac{a}{T}) = \psi(f(a)).$$

The proof can be found in [11, chapter 4.6] or [26].

Corollary 0.8. *Let $\psi : \mathbf{F}_q^+ \longmapsto \mathbf{C}^*$ be a non-trivial additive character. Let f be a polynomial in $\mathbf{F}_q[T]$ of degree d with $f(0) = 0$. Then we have*

$$|\sum_{a\in\mathbf{F}_q}\psi(f(a)) \leq (d-1)q^{1/2}.$$

Example 3.

Let ψ be a non-trivial additive characters of $\mathbf{F}_q$, $n \in \mathbf{N}$ and χ a multiplicative character of $\mathbf{F}_q^*$ of order $d = gcd(n, q-1)$. Then, we have

$$\sum_{a \in \mathbf{F}_q} \psi(ca^n + b) = \psi(b) \sum_{j=1}^{d-1} \chi^j(a) G(\overline{\chi^j}, \psi),$$

where $b \in \mathbf{F}_q$ and $c \neq 0$ and $G(\overline{\chi^j}, \psi)$ is the Gauss sum defined by ψ and χ.

Proof. Let τ be additive character of $\mathbf{F}_q$ defined by $\tau(a) = \psi(ca)$. Then

$$\sum_{a \in \mathbf{F}_q} \psi(ca^n + b) = \psi(b) \sum_{a \in \mathbf{F}_q} \tau(a^n).$$

We express $\tau(a^n)$ as

$$\tau(a^n) = \frac{1}{q-1} \sum_{\lambda} G(\overline{\lambda}, \tau) \lambda(a^n)$$

for $a \in \mathbf{F}_q$, where the sum is over all the multiplicative characters of $\mathbf{F}_q^*$. Therefore, we obtain

$$\sum_{a \in \mathbf{F}_q} \tau(a^n) = 1 + \frac{1}{q-1} \sum_{\lambda} G(\overline{\lambda}, \tau) \sum_{a \in \mathbf{F}_q^*} \lambda^n(a).$$

The inner sum in the last expression is equal to $q-1$ if λ^n is trivial and 0 otherwise. But λ^n is trivial if and only if the order of λ divides d. Since the order of $\overline{\chi}$ is d, the characters λ with order dividing d are $\lambda = \overline{\chi}^j$ with $j = 0, \ldots, d-1$. Then, we obtain the following:

$$\sum_{a \in \mathbf{F}_q} \tau(a^n) = 1 + \sum_{j=0}^{d-1} G(\chi^j, \tau) = \sum_{j=1}^{d-1} G(\chi^j, \tau).$$

This completes the proof of the example 3.

The following are some consequences of example 3.

1. If ψ is non-trivial additive character of $\mathbf{F}_q$ and $gcd(n, q-1) = 1$, then

$$\sum_{a \in \mathbf{F}_q} \psi(ca^n + b) = 0.$$

2. If ψ is non-trivial additive character of $\mathbf{F}_q$ and $gcd(n, q-1) = n$, then the function $a \mapsto \psi(ca^n + b)$ is a character of conductor $n + 1$.

Proof. By example 3, $\sum_{a \in \mathbf{F}_q} \psi(ca^n + b)$ is the sum of $n - 1$ Gauss sums. We know that any Gauss sum has absolute value equal to $q^{1/2}$. Hence, from Weil estimate we get

$$n - 1 \leq cond(\psi) - 2 \leq n + 1 - 2 \text{ then } cond(\psi) = n + 1.$$

From now on, we consider exponential sums of this type :

$$S_n(f) = \sum_{a \in \mathbf{F}_{q^n}} \psi(Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(f(a))),$$

where $\psi(a) = e^{2\pi i Tr_{\mathbf{F}_q/\mathbf{F}_p}(a)/p}$ and $f(T) \in \mathbf{F}_q[T]$. Let $L(t, f)$ be the function defined by :

$$L(t, f) = \exp\{\sum_{n=1}^{\infty} \frac{S_n(f)t^n}{n}\} \text{ for } |t| < \frac{1}{q}.$$

Therefore, we have

$$(0.2) \quad L(t, f) = \exp\{\sum_{n=1}^{\infty} \frac{S_n(f)t^n}{n}\} = \prod_P (1 - \psi(Tr(f(P)))t^{deg(P)})^{-1},$$

where the product is taken over all finite closed points of $\mathbf{P}^1$ and if $deg(P) = n$, then $Tr(f(P)) = Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(f(P))$.

Lemma 0.9. *Let $f(T)$ be a polynomial in $\mathbf{F}[T]$, defined over $\mathbf{F}_q$ of degree d, $gcd(d,p) = 1$, then*

$$S_n(f) = -\sum_{n=1}^{d-1} \theta_i^n, \text{ where } |\theta_i| = q^{n/2}.$$

If $gcd(d,p) = p$, then

$$S_n(f) = -\sum_{n=1}^{l} \theta_i^n, \text{ where } |\theta_i| = q^{n/2} \text{ and } l < d-1.$$

Proof. By Weil's estimate, we have $S_n(f) = -\sum_{i=1}^{l} \theta_i^n$, where $l \leq d-1$ and $|\theta_i| = q^{1/2}$, provided only that $f(T) \neq h(T)^p - h(T)$ for every polynomial $h(T)$ defined over $\mathbf{F}_q^{sep}$. Note that the last condition is satisfied if $gcd(d,p) = 1$. Let $L(t,f) = \sum_{m=1}^{l} A_m t^m$, we will prove that $A_{d-1} \neq 0$, therefore $l = d-1$. By the equation (0.2), we have

$$A_m = \sum_{D} \psi(Tr(f(D))),$$

where the summation is taken over all finite positive divisors of degree m. The positive divisors $D = \sum_v a_v P_v$ of degree m are in one to one correspondence with the polynomials of degree m over $\mathbf{F}_q$, i.e.,

$$\{D \mid deg(D) = m \text{ and } D \geq 0\} \longleftrightarrow \{G(T) \in \mathbf{F}_q[T] \mid deg(G) = m\}.$$

Therefore, we have the following:

$$A_m = \sum_{G(T)} \psi(Tr(\sum_{i=1}^{m} f(\lambda_i))), \tag{0.3}$$

where the sum is taken over all monic polynomials $G(T) = T^m + y_1 T^{m-1} + \cdots + y_m = \prod_{i=1}^{m}(T - \lambda_i)$ in $\mathbf{F}_q[T]$ of degree m. (0.3) is true since

$$\begin{aligned}\omega(G(\frac{1}{T})) &= \omega(\prod_{i=1}^{m}(\frac{1}{T} - \lambda_i) \\ &= \prod_{i=1}^{m}\omega(\frac{1}{T} - \lambda_i) \\ &= \prod_{i=1}^{m}\psi(f(\lambda_i)) \\ &= \psi(\sum_{i=1}^{m} f(\lambda_i))\end{aligned}$$

and $\Lambda(D) = \omega(f_D(\frac{1}{T}))$. Note that $\sum_{i=1}^{m} f(\lambda_i) \in \mathbf{F}_q$ since if $f(T) = a_0 T^d + \cdots + a_d$ then $\sum_{i=1}^{d} f(\lambda_i) = a_d S_d + a_{d-1} S_{d-1} + \cdots + a_d + S_0$, where $S_j = \sum_{i=1}^{m} \lambda_i^j$ but the S_j can be written in terms of the coefficients of G.

We take $m = d - 1$, then $G(T) = T^{d-1} + y_1 T^{d-1} + \cdots + y_{d-1}$. $[\frac{d}{2}]$ denotes the integer part of $\frac{d}{2}$. Using the Newton and Waring formulas for elementary symmetric functions, we get

$$\sum_{i=1}^{d-1} f(\lambda_i) = a_0 \sum_{1 \le m < \frac{d}{2}} y_{d-m}(dy_m + P_m(y_1, \ldots, y_{m-1})) + Q(y_1, \ldots, y_{[\frac{y}{2}]}),$$

where $a_0 \neq 0$ and Q is a polynomial in $y_1, \ldots, y_{[\frac{d}{2}]}$ which is quadratic in $y_{[\frac{d}{2}]}$ if d is even.

Remark: Waring formula for elementary symmetric functions.

Let $H(T) = T^l + a_1 T^{l-1} + \cdots + a_l = \prod_{i=1}^{l}(T - \alpha_i)$ and $S_m = \sum_{i=1}^{l} \alpha_i^m$.

The Waring formula is stated as follows:

$$S_m = \sum_{\substack{(r_1,\cdots,r_l) \\ r_1+2r_2+\cdots+lr_l=m \\ r_1+r_2+\cdots+r_l=r}} (-1)^r \frac{m(r_1+\cdots+r_l-1)!}{r_1!\ldots r_l!} y_1^{r_1} y_2^{r_2} \ldots y_l^{r_l}.$$

Then, the sum $a_0 \sum_{1\le m<\frac{d}{2}} y_{d-m}(dy_m + P_m(y_1,\ldots,y_{m-1})) + Q(y_1,\ldots,y_{[\frac{y}{2}]})$ is linear in $y_{[\frac{d}{2}]+1},\ldots y_{d-1}$. If we substitute the expression of $\sum_{i=1}^{d-1} f(\lambda_i)$ in (0.3), then we get

$$\begin{aligned}\sum_{G(T)=0} \psi(Tr(\sum_{i=1}^{d-1} f(\lambda_i)) &= \sum_{G(T)=0} \psi(a_0 \sum_{1\le m<\frac{d}{2}} y_{d-m}(dy_m - P_m(y_1,\ldots,y_{m-1})) \\ &\quad +Q(y_1,\cdots,y_{[\frac{d}{2}]}) \\ &= \sum_{(y_1,\ldots,y_{d-1})} \psi(a_0 \sum_{1\le m<\frac{d}{2}} y_{d-m}(dy_m - P_m(y_1,\ldots,y_{m-1})) \\ &\quad +Q(y_1,\cdots,y_{[\frac{d}{2}]}).\end{aligned}$$

If d is odd, then $[\frac{d}{2}] = \frac{d-1}{2}$. Therefore the above expression becomes

$$\begin{aligned}\sum_{G(T)=0} \psi(Tr(\sum_{i=1}^{d-1} f(\lambda_i)) &= \sum_{(y_1,\ldots,y_{\frac{d-1}{2}})} \psi(Tr(Q(y_1,\ldots y_{\frac{d-1}{2}}))) \times \cdots \\ &\quad \times \sum_{y_{\frac{d+1}{2}}} \psi(Tr(a_0 y_{\frac{d+1}{2}}(dy_{\frac{d-1}{2}} + P_m(y_1,\ldots,y_{\frac{d-3}{2}})))) \times \ldots \\ &\quad \times \sum_{y_{d-2}} \psi(Tr(a_0 y_{d-2}(dy_2 + P_2(y_1)))) \\ &\quad \times \sum_{y_{d-1}} \psi(Tr(a_0 y_{d-1}(dy_1 + P_1))).\end{aligned}$$

The sum over y_{d-1} is zero unless the coefficient of y_{d-1} is zero. As the coefficient of y_{d-1} is equal to $a_0(dy_1 + P_1)$ with constant P_1, we see the sum over y_{d-1} is 0 unless $y_1 = -\frac{P_1}{d}$. We take $y_1 = -\frac{P_1}{d}$, then the contribution

of $\sum_{y_{d-1}}$ is equal to q. The term with $m = 2$ is again zero unless $a_0(dy_2 + P_2(-\frac{P_1}{d}) = 0$. We take $y_2 = -d^{-1}P_2(\frac{-P_1}{d})$, then the contribution of $\sum_{y_{d-2}}$ is equal to q. We continue until $m = \frac{d-1}{2}$, then the total contribution is

$$\sum_D \psi(Tr(f(D)) = q^{d-1/2}\zeta_p^a,$$

where summation is over all divisor D of degree $d-1$ and $\zeta_p = e^{2\pi i/p}$. If d is even, then

$$\begin{aligned}
\sum_{G(T)=0} \psi(Tr(\sum_{i=1}^{d-1} f(\lambda_i)) &= \sum_{(y_1,\ldots,y_{\frac{d}{2}})} \psi(Tr(Q(y_1,\ldots y_{\frac{d-1}{2}}))) \times \cdots \\
&\quad \times \sum_{y_{\frac{d}{2}+1}} \psi(Tr(a_0 y_{\frac{d}{2}+1}(dy_{\frac{d}{2}-1} + P_m(y_1,\ldots,y_{\frac{d}{2}-2})))) \times \ldots \\
&\quad \times \sum_{y_{d-2}} \psi(Tr(a_0 y_{d-2}(dy_2 + P_2(y_1)))) \\
&\quad \times \sum_{y_{d-1}} \psi(Tr(a_0 y_{d-1}(dy_1 + P_1))) \\
&= q^{(d/2)-1} \sum_{y_{\frac{d}{2}}} \psi(Tr(Q'(y_{\frac{d}{2}}))),
\end{aligned}$$

where Q' is a quadratic polynomial in $y_{\frac{d}{2}}$. By the example 3, we have that $\sum_{\frac{d}{2}} \psi(Tr(Q'(y_{\frac{d}{2}})))$ is a Gauss sum. Therefore, we get in both cases the total contribution of the above sum when y_i's range over all values of $\mathbf{F}_q$ is $A_{d-1} = \epsilon(f)q^{(d-1)/2}$ where $\epsilon(p)$ has absolute value 1.

Remark. The above procedure provides a method for the study of the root number $\epsilon(f)$ in many cases of interest.

For the second part of the lemma 0.9, note that $Tr(a) = Tr(a^p)$. We may assume that $gcd(d,p) = 1$ since if $F(T) = f(T) + h(T)^p - h(T)$ for $h(T) \in$

$\mathbf{F}_q[T]$, then $S_n(f) = S_n(F)$. Therefore, if $gcd(d,p) = p$, then $deg(L(t,f)) < d-1$.

Examples 4.

1. $L(t, x^7 + x, 2) = 1 + 2t + 2t^2 + 6t^3 + 8t^4 + 8t^5 + 8t^6$.

2. $L(t, x^7 + x, 3) = (3t^2 + 1)(9t^4 + 1)$.

3.

$$L(t, x^7 + x, 5) = 1 + (\frac{5 - \sqrt{5}}{2})t + (\frac{15 - \sqrt{5}}{2})t^2 + \frac{-15 + 25\sqrt{5}}{2})t^3 + (\frac{-25 + 75\sqrt{5}}{2})t^4 + (\frac{125 - 25\sqrt{5}}{2})t^5 + 125t^6.$$

0.2 Artin-Schreier Coverings of Curves

Let X be a complete non-singular curve of genus g, defined over $\mathbf{F}_q$ and let $\mathbf{K}$ be its function field. Let $\mathbf{KF}_q^{sep}$ be the function field of X considered as a curve over $\mathbf{F}_q^{sep}$. Let $f \in K$ be a rational function of X satisfying the condition $f \neq h^p - h$ for every $h \in \mathbf{KF}_q^{sep}$. Let P_v be a closed point of X of degree n . Let T_v be the local uniformizing parameter of P_v and let ord_v be the exponential valuation of P_v. We say f has a pole at P_v, if $ord_v(f) < 0$, otherwise the value of f at P_v is defined to be a_0, where $f = \sum_{i \geq 0} a_i T_v^i$, $a_i \in \mathbf{F}_{q^n}$. If $\mathbf{k}_v$ is a finite extension of $\mathbf{F}_q$ with absolute trace $Tr_{\mathbf{k}_v/\mathbf{F}_p}(x) = x + x^p + \cdots + x^{p^{deg(\mathbf{k}_v)-1}}$, then we define the character

$$\psi_{\mathbf{k}_v}(x) = e^{2\pi i Tr_{\mathbf{k}_v/\mathbf{F}_p}(x)/p}.$$

We can define a multiplicative character on the group of divisors of X, i.e., $\Lambda : Div(X) \longrightarrow \mathbf{C}^*$, whose support is disjoint from the poles of f by setting

$$\Lambda(P_v) = \psi_{\mathbf{k}_v}(F(P_v)) = e^{2\pi i Tr_{\mathbf{k}_v/\mathbf{F}_p}(f(P_v))/p},$$

where P_v is a closed point of X and $\mathbf{k}_v$ is the residue field of $\mathbf{K}$ at P_v. Let X_m be the set of points of X defined over $\mathbf{F}_q$ and let

$$S_n(X, f) = \sum_{x \in X_n} e^{Tr_{\mathbf{F}_{q^n}/\mathbf{F}_p}(f(x))},$$

where the poles of f are excluded from the summation. This exponential sum is related to an Artin-Schreier covering of X. Let $\mathbf{K}'$ be a normal extension of $\mathbf{K}$ obtained by adjoining to $\mathbf{K}$ the roots of the equation $z^p - z = f$. Let X' be the smooth model corresponding to $\mathbf{K}'$. The covering

$$\pi : X' \longrightarrow X$$

is called the Artin-Schreier covering associated with the function f.

Definition 0.10. *The L-function associated to the Artin-Schreier covering $\pi : X' \longrightarrow X$ is defined to be*

$$L(t, f, X) = \exp\{\sum_{n=1}^{\infty} \frac{S_n(X, f)t^n}{n}\}.$$

Let $(f)_\infty$ be the divisor of poles of f on X, and we write

$$(f)_\infty = \sum_{i=1}^{l} d_i P_{v_i}.$$

Theorem 0.11. *With the above notation, we have*

$$S_n(X,f) = -\sum_{i=1}^{d} \theta_i^n, \quad \textit{where } |\theta_i| = q^{n/2}$$

and $d \leq 2g - 2 + deg((f)_\infty)$. *Moreover, we have* $d = 2g - 2 + l + deg((f)_\infty)$ *if and only if* $gcd(d_i, p) = 1$ *for* $i = 1, \ldots l$.

Proof. The first part of the theorem is a general result of the Artin L-function. To prove the second part of the theorem, we need to find the exponential conductor of the character ψ. Let $\mathbf{Q}(\zeta_p)$ be a cyclotomic extension obtained by adjoining $\zeta_p = e^{2\pi i/p}$ to $\mathbf{Q}$. Note that $L(t,f,X) \in \mathbf{Q}[t]$. If $d = deg(L(t,f,X))$, then the degree of any other conjugate of $L(t,f,X)$ is d. Note that $Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ is isomorphic to $(\mathbf{Z/pZ})^*$. If $\sigma \in Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, then $\sigma(\zeta_p) = \zeta_p^i$ for some $i \in (\mathbf{Z/pZ})^*$. Using the correspondence $\sigma \mapsto i$ we get that

$$\sigma L(t,\Lambda,X) = L(t,\Lambda^i,X),$$

where σ acts on the coefficient of $L(t,\Lambda,X)$. Note that

$$\begin{aligned} N_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(L(t,\Lambda,X)) &= \prod_{\sigma \in G(\mathbf{Q}(\zeta_p)/\mathbf{Q})} \sigma L(t,\Lambda,X) \\ &= \prod_{i=1}^{p-1} L(t,\Lambda^i,X) \\ &= \frac{Z(X',t)}{Z(X,t)}. \end{aligned}$$

By Riemann hypothesis, if X is a complete non-singular curve of genus g, then the degree of $Z(X,t)$ is $2g-2$. If g' and g denote the genus of X' and

X, respectively, we get from the above equation

$$(p-1)d = 2g' - 2 - (2g-2). \tag{0.4}$$

In order to estimate g', we need to use the Hurwitz formula for the covering $\pi : X' \longrightarrow X$. Let P_v be a point of X and suppose that $\pi(P_w) = P_v$. We denote the completion of $\mathbf{K}$ and $\mathbf{K}'$ at P_v and P_w as $\mathbf{K}_v$ and $\mathbf{K}'_w$, respectively. Since $deg(\mathbf{K}'/\mathbf{K}) = p$ then $G(\mathbf{K}'_w/\mathbf{K}_v) \simeq \mathbf{Z/p}$ or 0. The covering π can ramify only at the poles P_{v_i} of f, and if $gcd(d_i, p) = 1$ there is ramification and the ramification index is p (see [11, chapter 4.6]). Hence, in order to apply the Hurwitz formula we need to consider the ramification groups at various points P_w. We denote the decomposition group of G at P_w as $D(P_w)(= G(\mathbf{K}'_w/\mathbf{K}_v))$. Using the Hurwitz formula we get

$$2g' - 2 = p(2g-2) + \sum_{P_w} \sum_{i=1}^{\infty} (|G_i(P_w)| - 1),$$

where the summation is taken over all the closed points $P_w \in X'$ lying above the poles of f and $G_i(P_w)$ is the i-th ramification group of G at P_w.

Suppose that the covering $\pi : X' \longrightarrow X$ is ramified at the pole P_v of f with $ord_{P_v} = -s$; let P_w be a closed point lying above P_v, therefore $G_i = G$ or 0. Recall that $-s = d_i$ for some $i \in \{1, 2, \ldots, l\}$. By definition $G_i(P_w) = G$ if and only if $ord_{P_w}(\sigma(T_{P_w}) - T_{P_w}) \geq i + 1$, where T_{P_w} is the local uniformizing parameter of K'_w. Hence, if P_{w_i} is a closed point lying above P_{v_i}, then

$$2g' - 2 \leq (2g-2) + \sum_{i=1}^{l} (ord_{P_{w_i}}(\sigma(T_{P_{w_i}}) - T_{P_{w_i}}))(p-1)$$

and equality holds if and only if $gcd(d_i, p) = 1$ for every $i = 1 \ldots l$. In order to prove the theorem 0.11, we need to prove if $\sigma \in G$ and $\sigma \neq id$, then $ord_{P_{w_i}}(\sigma(T_{w_i}) - T_{w_i}) \leq d_i + 1$ with the equality if $gcd(p, d_i) = 1$. If $ord_{P_{w_i}}(\sigma(T_{w_i}) - T_{w_i}) \leq d_i + 1$ for $i \in \{1 \ldots l\}$ then

$$\begin{aligned} 2g' - 2 &\leq p(2g-2) + \sum_{i=1}^{l}(d_i + 1)(p-1) \\ d &\leq (2g-2) + l + \sum_{i=1}^{l} d_i \end{aligned}$$

with equality above if $gcd(p, d_i) = 1$ for every i. We have applied (0.4).

Now we are going to prove $ord_{P_{w_i}}(\sigma(T_{w_i}) - T_{w_i}) \leq d_i + 1$ for $i = 1, \ldots, l$ and $\sigma \neq id$. The question here is local, note that the extension $\mathbf{K}'_w/\mathbf{K}_v$ is defined by the Artin-Schreir $z^p - z = a$ where $a \in \mathbf{K}_v$. We are going take advantage of the useful fact that in a neighborhood of a simple point, the curve looks like the projective line. We can think of the point P_v as a point at infinity, we can introduce a local uniformizing parameter $\frac{1}{T}$ for the valuation ord_{P_v}; so that the local field $\mathbf{K}_v$ is isomorphic to the field $\mathbf{F}(\frac{1}{T})$ of formal Laurent series in $\frac{1}{T}$ with coefficients in the field of constant of $\mathbf{K}$. Also, if $gcd(d, p) = 1$ we may choose T such that $a = T^d$. If $gcd(d, p) = p$, we can take $a = P(T)$, where $P(T)$ is polynomial in T of degree d. In this setting, we think of X as the projective line $\mathbf{P}^1$ over the field of constant of $\mathbf{K}$ and the function f is a polynomial in T of degree d. The covering $\pi' : X'' \longmapsto \mathbf{P}^1$ is defined by $z^p - z = T^d$ if $gcd(p, d) = 1$ and $z^d - z = P(T)$ if $gcd(p, d) > 1$. Let $P'_w \in X''$ be a point lying above P_∞. In this case $g = 0$, $l = 1$ and

$P_v = P_\infty$, then using the Hurwitz formula we get

$$(p-1)s' = 2g''$$

and

$$2g'' - 2 = -2p + ord_{P'_w}(\sigma(T_{P'_w}) - T_{P'_w})(p-1),$$

where g'' is the genus of the curve $z^p - z = T^d$ if $gcd(p,d) = 1$ and $z^d - z = P(T)$ if $gcd(p,d) > 1$. By the local character of the construction we have

$$ord_{P_w}(\sigma(T_w) - T_w) = ord_{P'_w}(\sigma(T'_w) - T'_w).$$

By lemma 0.9, we have $s' = s-1$ if $gcd(p,d) = 1$ and $s' < s-1$ if $gcd(d,p) = p$. Therefore, if $gcd(s,p) = 1$, then

$$(p-1)(s-1) = -2(p-1) + ord_{P'_w}(\sigma(T_{P'_w}) - T_{P'_w})(p-1).$$

Recall that $ord_{P_v}(f) = -s$. If we divide by $p-1$ in the above equality, we get

$$s + 1 = ord_{P'_w}(\sigma(T_{P'_w}) - T_{P'_w}).$$

This proves that $ord_{P_{w_i}}(\sigma(T_{P_{w_i}}) - T_{P_{w_i}}) = d_i + 1$ if and only if $gcd(d_i, p) = 1$. This completes the proof.

Chapter 1

Composites and Mixed Exponential Sums

In this chapter we compute all the possible filtrations for the ramification groups of the composite field of an Artin-Schreier and a cyclic extension of degree p^i for $i = 1, 2$. This calculation gives an easy method to compute the conductor associated to a character of the Galois group of such field extension. In addition, we calculate the conductor of a character that consists of the product of an additive and a multiplicative character. This computation improves the bound for exponential sums given by G.I. Perel'muter on [17, theorem 1].

1.1 Summary of Results for Ramification Groups

In this section we present all the facts that we need in the following sections. We follow the notation of [20]. The proof of all the theorems that we quote in this section can be found in [20, chapter 5,6].

Let $\mathbf{k}$ be a local field and $\overline{\mathbf{k}}$ be its residue field. Let $ord_{\mathbf{k}}$ be the discrete valuation of $\mathbf{k}$. Let $\mathbf{K}$ be a finite Galois extension of $\mathbf{k}$ and $\overline{\mathbf{K}}$ be its residue field. Let $ord_{\mathbf{K}}$ be the discrete valuation of $\mathbf{K}$ and let $P_{\mathbf{K}}$ be the maximal ideal of $\mathbf{K}$. Let T be a generator of $P_{\mathbf{K}}$. We assume that the extension of residue field $\overline{\mathbf{K}}/\overline{\mathbf{k}}$ is a separable extension. Let G be the Galois group of the extension $\mathbf{K}/\mathbf{k}$.

Definition 1.1. *The i-th ramification group G_i of G is defined to be*

$$G_i = \{\sigma \in G \,|\, \sigma(T) \equiv T \bmod P_{\mathbf{K}}^{i+1}\}.$$

It is clear that the G_i form a decreasing sequence of normal subgroups of G and there is an i_0 such that $G_{i_0} = 1$. We define the function i_G on G by the following formula:

$$i_G(\sigma) = ord_{\mathbf{K}}(\sigma(T) - T).$$

Note that $i_G(\sigma)$ is an integer, if $\sigma \neq 1$ and $i_G(\sigma) = \infty$ if $\sigma = 1$. Let H be a normal subgroup of G and let $\mathbf{K}'$ be the subfield of $\mathbf{K}$ fixed by H.

Proposition 1.2. *For every $\beta \in G/H$,*

$$i_{G/H}(\beta) = \frac{1}{e(\mathbf{K}/\mathbf{k})} \sum_{\sigma \mapsto \beta} i_G(\sigma),$$

where $e(\mathbf{K}/\mathbf{k})$ is the ramification index of $P_{\mathbf{K}}$ in the extension $\mathbf{K}/\mathbf{k}$ and

$\sigma \to \beta$ means that the sum runs over all the elements σ of G in the coset β.

The proof of proposition 1.2 can be found in [20, chapter 4.1].

Corollary 1.3. *If $H = G_j$ for some integer $j \geq 0$, then $(G/H)_i = G_i/H$ for $i \leq j$, and $(G/H)_i = 1$ for $i \geq j$.*

Proof. The G_i/H for $i \leq j$, form a decreasing sequence of subgroups in G/H, i.e., $G_0/H \supseteq G_1/H \supseteq \cdots G_{j-1}/H \supset 0$. If $\beta \in G/H$ and $\beta \neq 1$, then there is a unique $i \leq j$ such that $\beta \in G_i/H$ and $\beta \notin G_{i+1}/H$. If $\sigma \in G$ is in β, then $\sigma \in G_i - G_{i+1}$, hence $i_G(\sigma) = i+1$. Since $H \subset G_0$ by hypothesis, $\mathbf{K}/\mathbf{K}'$ is a totally ramified extension and $|H| = e(\mathbf{K}/\mathbf{K}')$. From the proposition 1.2, we get $i_{G/H}(\beta) = i+1$, therefore the two filtrations coincide for $i \leq j$. For $i \geq j$, the corollary is clear.

We have

$$\sigma \in G_i \Leftrightarrow \sigma(T) \equiv T \bmod P_{\mathbf{K}}^{i+1} \Leftrightarrow \frac{\sigma(T)}{T} \equiv 1 \bmod P_{\mathbf{K}}^{i}.$$

We now define a filtration for the group $U_{\mathbf{K}}$, i.e,

$$U_{\mathbf{K}} = \{\, x \in \mathbf{K} \mid ord_{\mathbf{K}}(x) = 0 \,\},$$

by

$$\begin{aligned} U_{\mathbf{K}}^0 &= U_{\mathbf{K}} \\ U_{\mathbf{K}}^i &= 1 + P_{\mathbf{K}}^i \text{ for } i \geq 1. \end{aligned}$$

We have two group isomorphisms

1. $U^0_{\mathbf{K}}/U^1_{\mathbf{K}} \simeq \overline{\mathbf{K}}^*$, where $\overline{\mathbf{K}}^*$ is the multiplicative group of $\overline{\mathbf{K}}$.

2. For $i \geq 1$, $U^i_{\mathbf{K}}/U^{i+1}_{\mathbf{K}} \simeq P^i_{\mathbf{K}}/P^{i+1}_{\mathbf{K}} \simeq \overline{\mathbf{K}}$, where the first isomomorphism is canonical while the second one is not.

Theorem 1.4. *If the characteristic of $\overline{\mathbf{K}}$ is $p > 0$, then the quotients G_i/G_{i+1}, $i \geq 1$, are abelian groups, and are direct products of cyclic groups of order p. The group G_1 is a p-group.*

Proof. For $i \geq 1$, $U^i_{\mathbf{K}}/U^{i+1}_{\mathbf{K}}$ is isomorphic to the additive group $\overline{\mathbf{K}}$ and any subgroup of $\overline{\mathbf{K}}$ is a p-group. But G_i/G_{i+1} is isomorphic to a subgroup of $U^i_{\mathbf{K}}/U^{i+1}_{\mathbf{K}}$. This proves the first part of the theorem. The second part of the theorem is a consequence of the fact that the cardinality of G_1 is equal to $\prod_{i\geq 1} |G_i/G_{i+1}|$.

Definition 1.5. *If $G_i \neq G_{i+1}$, we say that i is a jump in the filtration of the ramification groups of G.*

Theorem 1.6. *The integers $i \geq 1$ such that $G_i \neq G_{i+1}$ are all congruent to one another* mod p.

The proof of theorem 1.6 can be found in [20].

The theorems that we are going to use the most in the following sections are Herbrand's and Hasse-Arf's theorems. The Herbrand's theorem gives the

relation between the ramification groups of G and the ramification groups of G/H. The Hasse-Arf's theorem states where the jumps can happen in the filtration of the ramification groups for an abelian extension. Before we can present these two theorems we need to define the function φ. Let $u \in [-1, \infty)$, then G_u denotes the ramification group G_i, where i is the smallest integer $\geq u$.

Theorem 1.7. *For a real number $u \geq -1$ we put,*

$$\varphi_{\mathbf{K/k}}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}.$$

When $-1 \leq f \leq 0$, our convention is that $[G_0 : G_t]$ is equal to $[G_{-1} : G_0]^{-1}$ for $t = -1$ and is equal to $1 = [G_0 : G_0]^{-1}$ for $-1 < t \leq 0$. It is clear that if $u \in [m, m+1]$, where m is a positive integer, then

$$\varphi_{\mathbf{K/k}}(u) = \frac{1}{g_0}(g_1 + \cdots + g_m + (u-m)g_{m+1}), \text{ where } g_i = |G_i|.$$

Note that φ is an increasing function. Now we can define the upper numbering of the ramification groups. We put

$$G^{\varphi_{\mathbf{K/k}}(u)} = G_u.$$

We can now state the Herbrand's theorem.

Theorem 1.8. (Herbrand) *If $v = \varphi_{\mathbf{K/K'}}(u)$, then*

$$G_u H = (G/H)_v.$$

Proof. In the proof of Herbrand's theorem, we need two properties of φ. The first is the transitivity, i.e., $\varphi_{\mathbf{K}/\mathbf{k}} = \varphi_{\mathbf{K}'/\mathbf{k}} \circ \varphi_{\mathbf{K}/\mathbf{K}'}$. The second property of φ is the following: Let $\beta \in G/H$, let $j(\beta)$ be the upper bound of the integer $i_G(\sigma)$ as σ runs over the coset β. Then $i_{G/H}(\beta) = \varphi_{\mathbf{K}/\mathbf{K}'}(j(\beta) - 1)$. Now we are ready to prove Herbrand 's theorem, then

$$\beta \in G_u H/H \iff j(\beta) - 1 \geq u \iff \varphi_{\mathbf{K}/\mathbf{K}'}(j(\beta) - 1) \geq \varphi_{\mathbf{K}/\mathbf{K}'}(u)$$
$$\iff i_{G/H}(\beta) - 1 \geq \varphi_{\mathbf{K}/\mathbf{K}'}(u) \iff \beta \in (G/H)_u.$$

This completes the proof of theorem 1.8.

If $\mathbf{K}/\mathbf{k}$ is an infinite Galois extension, then one can define

$$G^v := \varprojlim G(\mathbf{K}'/\mathbf{k})^v,$$

where $\mathbf{K}'$ runs over all the finite Galois subextensions of $\mathbf{K}$. The G^v form a filtration of G. This filtration is left continuous: $G^v = \bigcap_{w<v} G^w$. We say that v is a jump in the filtration of the ramification groups of G if $G^v \neq G^{v+\epsilon}$ for every $\epsilon > 0$.

Now we state Hasse-Arf's theorem.

Theorem 1.9. (Hasse-Arf) *If G is an abelian group, and if v is a jump in the filtration G^v, then v is an integer, equivalently, if $G_i \neq G_{i+1}$, then $\varphi_{\mathbf{K}/\mathbf{k}}(i)$ is an integer.*

The proof of theorem 1.9 can be found in [20, chapter 5.7].

We recall the definition of a linear representation of a group G and give some equivalent definitions of the exponential conductor of a representation of G. We gave the definition of the exponential conductor $\mathcal{F}(\chi)$ in the chapter 0.1.

Definition 1.10. *By a representation ρ of the group G we shall mean a homomorphism of G into the group $Aut(V)$ of automorphism of a finite dimensional vector space V over* $\mathbf{C}$.

If $\sigma \in G$, then we set $\chi_\rho(\sigma) = Tr(\rho(\sigma))$. The function χ_ρ is class function.

Example 1

The Artin character of G is defined to be

$$a_G(\sigma) = \begin{cases} -f(\mathbf{K}/\mathbf{k}).i_{\mathbf{K}/\mathbf{k}}(\sigma) & \text{if } \sigma \neq 1 \\ f(\mathbf{K}/\mathbf{k}) \sum_{\sigma \neq 1} i_G(\sigma) & \text{otherwise,} \end{cases}$$

where $f(\mathbf{K}/\mathbf{k}) = [\overline{\mathbf{K}} : \overline{\mathbf{k}}]$. It can be proved that $\mathcal{F}(\chi) = \sum_{\sigma \in G} a_G(\sigma)\chi(\sigma^{-1})$, where χ is an irreducible character of G.

Theorem 1.11. *If χ is the character of a representation of G in V, then*

the exponential conductor is

$$\mathcal{F}(\chi) = \sum_i \frac{g_i}{g_0} dim(V/V^{G^i}),$$

where V^{G_i} *is the subspace of* V *fixed by* G_i *and* $g_i = |G_i|$.

Proof. This is another way to write the definition 0.1 since $\chi(1) = dim(V)$ and $\chi(G_i) = dim(V^{G_i})$.

We now prove another equivalent definition of the exponential conductor of χ when χ is a character of degree 1.

Theorem 1.12. *Let* χ *be a character of degree 1 on* G. *Let* c_χ *be the largest integer for which the restriction of* χ *to the ramification group* G_{c_χ} *is not the trivial character(if* $\chi = 1$, *take* $c_\chi = -1$*). Then*

$$\mathcal{F}(\chi) = \varphi_{\mathbf{K/k}}(c_\chi) + 1.$$

Proof. If $c_\chi \geq i$, then $\chi(G_i) = 0$ and if $c_\chi < i$, then $\chi(G_i) = 1$. Now we substitute this value in the definition of conductor

$$\begin{aligned} \mathcal{F}(\chi) &= \sum_{i \geq 0} \frac{g_i}{g_0}(\chi(1) - \chi(G_i)) \\ &= \sum_{i=0}^{c_\chi} \frac{g_i}{g_0} \\ &= \varphi_{\mathbf{K/k}}(c_\chi) + 1. \end{aligned}$$

This proves the theorem.

So far, we have been working with local fields. We now begin to consider arbitrary field extensions. Now we define the exponential conductor for an arbitrary finite Galois extension $\mathbf{K}/\mathbf{k}$. Let $\mathbf{K}/\mathbf{k}$ be a finite Galois extension, with Galois group G. Let P be a non-zero prime ideal of $\mathbf{K}$ lying over a prime ideal $\mathbf{p}$ in $\mathbf{k}$. Let $\mathbf{K}_P$ and $\mathbf{k}_\mathbf{p}$ be the completions of $\mathbf{K}$ and $\mathbf{k}$ at P and $\mathbf{p}$, respectively. We assume that $\overline{\mathbf{K}}_P/\overline{\mathbf{k}}_\mathbf{p}$ is a separable extension. Note that the Galois group of the field extension $\mathbf{K}_P/\mathbf{k}_\mathbf{p}$ is the decomposition group $D(P)$. Now we can apply the above definitions and theorems to the field extension $\mathbf{K}_P/\mathbf{k}_\mathbf{p}$ and the group $D(P)$. Let χ be a character of $G(\mathbf{K}/\mathbf{k})$, then we define

$$\mathcal{F}(\chi, \mathbf{p}) = \mathcal{F}(\chi | D(P)).$$

$\mathcal{F}(\chi, \mathbf{p})$ is called the local exponential conductor of χ at $\mathbf{p}$. Note that if $\mathbf{p}$ is unramified, then $f(\chi, \mathbf{p}) = 0$.

Definition 1.13. *Let χ be a character of G, then the global conductor of χ is defined to be*

$$\mathcal{F}(\chi) = \prod_{\mathbf{p}} \mathbf{p}^{\mathcal{F}(\chi,\mathbf{p})}.$$

In the following sections we compute the global conductor for some particular field extensions.

1.2 Ramification Groups of the Composite Field of two Artin-Schreier Extensions

Let $\mathbf{k}$ be a local function field of characteristic p. Let b_1, b_2 be elements of $\mathbf{k}$ such that $f^p - f \neq b_1$ and $g^p - g \neq b_2$ for every $g, f \in \mathbf{F}$, where $\mathbf{F}$ is the composite field of $\mathbf{k}$ and the algebraic closure of the field of constant of $\mathbf{k}$. Let $\mathbf{k}(z)$ be the Artin-Schreier extension of $\mathbf{k}$ defined by the equation $z^p - z = b_1$, where $b_1 \in \mathbf{k}$ and let $\mathbf{k}(y)$ be the Artin-Schreier extension of $\mathbf{k}$ defined by the equation $y^p - y = b_2$, where $b_2 \in \mathbf{k}$.

Remarks about Artin-Schreier extension.

If $\mathbf{k}$ is the function field of a curve with exact field of constants $\mathbf{F}_q$ where $q = p^f$. If $\mathbf{K}/\mathbf{k}$ is a normal extension of $\mathbf{k}$ of degree p, then $\mathbf{K}$ can be generated by the adjuction of a single element. This element satisfies a polynomial equation of the form $t^p - t - b = 0$, where $b \in \mathbf{k}$. Suppose that $\mathbf{K} = \mathbf{k}(\alpha)$, where α is a root of $t^p - t - b = 0$, then the only closed points of $\mathbf{k}$ that can ramify in $\mathbf{K}$ are the poles of b. In fact, a closed point $\mathbf{p}$ of $\mathbf{k}$ ramifies in $\mathbf{K}$ if and only if $\mathbf{p}$ is pole of b and $gcd(ord_{\mathbf{p}}(b), p) = 1$.

Suppose that $\mathbf{K} = \mathbf{k}(\alpha) = \mathbf{k}(\gamma)$ with generators α, γ which satisfy

$$\alpha^p - \alpha = a, \quad \gamma^p - \gamma = b,$$

then $\gamma = r(\alpha + \eta)$ with $r \in (\mathbf{Z}/p)^*$ and $\eta \in \mathbf{k}$.

We assume that $\mathbf{k}(y)$ and $\mathbf{k}(z)$ ramify at the same prime. Let $\mathbf{K}$ be the

composite field of $\mathbf{k}(z)$ and $\mathbf{k}(y)$. We assume that $deg(\mathbf{K}/\mathbf{k}) = p^2$, therefore the extension $\mathbf{K}/\mathbf{k}$ is totally ramified. We assume that the fields of constants of $\mathbf{k}$, $\mathbf{k}(y)$, $\mathbf{k}(z)$ and $\mathbf{K}$ are the same.

Let $H = G(\mathbf{k}(y)/\mathbf{k})$ and $H' = G(\mathbf{k}(z)/\mathbf{k})$. Note that $H' \simeq H \simeq \mathbf{Z}/p$. Since $\mathbf{k}(z)$ and $\mathbf{k}(y)$ are linearly disjoint, then $G(\mathbf{K}/\mathbf{k}) \simeq \mathbf{Z}/p \times \mathbf{Z}/p$. Let G be equal to $G(\mathbf{K}/\mathbf{k})$. Recall that the subgroups of $\mathbf{Z}/p \times \mathbf{Z}/p$ are:

1. $\mathbf{Z}/p \times \mathbf{Z}/p$
2. $\mathbf{Z}/p \times 0$
3. $0 \times \mathbf{Z}/p$
4. $N_{x,y} =< (x,y) > \quad x \neq 0 \text{ and } y \neq 0$
5. (0,0)

We can identify $G(\mathbf{K}/\mathbf{k}(z)) \simeq \mathbf{Z}/p \times 0$ and $G(\mathbf{K}/\mathbf{k}(y)) \simeq 0 \times \mathbf{Z}/p$. We assume that the filtration of the ramification groups of $G(\mathbf{k}(y)/\mathbf{k})$ are as follows:

$$G(\mathbf{k}(y)/\mathbf{k})_0 = \cdots = G(\mathbf{k}(y)/\mathbf{k})_l \supset 0.$$

We assume that the filtration of the ramification groups of $G(\mathbf{k}(z)/\mathbf{k})$ are also given as follows:

$$G(\mathbf{k}(z)/\mathbf{k})_0 = \cdots = G(\mathbf{k}(z)/\mathbf{k})_j \supset 0.$$

Note that because the degree of both extensions are p, there is only one jump in the filtration. We now prove a lemma that is used later.

Lemma 1.14. *$G(\mathbf{K}/\mathbf{k}(y))$ and $G(\mathbf{k}(z)/\mathbf{k})$ have the same filtration.*

Proof. Note that $\mathbf{K} = \mathbf{k}(y)(z)$, and $t^2 - t - b_2$ is irreducible over $\mathbf{k}(y)$ by hypothesis. We have

$$G(\mathbf{K}/\mathbf{k}(y)) = \{\sigma(z) = z + i \,|\, i \in \mathbf{Z}/p\}$$

and

$$G(\mathbf{k}(z)/\mathbf{k}) = \{\sigma(z) = z + i \,|\, i \in \mathbf{Z}/p\}.$$

Let $T_{\mathbf{k}}$, $T_{\mathbf{k}(y)}$, $T_{\mathbf{k}(z)}$ and $T_{\mathbf{K}}$ be the local uniformizing parameters of the fields $\mathbf{k}$, $\mathbf{k}(y)$, $\mathbf{k}(z)$ and $\mathbf{K}$, respectively. Let $\mathfrak{p}_{\mathbf{k}}$, $P_{\mathbf{k}(y)}$, $P_{\mathbf{k}(z)}$ and $P_{\mathbf{K}}$ be the corresponding maximal ideals generated by $T_{\mathbf{k}}$, $T_{\mathbf{k}(y)}$, $T_{\mathbf{k}(z)}$ and $T_{\mathbf{K}}$, respectively.

If $b \in \mathbf{k}$, then $ord_{P_{\mathbf{k}(y)}}(b) = p\, ord_{\mathfrak{p}_{\mathbf{k}}}(b)$. Since the last nontrivial ramification group of $\mathbf{k}(z)/\mathbf{k}$ is G_j, then $ord_{\mathfrak{p}_{\mathbf{k}}}(b_2) = -(j+1)$, therefore we can write this

$$b_2 = \sum_{n=-j-1}^{\infty} a_n T_{\mathbf{k}}^n \text{ where } a_n \in \mathbf{F}_q.$$

Since $t^p - t - b_2$ is irreducible over $\mathbf{k}(y)$, we have $\mathbf{K} = \mathbf{k}(y)(z)$ and $\mathbf{K}/\mathbf{k}(y)$ is an Artin-Schreier extension. Recall that $T_k = u\, T_{\mathbf{k}(y)}^p$, where u is a unit. Then, we have

$$b_2 = \sum_{n=-j-1}^{\infty} a_n' T_{\mathbf{k}(y)}^{pn} \text{ over } \mathbf{k}(y).$$

and hence

$$ord_{P_{\mathbf{k}(y)}}(b_2) = p\, ord_{\mathfrak{p}}(b_2) = -(j+1)\, p.$$

We can replace b_2 by an element with a simpler expansion. First, we modify b_2 by subtracting those terms in the $T_{P_{\mathbf{k}(y)}}$-expansion corresponding to the

negative multiples of p, i.e., if the term $a'_r T_{\mathbf{k}(y)}^{-pr}$ appears in the $T_{\mathbf{k}(y)}$- expansion of b_2, we can subtract it without affecting the structure of $\mathbf{K}$. Note that $z^p - z = b'_2$ with $b'_2 = b_2 - (a_{-j-1}^{1/p} T_{\mathbf{k}(z)}^{-j-1})^p + a_{-j-1}^{1/p} T_{\mathbf{k}(z)}^{-j-1}$ also generates $\mathbf{K}$. If we iterate this procedure for a finite number of times, we can replace b_2 by another element whose $T_{\mathbf{k}(y)}$-expansion does not contain terms with negative multiples of p:

$$b'_2 = b + \omega + \sum_{n=1}^{j+1} a'_n T_{\mathbf{k}(y)}^{-n},$$

where $a'_n = 0$ if p divide n, $\omega \in \mathbf{F}_q$ and $ord_{P_{\mathbf{k}(y)}}(b) > 0$. Then $ord_{P_{\mathbf{k}(y)}}(b'_2) = -j-1$ and therefore the ramification groups of $G(\mathbf{K}/\mathbf{k}(y))$ are as follows :

$$G(\mathbf{K}/\mathbf{k}(y)) = G(\mathbf{K}/\mathbf{k}(y))_0 = \cdots G(\mathbf{K}/\mathbf{k}(y))_j \supset 0.$$

This proves the lemma 1.14.

We next compute all the possible filtrations of the group G.

Theorem 1.15. *With notation and assumptions as above, the possible filtrations of the ramification groups of $G = G(\mathbf{K}/\mathbf{k})$ are as follows:*

Case 1. $G_0 = \cdots = G_l \supset G_{l+1} = \cdots = G_{(j-l)p+l} \supset 0$, *where* $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$ *and* $G_{l+1} = 0 \times \mathbf{Z}/p$.

Case 2. $G_0 = \cdots = G_j \supset G_{j+1} = \cdots = G_{(l-j)p+j} \supset 0$, *where* $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$ *and* $G_{j+1} = \mathbf{Z}/p \times 0$.

Case 3. $G_0 = \cdots = G_l \supset 0$, *where* $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$.

Moreover, case 1 happens only when $j > l$, case 2 happens only when $l > j$, and case 3 happens only when $j = l$.

Proof. We divide the proof in two parts. In the first part we prove that $G_n = \mathbf{Z}/p \times \mathbf{Z}/p$ for $1 \leq n \leq min(l, j)$. In the second part we check the possible subgroups of G that can be present in the filtration of G for $n > min(l, j)$. We assume that the ramification groups of G are as follows:

$$G = G_0 \supset G_1 \cdots \supset G_i \supset 0.$$

We have $G_1 = G = \mathbf{Z}/p \times \mathbf{Z}/p$ since $(|G_0/G_1|, p) = 1$. We will prove that $G = \mathbf{Z}/p \times \mathbf{Z}/p$ for $1 < n \leq min(l, j)$. But first we need to prove that $G_n = \mathbf{Z}/p \times \mathbf{Z}/p$ or $N_{x,y}$ for $1 < n \leq min(j, l)$. We assume $G_n \neq \mathbf{Z}/p \times \mathbf{Z}/p$ or $N_{x,y}$. Then G_n can only be equal to:

$$G_n = \begin{cases} (0,0) \\ \mathbf{Z}/p \times 0 \\ 0 \times \mathbf{Z}/p. \end{cases}$$

By Herbrand's theorem, we have

$$G_n G(\mathbf{K}/\mathbf{k}(y))/G(\mathbf{K}/\mathbf{k}(y)) = (G/G(\mathbf{K}/\mathbf{k}(y)))_{\varphi_{\mathbf{K}/\mathbf{k}(y))}(n)} \simeq \mathbf{Z}/p$$

since $\varphi_{\mathbf{K}/\mathbf{k}(y))}(n) \leq n$ and

$$G_n G(\mathbf{K}/\mathbf{k}(z))/G(\mathbf{K}/\mathbf{k}(z)) = (G/G(\mathbf{K}/\mathbf{k}(z)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)} \simeq \mathbf{Z}/p$$

since $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) \leq n$. But G_n cannot satisfy the above two inequalities for $G_n = (0,0)$ or $\mathbf{Z}/p \times 0$ or $0 \times \mathbf{Z}/p$. We are left to prove that $G_n \neq N_{x,y}$ for $1 < n \leq min(l, j)$, and we will prove it after the following example.

Example 2.

If we assume $min(l,j) = 1$, then $l = 1$ or $j = 1$. If $l = 1$, then the filtration of H is equal to $H_0 = H_1 \supset 0$. We claim that G_2 cannot be $\mathbf{Z}/p \times \mathbf{Z}/p$. If $G_2 = \mathbf{Z}/p \times \mathbf{Z}/p$, then $G(\mathbf{K}/\mathrm{k}(y))_2 = 0 \times \mathbf{Z}/p$ and $G(\mathbf{K}/\mathrm{k}(z))_2 = \mathbf{Z}/p \times 0$. In general, if H is a subgroup of G, then $H_n = G_n \bigcap H$. Therefore

$$\begin{aligned} G(\mathbf{K}/\mathrm{k}(y))G_2/G(\mathbf{K}/\mathrm{k}(y)) &= (\mathbf{Z}/p \times \mathbf{Z}/p)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &= \mathbf{Z}/p \times 0 \\ &= (G/G(\mathbf{K}/\mathrm{k}(y)))_{\varphi_{\mathbf{K}/\mathrm{k}(y)}(2)} \\ &= (G/G(\mathbf{K}/\mathrm{k}(y)))_2 = 0 \end{aligned}$$

since $\varphi_{\mathbf{K}/\mathrm{k}(y)}(2) = 2$. This is a contradiction. We have proved the claim in this case.

We now claim that G_2 cannot be equal to $N_{x,y}$. Suppose that $G_2 = N_{x,y}$, then $G(\mathbf{K}/\mathrm{k}(y))_2 = (0,0)$ and $G(\mathbf{K}/\mathrm{k}(z))_2 = (0,0)$. By Herbrand 's theorem we have

$$\begin{aligned} G(\mathbf{K}/\mathrm{k}(y))G_2/G(\mathbf{K}/\mathrm{k}(y)) &= (0 \times \mathbf{Z}/p)N_{x,y}/(0 \times \mathbf{Z}/p) \\ &\simeq \mathbf{Z}/p \\ &\simeq (G/G(\mathbf{K}/\mathrm{k}(y)))_{\varphi_{\mathbf{K}/\mathrm{k}(y)}(2)} \\ &= (G/G(\mathbf{K}/\mathrm{k}(y)))_2 \\ &= (0,0). \end{aligned}$$

This is a contradiction since $\varphi_{\mathbf{K}/\mathbf{k}(y)}(2) = \frac{p+1}{p} = 1 + \frac{1}{p} > 1$. This proves the claim.

If $G_2 = (0,0)$, then $G(\mathbf{K}/\mathbf{k}(y))_2 = G(\mathbf{K}/\mathbf{k}(z))_2 = (0,0)$. Therefore,

$$\begin{aligned} G(\mathbf{K}/\mathbf{k}(z))G_2/G(\mathbf{K}/\mathbf{k}(z)) &= (G/G(\mathbf{K}/\mathbf{k}(z)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(2)} \\ &= (G/G(\mathbf{K}/\mathbf{k}(z))_2 \\ &= (0,0) \end{aligned}$$

since $\varphi_{\mathbf{K}/\mathbf{k}(y)}(2) = 1 + \frac{1}{p}$, this implies that $j = 1$. This is possible only if $j = l = 1$, then we get the following filtration $G_0 = G_1 \supseteq (0,0)$. If $G_2 = 0 \times \mathbf{Z}/p$, then $G(\mathbf{K}/\mathbf{k}(y))_2 = 0 \times \mathbf{Z}/p$ and $G(\mathbf{K}/\mathbf{k}(z))_2 = (0,0)$, and therefore

$$\begin{aligned} \Big(G/G(\mathbf{K}/\mathbf{k}(y))\Big)_2 &= G_2/G(\mathbf{K}/\mathbf{k}(y)) \\ &= (0,0), \end{aligned}$$

and

$$\begin{aligned} G_2G(\mathbf{K}/\mathbf{k}(z))/G(\mathbf{K}/\mathbf{k}(z)) &= \Big((0 \times \mathbf{Z}/p)(\mathbf{Z}/p \times 0)\Big)/(\mathbf{Z}/p \times 0) \\ &\neq (0,0) \\ &= (G/G(\mathbf{K}/\mathbf{k}(z)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(2)} \\ &= (G/G(\mathbf{K}/\mathbf{k}(z)))_2. \end{aligned}$$

Since $\varphi_{\mathbf{K}/\mathbf{k}(z)}(2) = 1 + \frac{1}{p}$, we do not have a contradiction if $j \geq 2$. This has to

continue until $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) = j$, otherwise we have a contradiction. Therefore,

$$\begin{aligned}\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) &= \frac{1}{p}(p + \overbrace{1 \cdots + 1}^{n-1}) \\ &= \frac{1}{p}(p + (n-1)) \\ &= j\end{aligned}$$

If we solve for n, we get $n = p(j-1)+1$, and therefore the filtration of G is

$$G_0 = G_1 \supset G_2 = \cdots = G_{p(j-1)+1} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$ and $G_2 = 0 \times \mathbf{Z}/p$.

If $G_2 = \mathbf{Z}/p \times 0$, then $G(\mathbf{K}/\mathbf{k}(y))_2 = (0,0)$ and $G(\mathbf{K}/\mathbf{k}(z))_2 = \mathbf{Z}/p \times 0$. We have

$$\begin{aligned}\Big(G/G(\mathbf{K}/\mathbf{k}(z))\Big)_2 &= G_2/G(\mathbf{K}/\mathbf{k}(z)) \\ &= (0,0)\end{aligned}$$

but $\varphi_{\mathbf{K}/\mathbf{k}(z)}(2) = \frac{1}{p}(p+p) = 2$, then $j < 2$ and that implies $j = 1$. We obtain

$$\begin{aligned}\Big(G/G(\mathbf{K}/\mathbf{k}(y))\Big)_{\varphi_{\mathbf{K}/\mathbf{k}(y)}(2)} &= \Big(G/G(\mathbf{K}/\mathbf{k}(y))\Big)_2 \\ &= (0,0) \\ &= G_2 G(\mathbf{K}/\mathbf{k}(y))/G(\mathbf{K}/\mathbf{k}(y)) \\ &= \Big((\mathbf{Z}/p \times 0)(0 \times \mathbf{Z}/p)\Big)/(0 \times \mathbf{Z}/p) \\ &\neq (0,0).\end{aligned}$$

This is a contradiction, therefore $G_2 \neq 0 \times \mathbf{Z}/p$.

A similar argument for $j = 1(= min(l, j))$ gives the following filtration of G.

$$G_0 = G_1 \supset G_2 = \cdots = G_{p(l-1)+1} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$ and $G_2 = \mathbf{Z}/p \times 0$. The general case is similar to the **Example 2**. This complete the discussion of example 2.

Now we are going to prove that $G_n = \mathbf{Z}/p \times \mathbf{Z}/p$ for $1 < n \leq min(l, j)$. The only case left to prove is that $G_n \neq N_{x,y}$ for $1 < n \leq min(l, j)$.

We assume that $G_n = N_{x,y}$, where $1 < n \leq min(l, j)$; therefore we have $G(\mathbf{K}/\mathrm{k}(y))_n = 0$ and $G(\mathbf{K}/\mathbf{k}(z))_n = 0$. But according to the theorem 1.14, $G(\mathbf{K}/\mathrm{k}(y))_n \neq 0$ and $G(\mathbf{K}/\mathbf{k}(z))_n \neq 0$ since $n \leq min(l, j)$. We get a contradiction, and therefore we have proved $G_n = \mathbf{Z}/p \times \mathbf{Z}/p$ for $1 \leq n \leq min(l, j)$. So far, we have

$$G_0 = G_1 = \cdots = G_{min(l,j)} \cdots,$$

where $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$.

In the second part of the proof, we will assume that G_n is equal to each one of the subgroups of G and we use Herbrand's theorem to see if the subgroup can be present in the filtration of G for $n > min(l, j)$.

Claim. $G_n \neq \mathbf{Z}/p \times \mathbf{Z}/p$ for $n > min(l, j)$.

If $n > min(l, j)$, we suppose that $G_n = \mathbf{Z}/p \times \mathbf{Z}/p$, then we will have a contradiction. Since $G(\mathbf{K}/\mathbf{k}(z))_n = G(\mathbf{K}/\mathbf{k}(z))$ and $G(\mathbf{K}/\mathbf{k}(y))_n = G(\mathbf{K}/\mathbf{k}(y))$,

then $\varphi_{\mathbf{K}/\mathbf{k}(y)}(n) = n = \varphi_{\mathbf{K}/\mathbf{k}(z)}(n)$. Hence $(G/G(\mathbf{K}/\mathbf{k}(y)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}$ or $(G/G(\mathbf{K}/\mathbf{k}(z)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}$ is equal to $(0,0)$, but $(G/G(\mathbf{K}/\mathbf{k}(y)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}$ and $(G/G(\mathbf{K}/\mathbf{k}(z)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}$ are not trivial groups. This is a contradiction. We now assume that $max(l,j) \geq n > min(l,j)$. In particular this implies $l \neq j$. The following are all the possible subgroups:

$$G_n = \begin{cases} (0,0) \\ N_{x,y} \\ 0 \times \mathbf{Z}/p \\ \mathbf{Z}/p \times 0. \end{cases}$$

We assume $G_n = (0,0)$, then $G(\mathbf{K}/\mathbf{k}(y)) = G(\mathbf{K}/\mathbf{k}(z)) = (0,0)$, therefore

$$(0,0) = G_n G(\mathbf{K}/\mathbf{k}(y))/G(\mathbf{K}/\mathbf{k}(y)) = (G/G(\mathbf{K}/\mathbf{k}(y)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}$$

and

$$(0,0) = G_n G(\mathbf{K}/\mathbf{k}(z))/G(\mathbf{K}/\mathbf{k}(z)) = (G/G(\mathbf{K}/\mathbf{k}(y)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}.$$

We get $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) > j$ and $\varphi_{\mathbf{K}/\mathbf{k}(y)}(n) > l$, but $\varphi_{\mathbf{K}/\mathbf{k}(y)}(n)$ or $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) \leq max(l,j)$ and this is a contradiction. Therefore, $G_n \neq (0,0)$.

We keep the previous assumption on n. If $G_n = N_{x,y}$, then in particular $G_{min(l,j)+1} = N_{x,y}$. Let $n = min(l,j) + 1$. Therefore, we have

$$\begin{aligned} 0 &\neq N_{x,y}(0 \times \mathbf{Z}/p)/(\mathbf{Z}/p \times 0) \\ &= G_n G(\mathbf{K}/\mathbf{k}(y))/G(\mathbf{K}/\mathbf{k}(y)) \\ &= \Big(G/G(\mathbf{K}/\mathbf{k}(y))\Big)_{\varphi_{\mathbf{K}/\mathbf{k}(y)}(n)} \\ &= \Big(G/G(\mathbf{K}/\mathbf{k}(y))\Big)_{min(l,j)+1} \end{aligned}$$

and

$$\begin{aligned} 0 &\neq N_{x,y}(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &= G_n G(\mathbf{K}/\mathbf{k}(z))/G(\mathbf{K}/\mathbf{k}(z)) \\ &= \Big(G/G(\mathbf{K}/\mathbf{k}(z))\Big)_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)} \\ &= \Big(G/G(\mathbf{K}/\mathbf{k}(z))\Big)_{min(l,j)+1}. \end{aligned}$$

But one of these groups is trivial since l or $j > min(l,j)$. Therefore $G_n \neq N_{x,y}$.

If $G_n = 0 \times \mathbf{Z}/p$ then $G(\mathbf{K}/\mathbf{k}(y))_n = G_n$ and $G(\mathbf{K}/\mathbf{k}(z))_n = (0,0)$, therefore

$$\begin{aligned} G_n/G(\mathbf{K}/\mathbf{k}(y)) &= (G/G(\mathbf{K}/\mathbf{k}(y)))_n \\ &= (0,0). \end{aligned}$$

We do not have a contradiction if $n > l$. Recall that the last non-trivial ramification group of $G(\mathbf{k}(y)/\mathbf{k})$ is $G(\mathbf{k}(y)/\mathbf{k})_l$. This implies that $l = min(l,j)$.

$$\begin{aligned} G_n G(\mathbf{K}/\mathbf{k}(z))/G(\mathbf{K}/\mathbf{k}(z)) &= \Big(\mathbf{Z}/p \times 0)(0 \times \mathbf{Z}/p)\Big)/(0 \times \mathbf{Z}/p) \\ &= (\mathbf{Z}/p \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\neq (0,0) \\ &= \Big(G/G(\mathbf{K}/\mathbf{k}(z))\Big)_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}. \end{aligned}$$

Therefore, $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) = l + \frac{n-l}{p} \leq j$. If we take $n = (j-l)p + l$, then $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) = j$ and $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n+1) > j$. We do not have a contradiction. Therefore, we have the following filtration for G:

$$G_0 = \cdots = G_l \supset G_{l+1} = \cdots G_{(j-l)p+l} \supset (0,0)$$

where $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$ and $G_{l+1} = 0 \times \mathbf{Z}/p$.

If we take $G_n = \mathbf{Z}/p \times 0$. We get that $min(l,j) = j$ and the ramification groups of G are as follows:

$$G_0 = \ldots G_j \supset G_{j+1} \cdots G_{p(l-j)+j} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p \times \mathbf{Z}/p$ and $G_{j+1} = \mathbf{Z}/p \times 0$. We now work on the last case, $l = j$. If $l = j$, we claim that

$$G_{l+1} = (0,0).$$

Let $n = l + 1$. If $G_n = N_{x,y}$, then $G(\mathbf{K}/\mathbf{k}(y))_n = G(\mathbf{K}/\mathbf{k}(z))_n = (0,0)$ and hence

$$\begin{aligned} 0 \neq\ & G_n G(\mathbf{K}/\mathbf{k}(y))/G(\mathbf{K}/\mathbf{k}(y)) \\ =\ & (G/G(\mathbf{K}/\mathbf{k}(y)))_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)} \\ =\ & (G/G(\mathbf{K}/\mathbf{k}(y)))_n = (0,0), \end{aligned}$$

since $\varphi_{\mathbf{K}/\mathbf{k}(z)}(n) = l + \frac{1}{p}$. This is a contradiction. If $G_n = \mathbf{Z}/p \times 0$, then $G(\mathbf{K}/\mathbf{k}(z)) = G_n$ and $G(\mathbf{K}/\mathbf{k}(y)) = (0,0)$ and hence

$$G_n G(\mathbf{K}/\mathbf{k}(y))/G(\mathbf{K}/\mathbf{k}(y)) = \Big(G/G(\mathbf{K}/\mathbf{k}(y))\Big)_{\varphi_{\mathbf{K}/\mathbf{k}(z)}(n)}$$

$$\begin{aligned} &\neq (0,0) \\ &= (G/G(\mathbf{K}/\mathbf{k}(y)))_{l+1} \\ &= (0,0), \end{aligned}$$

since $l+1 > l$. This is a contradiction, therefore $G_n \neq \mathbf{Z}/p \times 0$.

The same argument applies for $G_n = 0 \times \mathbf{Z}/p$. We get the following filtration of ramification groups of G:

$$G_0 = \cdots = G_l \supset (0,0).$$

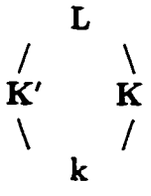
This completes the proof of theorem 1.15.

1.3 Ramification Groups for the Composite Field of an Artin-Schreier Extension and a Cyclic Extension of Degree p^2

In this section we give all the possible filtrations of the ramification groups of the composite field of an Artin-Schreier extension and a cyclic extension of degree p^2. This situation is more complicated than the previous section since the group has more subgroups. This case helps us to see how complicated the general case is, i.e., the composite field of an Artin-Schreier extension and a cyclic extension of degree p^n.

Let $\mathbf{k}$ be a local function field of characteristic p. Let b_1 be an element of $\mathbf{k}$ such that $f^p - f \neq b_1$ for every $f \in \mathbf{F}$, where $\mathbf{F}$ is the composite field of $\mathbf{k}$ and the algebraic closure of the field of constant of $\mathbf{k}$. Let $\mathbf{K}$ be the

cyclic Galois extension of $\mathbf{k}$ of degree p^2 and let $\mathbf{K}'$ be the Artin-Schreier extension of $\mathbf{k}$ defined by the equation $y^p - y = b_1$, where $b_1 \in \mathbf{k}$. We assume that $\mathbf{K}'$ and $\mathbf{K}$ are totally ramified at the same prime. We identify $G(\mathbf{K}/\mathbf{k})$ with $\mathbf{Z}/p^2$. Recall that the only proper subgroup of $\mathbf{Z}/p^2$ of order p is $N := \{p, 2p, \ldots, (p-1)p, 0\}$. Let $\mathbf{L}$ be the composite field of $\mathbf{K}$ and $\mathbf{K}'$. We assume that $deg(\mathbf{L}/\mathbf{k}) = p^3$, therefore the extension $\mathbf{L}/\mathbf{k}$ is totally ramified. We have the following diagram:



Since $\mathbf{K}$ and $\mathbf{K}'$ are linearly disjoint, then $G(\mathbf{L}/\mathbf{k}) \simeq \mathbf{Z}/p^2 \times \mathbf{Z}/p$. We use this identification throughout the whole sections. Let G be equal to $G(\mathbf{L}/\mathbf{k})$. The subgroups of $\mathbf{Z}/p^2 \times \mathbf{Z}/p$ are:

1. $\mathbf{Z}/p^2 \times \mathbf{Z}/p$
2. $N \times 0$
3. $N \times \mathbf{Z}/p$
4. $\mathbf{Z}/p^2 \times 0$
5. $0 \times \mathbf{Z}/p$

6. $M_{x,y} =< (x,y) >$, where $x \not\equiv 0 \bmod p$ and $y \neq 0$

7. $M_y =< (p,y) >$, where $y \neq 0$

8. $(0,0)$

Note $M_{x,y} \simeq \mathbf{Z}/p^2$ and $M_y \simeq \mathbf{Z}/p$. We can identify $G(\mathbf{L}/\mathbf{K}') \simeq \mathbf{Z}/p^2 \times 0$ and $G(\mathbf{L}/\mathbf{K}) \simeq 0 \times \mathbf{Z}/p$. We will prove that the filtration of the ramification groups of $G(\mathbf{K}/\mathbf{k})$ has two jumps.

Theorem 1.16. *Let H be a cyclic group of order p^2. Let H be the Galois group of an extension $\mathbf{K}/\mathbf{k}$. We assume that the field extension $\mathbf{K}/\mathbf{k}$ is totally ramified and the characteristic of $\mathbf{k}$ is p. Then the filtration of the ramification groups of $\mathbf{K}/\mathbf{k}$ has two jumps.*

Proof. Let σ be the generator of H and let P be the maximal ideal of $\mathbf{K}$. Let π be the local uniformizing parameter of $\mathbf{K}$. We assume that $\sigma \in H_i$ and $\sigma \notin H_{i+1}$, i.e., $\mathrm{ord}_P(\sigma(\pi) - \pi) = i + 1$, for $i > 0$. Since $\sigma \in G_i$, then $\sigma(\pi) = \pi(1 + a)$, where $a \in P^i$.

Claim 1. $(\sigma - 1)(x) \equiv jxa \bmod P^{i+j+1}$ if $x \in m_{\mathbf{K}}^j$.

Proof.

If $x \in P^j$, then $x = u\pi^j$, where u is a unit. We have

$$\sigma(x) = \sigma(u)\sigma(\pi)^j$$

$$\begin{aligned} &= \sigma(u)\pi^j(1+a)^j \\ &= \sigma(u)\pi^j(1+ja+\binom{j}{2}a^2+\cdots+a^j). \end{aligned}$$

Therefore, we have

$$\begin{aligned} \sigma(x)-x &= \sigma(u)\pi^j + j\sigma(u)a\pi^j + \cdots + \sigma(u)(a\pi)^j - u\pi^j \\ &\equiv (\sigma(u)-u)\pi^j + j\sigma(u)a\pi^j \bmod P^{i+j+1} \\ &\equiv j\sigma(u)\pi^j \bmod P^{i+j+1} \text{ since } \sigma(u)-u \in P^{i+1}. \end{aligned}$$

We need to prove that

$$j\sigma(u)a\pi^j \equiv j\,u\,a\pi^j \bmod P^{i+j+1}.$$

Since $\sigma(u)-u \in P^{i+1}$, then $j\sigma(u)\pi^j - ju\pi^j \in P^{i+j+1}$. Therefore $jxa = ju\pi^j a \equiv j\sigma(u)a\pi^j \bmod P^{i+j+1}$. This proves the claim 1.

We assume that $p > 2$. We need to prove that $(\sigma^p - 1)(\pi) \in P^{i+2}$. This will prove the theorem. Note that $\sigma^p \neq 1$. The claim 1 implies $(\sigma-1)(\pi) \equiv a\pi \bmod P^{i+2}$.

Claim 2. $(\sigma-1)^{p-1}(a\pi) \in P^{pi+2}$

A. $(\sigma-1)(a\pi) - (i+1)a\pi^2 \in P^{2i+2}$ by the claim 1.

B. We have $(\sigma-1)^2(a\pi) \equiv (i+2)(\sigma-1)(a\pi)a \in P^{2i+3}$ by the claim 1. But $(\sigma-1)(a\pi)a \in P^{2i+2}$, therefore, $(\sigma-1)^2(a\pi) \in P^{2i+2}$.

C. If we repeat the procedure $p-1$ times, we get $(\sigma-1)^{p-1}(a\pi) \in P^{pi+2}$. This completes the proof of claim 2.

By the claim 1, we have $(\sigma-1)(\pi) - a\pi \in P^{i+2}$. If we apply $(\sigma-1)^{p-1}$ to $(\sigma-1)(\pi) - a\pi$, we get

$$(\sigma-1)^p(\pi) - (\sigma-1)^{p-1}(a\pi) \in (\sigma-1)^p(P^{i+2}) \subset P^{pi+2}.$$

Since $(\sigma-1)^{p-1}(a\pi) \in P^{pi+2}$, then $(\sigma-1)^p(\pi) \in P^{pi+2}$. But we have $(\sigma-1)^p = \sigma^p - 1$ since $\mathrm{char}(\mathbf{k}) = p$ and this proves that $\sigma^p(\pi) \equiv \pi \bmod P^{pi+2}$. We have proved that $\sigma^p \in H_{pi+1}$. When $p = 2$ the theorem is clear. We can conclude that the filtration of the ramification groups of H is of the form

$$H_0 = H_1 = \cdots = H_i \supset H_{i+1} = \cdots = H_{pi+2} = \cdots$$

where $H_0 = H$ and H_{i+1} is the subgroup of H of order p. This proves the theorem 1.16.

We assume that the ramification groups of $G(\mathbf{K}/\mathbf{k})$ are as follows:

$$G(\mathbf{K}/\mathbf{k})_0 = G(\mathbf{K}/\mathbf{k})_1 = \cdots = G(\mathbf{K}/\mathbf{k})_{j_1} \supset G(\mathbf{K}/\mathbf{k})_{j_1+1} \cdots = G(\mathbf{K}/\mathbf{k})_{j_2} \supset 0,$$

where $G(\mathbf{K}/\mathbf{k}) = \mathbf{Z}/p^2$ and $G(\mathbf{K}/\mathbf{k})_{j_1+1} = N$. We assume that the ramification groups of $G(\mathbf{K}'/\mathbf{k})$ are as follows:

$$G(\mathbf{K}'/\mathbf{k})_0 = G(\mathbf{K}'/\mathbf{k})_1 = \cdots = G(\mathbf{K}'/\mathbf{k})_d \supset 0.$$

First, we state a lemma that is used in the proof of theorem 1.18.

Lemma 1.17. The filtration of $G(\mathbf{L}/\mathbf{K})$ and $G(\mathbf{K}'/\mathbf{k})$ are the same.

Remark. The proof of lemma 1.17 is similar to the proof of lemma 1.14.

Now we are ready to state the main theorem of this section.

Theorem 1.18. *With the notation and assumptions as above, we have that the possible filtrations of G are as follows:*

Case 1.

$$G_0 = G_1 = \cdots = G_d \supset G_{d+1} = \cdots = G_{d+p(j_1-d)}$$
$$\supset G_{d+1+p(j_1-d)} = \cdots = G_{j_2p-d(p-1)} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ *and* $G_{d+1} = \mathbf{Z}/p^2 \times 0$ *and* $G_{d+1+p(j_1-d)} = N \times 0$.

Case 2.

$$G_0 = \cdots = G_{j_1} \supset G_{j_1+1} = \cdots = G_{(j_2-j_1)p+d} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ *and* $G_{j_1+1} = N \times 0$.

Case 3.

$$G_0 = \cdots = G_{j_1} \supset G_{j_1+1} = \cdots = G_{j_2} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ *and* $G_{j_1+1} = N \times \mathbf{Z}/p$.

Case 4.

$$G_0 = \cdots = G_{j_1} \supset G_{j_1+1} = \cdots = G_{j_2} \supset G_{j_2+1} = G_{p(p-1)(d-j_1-j_2)+dp} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ *and* $G_{j_1+1} = N \times \mathbf{Z}/p$ *and* $G_{j_2+1} = 0 \times \mathbf{Z}/p$.

Case 5.

$$G_0 = \cdots = G_{j_1} \supset G_{j_1+1} = \cdots = G_d \supset G_{d+1} = \cdots = G_{(j_2-d)p+d} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ *and* $G_{j_1+1} = N \times \mathbf{Z}/p$ *and* $G_{d+1} = M_y$.

Proof. Suppose that the ramification groups of G are as follows:

$$G_0 \supset G_1 \supset \cdots \supset G_i \supset (0,0).$$

Note that $G_1 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$, since $(|G_0/G_1|, p) = 1$. Let $l \leq min(d, j_1)$, then by Herbrand's theorem we have the following:

$$\begin{aligned} G_lG(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= G_i(0 \times \mathbf{Z}/p)/0 \times \mathbf{Z}/p \\ &= \left(G/G(\mathbf{L}/\mathbf{K})\right)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \\ &\simeq \mathbf{Z}/p^2 \end{aligned}$$

since $\varphi_{\mathbf{L}/\mathbf{K}}(l) \leq l$, and

$$\begin{aligned} G_lG(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= G_i(\mathbf{Z}/p^2 \times 0)/\mathbf{Z}/p^2 \times 0 \\ &= \left(G/G(\mathbf{L}/\mathbf{K}')\right)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)} \\ &\simeq \mathbf{Z}/p, \end{aligned}$$

since $\varphi_{\mathbf{L}/\mathbf{K}'}(l) \leq l$.

If $G_l(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \simeq \mathbf{Z}/p^2$ and $G_l(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \simeq \mathbf{Z}/p$,

then

$$|G_l(\mathbf{Z}/p^2 \times 0)| = |G_l(0 \times \mathbf{Z}/p)| = p^3$$

and

$$G_l(0 \times \mathbf{Z}/p) = \mathbf{Z}/p^2 \times \mathbf{Z}/p \tag{1.1}$$

$$G_l(\mathbf{Z}/p^2 \times 0) = \mathbf{Z}/p^2 \times \mathbf{Z}/p \tag{1.2}$$

therefore, $G_l = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ or $M_{x,y}$ since these groups are the only subgroups of $\mathbf{Z}/p^2 \times \mathbf{Z}/p$ that satisfy (1.1) and (1.2). Note that $(N \times \mathbf{Z}/p)(0 \times \mathbf{Z}/p) \neq \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $M_y(0 \times \mathbf{Z}/p) \neq \mathbf{Z}/p^2 \times \mathbf{Z}/p$. Now we divide the proof in 9 cases.

Case 1. $G_l \neq \mathbf{Z}/p^2 \times \mathbf{Z}/p$ for $l > min(j_1, d)$.

Proof. By Herbrand's theorem we have

$$\begin{aligned}\Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_l \\ &= (\mathbf{Z}/p^2 \times \mathbf{Z}/p)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq \mathbf{Z}/p^2\end{aligned}$$

that implies $l \leq j_1$.

$$\begin{aligned}\Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)} &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_l \\ &= (\mathbf{Z}/p^2 \times \mathbf{Z}/p)(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq \mathbf{Z}/p\end{aligned}$$

this implies $l \leq d$. But we have $l > min(d, j_1)$ and this is a contradiction.

Case 2. $G_l \neq M_{x,y}$ for $1 < l \leq min(j_1, d)$.

Proof. We can assume that $G_{l-1} = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_l = M_{x,y}$, then $G(\mathbf{L}/\mathbf{K})_l = G(\mathbf{L}/\mathbf{K}') = (0,0)$. Since $G(\mathbf{L}/\mathbf{K}) = (0,0)$ and lemma 1.17, we have $l > d$. This is a contradiction. Moreover, this proves that for $l \leq min(j_1, d)$, we have $G_l = \mathbf{Z}/p^2 \times \mathbf{Z}/p$.

Case 3. $G_l \neq M_{x,y}$ for $max(j_1, d) \geq l > min(j_1, d)$.

Proof. If $G_l = M_{x,y}$, then $G(\mathbf{L}/\mathbf{K})_l = G(\mathbf{L}/\mathbf{K}')_l = (0,0)$. By lemma 1.17, we have $l > d$. Then, we can conclude that $min(d, j_1) = d$. If $min(j_1, d) = d$, then

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= M_{x,y} G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') \\ &= M(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq \mathbf{Z}/p \\ &= \left(G/G(\mathbf{L}/\mathbf{K}')\right)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)} \\ &= (0,0) \text{ since } \varphi_{\mathbf{L}/\mathbf{K}'}(l) > d. \end{aligned}$$

This is a contradiction. This proves claim 3.

Case 4. If $j_1 = d$, we have that $G_{j_1+1} \neq M_{x,y}$.

Proof. If $G_{j_1+1} = M_{x,y}$, then we have the following:

$$\begin{aligned} G_{j_1+1}G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= M_{x,y}G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) \\ &= M_{x,y}(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq \mathbf{Z}/p^2 \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(j_1+1)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{j_1+1} \\ &\simeq N. \end{aligned}$$

We have a contradiction. This proves that $M_{x,y}$ cannot be present in the filtration of G.

Case 5. $G_l \neq M_y$ for $l = min(j_1, d) + 1$.

Proof. We have $G(\mathbf{L}/\mathbf{K})_l = G(\mathbf{L}/\mathbf{K}')_l = (0,0)$, then $l > d$ by lemma 1.17, equivalently, $min(d, j_1) + 1 > d$. We have two subcases:

1. If $min(d, j_1) = j_1$, then $j_1 + 1 > d \geq j_1$ that implies $j_1 = d$. Therefore, we get the following:

$$\begin{aligned} G_lG(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= G_l/G(\mathbf{L}/\mathbf{K}') \\ &= M_y(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq \mathbf{Z}/p \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)} \end{aligned}$$

$$= \left(G/G(\mathbf{L}/\mathbf{K}')\right)_{l-1+\frac{1}{p^2}}$$

The above implies $l = d + 1 \leq d$ and this is a contradiction.

2. If $min(d, j_1) = d$, then $(G/G(\mathbf{L}/\mathbf{K}'))_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)} = (0,0)$ since $\varphi_{\mathbf{L}/\mathbf{K}'}(l) > d$ and this is a contradiction.

Case 6. $G_{min(j_1,d)+1}$ can be equal to $\mathbf{Z}/p^2$. This determines a filtration of the ramification groups of G.

Proof. If $G_l = \mathbf{Z}/p^2 \times 0$, where $l = min(j_1, d) + 1$, then we have $G(\mathbf{L}/\mathbf{K}') = G_l$ and $G(\mathbf{L}/\mathbf{K})_l = (0,0)$. Then

$$G_l/G(\mathbf{L}/\mathbf{K}') = (0,0) = \left(G/G(\mathbf{L}/\mathbf{K}')\right)_l.$$

We can conclude that $l > d$ or equivalently $min(d, j_1) + 1 > d$. Therefore we have two cases:

1. If $j_1 = min(d, j_1)$, we have $d + 1 \geq j_1 + 1 > d$ that implies $d = j_1$. By Herbrand's theorem

$$\begin{aligned} G_lG(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (\mathbf{Z}/p^2 \times 0)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq \mathbf{Z}/p^2 \\ &= \left(G/G(\mathbf{L}/\mathbf{K})\right)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \\ &= \left(G/G(\mathbf{L}/\mathbf{K})\right)_{l+\frac{1}{p}}. \end{aligned}$$

Therefore, $l+1 = min(j_1, d)+1 = j_1+1 < j_1$ and this is a contradiction.

2. If $min(j_1, d) = d$, then G_l has to satisfy the following:

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= \Big((\mathbf{Z}/p^2 \times 0)(0 \times 0)\Big)/(0 \times \mathbf{Z}/p) \\ &\simeq \mathbf{Z}/p^2 \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \end{aligned}$$

where $\varphi_{\mathbf{L}/\mathbf{K}}(l) = d + \frac{1}{p} \leq j_1$.

We can conclude that $j_1 \neq d$. We have

$$G_0 = \cdots = G_d \supset_{d+1} \cdots,$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_{d+1} = \mathbf{Z}/p^2 \times 0$. We have $G_{d+r} = \mathbf{Z}/p^2 \times 0$ for $1 \leq r \leq p$ since if there is a jump at $d + r$. Then $d \equiv d + r \bmod p$. If $G_{d+r} = \mathbf{Z}/p^2 \times 0$ and $G_{d+r+1} \neq \mathbf{Z}/p^2 \times 0$(Note that $r \geq p$), then we get the following:

$$\begin{aligned} G_{d+r} G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (0 \times \mathbf{Z}/p)(\mathbf{Z}/p^2 \times 0)/(0 \times \mathbf{Z}/p) \\ &\simeq \mathbf{Z}/p^2 \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(d+r)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{d+\frac{r}{p}}. \end{aligned}$$

Therefore, we get that $\varphi_{\mathbf{L}/\mathbf{K}}(d + r) = d + \frac{r}{p} \leq j_1$, hence $r \leq p(j_1 - d)$

We have two possibilities for G_{d+r+1}

$$G_{d+r+1} = \begin{cases} N \times 0 \\ (0,0). \end{cases}$$

If $G_{d+r+1} = (0,0)$ we have the following:

$$\begin{aligned} G_{d+r+1}G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (0,0) \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(d+r+1)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{d+\frac{r+1}{p}}. \end{aligned}$$

Therefore, we have two inequalities $\varphi_{\mathbf{L}/\mathbf{K}}(d+r) \leq j_1$ and $\varphi_{\mathbf{L}/\mathbf{K}}(d+r+1) > j_2$. If we put together all the above information, we get

$$d + \frac{r}{p} \leq j_1 < j_2 < d + \frac{r+1}{p}.$$

This is a contradiction, therefore $G_{d+r+1} \neq (0,0)$. If $G_{d+r+1} = N \times 0$, then we have

$$\begin{aligned} G_{d+r+1}G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (N \times 0)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &= (N \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq N \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(d+r+1)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{d+\frac{r+1}{p}}. \end{aligned}$$

Therefore,

$$j_2 \geq \varphi_{\mathbf{L}/\mathbf{K}}(d+r+1) = d + \frac{r+1}{p} > j_1 \geq d + \frac{r}{p},$$

hence $j_1 = d + \frac{r}{p}$ therefore, $r = p(j_1 - d)$. We do not have a contradiction. So far in this case, we have the following filtration of the

ramification groups of G,

$$G_0 = \cdots G_d \supset G_{d+1} = \cdots = G_{d+p(j_1-d)} \supset G_{d+p(j_1-d)+1} \cdots,$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_{d+1} = \mathbf{Z}/p^2 \times 0$ and $G_{d+p(j_1-d)+1} = N \times 0$. Let $l = d + p(j_1 - d) + r$, where $r \geq 1$. We suppose that $G_l = N \times 0$ and $G_{l+1} = (0,0)$. Note that $r \geq p$ since $d \equiv d + p(j_1 - d) + r \bmod p$. Then, we have the following:

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (N \times 0)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &= (N \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq N \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \end{aligned}$$

therefore, we get $j_1 < \varphi_{\mathbf{L}/\mathbf{K}}(l) \leq j_2$ and

$$\begin{aligned} G_{l+1} G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (0,0) \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l+1)} \end{aligned}$$

this implies that $\varphi_{\mathbf{L}/\mathbf{K}}(l+1) > j_2$. We can deduce the following $d + \frac{p(j_1-d)+r}{p} \leq j_2 < d + \frac{p(j_1-d)+r+1}{p}$ then $j_2 = d + \frac{p(j_1-d)+r}{p}$. If we solve for r, we get $r = (j_2 - j_1)p$. We get that $l = j_2 p - d(p-1)$.

Therefore, the ramification groups of G are as follows:

$$G_0 = G_1 \cdots = G_d \supset G_{d+1} = \cdots = G_{d+p(j_1-d)}$$

$$\supset G_{d+1+p(j_1-d)} = \cdots = G_{pj_2-d(p-1)} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$, $G_{d+1} = \mathbf{Z}/p^2 \times 0$ and $G_{+pj_1+1-d(p-1)} = N \times 0$. Note this case 1 of theorem 1.18. This finishes case 6.

Case 7. $G_l \neq 0 \times \mathbf{Z}/p$ for $l = min(d, j_1) + 1$.

Proof. If $G_l = 0 \times \mathbf{Z}/p$ for $l = min(d, j_1) + 1$. Note that

$$\begin{aligned} G(\mathbf{L}/\mathbf{K}')_l &= G_l \bigcap G(\mathbf{L}/\mathbf{K}') \\ &= (0,0) \end{aligned}$$

and

$$\begin{aligned} G(\mathbf{L}/\mathbf{K})_l &= G_l \bigcap G(\mathbf{L}/\mathbf{K}) \\ &= G_l. \end{aligned}$$

Since $G(\mathbf{L}/\mathbf{K}) = G_l$, then $(G/G(\mathbf{L}/\mathbf{K}))_i = G_i/G(\mathbf{L}/\mathbf{K})$ for $i \leq l$ and $(G/G(\mathbf{L}/\mathbf{K}))_i = 0$ for $l \leq i$. That implies $l > j_2$. This is a contradiction since $j_2 > min(j_1, d)$.

Case 8. $G_{min(d,j_1)+1}$ can be equal to $N \times 0$. This determines a filtration of the ramification groups of G.

Proof. Suppose that $G_l = N \times 0$, then

$$G(\mathbf{L}/\mathbf{K})_l = G_l \bigcap G(\mathbf{L}/\mathbf{K}) = (0,0)$$

and

$$G(\mathbf{L}/\mathbf{K}')_l = G_l \bigcap G(\mathbf{L}/\mathbf{K}') = G_l.$$

By Herbrand's theorem

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K})/(G(\mathbf{L}/\mathbf{K}) &= (N \times 0)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq N \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)}, \end{aligned}$$

where $\varphi_{\mathbf{L}/\mathbf{K}}(l) = min(d, j_1)+\frac{1}{p} = min(d, j_1)+\frac{1}{p}$. Since $G_l G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) \simeq N$, then $j_1 < \varphi_{\mathbf{L}/\mathbf{K}}(l) \leq j_2$. On the other hand,

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}) &= (N \times 0)(\mathbf{Z}/p^2 \times 0)/\mathbf{Z}/p^2 \times 0) \\ &= 0 \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)}, \end{aligned}$$

where $\varphi_{\mathbf{L}/\mathbf{K}'}(l) = min(d, j_1) + \frac{1}{p} > d$. Note that $\varphi_{\mathbf{L}/\mathbf{K}}(l) = \varphi_{\mathbf{L}/\mathbf{K}'}(l)$. If $min(d, j_1) = j_1$, then

$$d < j_1 + 1.$$

This implies $d = j_1$. If we take $min(j_1, d) = d$, then a similar argument proves that $d = j_1$. Since $N \times 0$ does not have a proper subgroup, we can assume that $G_l = N \times 0$ and $G_{l+1} = (0, 0)$ for some $l > min(j_1, d)$. We have

$$G_l G(\mathbf{L}/\mathbf{K})/(G(\mathbf{L}/\mathbf{K}) = (N \times 0)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p)$$

$$\simeq N$$
$$= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)},$$

where $\varphi_{\mathbf{L}/\mathbf{K}}(l) = j_1 + \frac{(l-j_1)}{p}$. Since $G_lG(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) \simeq N$, then $j_1 < \varphi_{\mathbf{L}/\mathbf{K}}(l) \leq j_2$

$$G_{l+1}G(\mathbf{L}/\mathbf{K})/(G(\mathbf{L}/\mathbf{K}) = 0$$
$$= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l+1)},$$

where $\varphi_{\mathbf{L}/\mathbf{K}}(l+1) = j_1 + \frac{l+1-j_1}{p}$. Since $G_lG(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/K) = 0$, then $\varphi_{\mathbf{L}/\mathbf{K}}(l+1) > j_2$. If we put together the above inequalities, we get

$$j_1 + \frac{l-j_1}{p} \leq j_2 < j_1 + \frac{l-j_1}{p} + \frac{1}{p^2}.$$

Therefore, we can conclude that $j_2 = j_1 + \frac{l-j_1}{p}$ if we solve for l, we get $l = (j_2 - j_1)p + j_1$. We obtain the following filtration of the ramification groups of G

$$G_0 = \cdots = G_{j_1} \supset G_{j_1+1} = \cdots = G_{(j_2-j_1)p+j_1} \supset 0,$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_{j_1+1} = N \times 0$. Recall, that in this case $j_1 = d$. This filtration is case 2 of theorem 1.18.

Case 9. If $G_{min(j_1,d)+1} = N \times \mathbf{Z}/p$.

This is the most complicated case. In this case, we get three filtrations of the ramification groups of G.

Let $l = min(d, j_1)+1$. If $G_l = N \times \mathbf{Z}/p$, then $G(\mathbf{L}/\mathbf{K})_l = G_l \bigcap G(\mathbf{L}/\mathbf{K}) = 0 \times \mathbf{Z}/p$ and $G(\mathbf{L}/\mathbf{K}')_l = G_l \bigcap G(\mathbf{L}/\mathbf{K}') = N \times 0$, therefore we have $\varphi_{\mathbf{L}/\mathbf{K}}(l) = l$ and $\varphi_{\mathbf{L}/\mathbf{K}'}(l) = l-1+\frac{1}{p}$. By lemma 1.17, we have that $l \leq d$. By Herbrand's theorem we have

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= (N \times \mathbf{Z}/p)(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq \mathbf{Z}/p \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_l \end{aligned}$$

and

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (N \times \mathbf{Z}/p)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq N \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_l. \end{aligned}$$

The above expressions imply that $l \leq d$ and $j_1 < l \leq j_2$. If we put together all the above inequalities, we get $j_1 < l = min(d, j_1)+1 \leq d$. Then $min(d, j_1) = j_1$. In particular, $j_1 < d$. From now on, we assume that $j_1 < l$ and $G_l = N \times \mathbf{Z}/p$ and $G_{l+1} \neq N \times \mathbf{Z}/p$, then G_{l+1} can be equal to

$$G_{l+1} = \begin{cases} N \times 0 \\ 0 \times \mathbf{Z}/p \\ M_y \\ (0,0). \end{cases}$$

Using Herbrand's theorem, we get

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= (N \times \mathbf{Z}/p)(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq N \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{l} \end{aligned}$$

and

$$\begin{aligned} G_l G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= (N \times \mathbf{Z}/p)(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq \mathbf{Z}/p \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{j_1+\frac{l-j_1}{p}}. \end{aligned}$$

The above identities implies $j_1 < \varphi_{\mathbf{L}/\mathbf{K}}(l) \leq j_2$ and $\varphi_{\mathbf{L}/\mathbf{K}'}(l) = j_1 + \frac{l-j_1}{p} \leq d$. We have the following filtration of G

$$G_0 = \cdots = G_{j_1} \supset G_{j_1+1} = \cdots = G_l \supset G_{l+1} \cdots,$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_{j_1+1} = N \times \mathbf{Z}/p$. We are going to check if G_{l+1} can be equal to each one of the subgroups of $N \times \mathbf{Z}/p$.

Subcase 1. Let $G_{l+1} = (0,0)$.

If $G_{l+1} = (0,0)$, then

$$\Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(l+1)} = (0,0) = \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(l+1)},$$

this implies

$$\varphi_{\mathbf{L}/\mathbf{K}}(l+1) = l + \frac{1}{p} > j_2$$

and

$$\varphi_{\mathbf{L}/\mathbf{K}'}(l+1) = j_1 + \frac{l-j_1}{p} + \frac{1}{p^2} > d.$$

If we put together all the above inequalities, we get $l \leq j_2 < l + \frac{1}{p}$ and $j_1 + \frac{l-j_1}{p} \leq d < j_1 + \frac{l-j_1}{p} + \frac{1}{p^2}$; therefore we can conclude that $j_2 = l$ and $d = j_1 + \frac{l-j_1}{p}$. If we solve for l, we get

$$l = j_2 = p(d - j_1) + j_1.$$

In this case we get the following filtration:

$$G_0 = \cdots = G_{j_1} \supset G_{j_1+1} = \cdots = G_{j_2} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_{j_1+1} = N \times \mathbf{Z}/p$. This filtration of G is the third case of the theorem 1.18.

Subcase 2. Let $N \times 0$.

If $G_{l+1} = N \times 0$, then

$$G(\mathbf{L}/\mathbf{K})_{l+1} = G_{l+1} \bigcap G(\mathbf{L}/\mathbf{K}) \simeq 0$$

and

$$G(\mathbf{L}/\mathbf{K}')_{l+1} = G_{l+1} \bigcap G(\mathbf{L}/\mathbf{K}') \simeq N.$$

By lemma 1.17, $d < l+1$. Note that $l \leq d$ since $G(\mathbf{L}/\mathbf{K})_l \simeq \mathbf{Z}/p$, therefore $l = d$. By Herbrand's theorem

$$\begin{aligned} G_{d+1}G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= (N \times 0)(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq 0 \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(d+1)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{j_1+\frac{d+1-j_1}{p}}. \end{aligned}$$

The above expression implies that $d < j_1+\frac{d+1-j_1}{p}$ since $G_{l+1}G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') = 0$. If we solve for d, we get $d(p-1) < j_1(p-1)+1$ but $d > j_1$, therefore $j_1 < d < j_1 + \frac{1}{p-1}$. This is a contradiction, because $d \in \mathbf{Z}$.

Subcase 3. Let $G = 0 \times \mathbf{Z}/p$.

If $G_{l+1} = 0 \times \mathbf{Z}/p$, then

$$G(\mathbf{L}/\mathbf{K})_{l+1} = G_{l+1} \bigcap G(\mathbf{L}/\mathbf{K}) = 0 \times \mathbf{Z}/p$$

and

$$G(\mathbf{L}/\mathbf{K}')_{l+1} = G_{l+1} \bigcap G(\mathbf{L}/\mathbf{K}') = (0,0).$$

Since $G_l = G(\mathbf{L}/\mathbf{K})$, then $G_i/G(\mathbf{L}/\mathbf{K}) = \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_i$ for $i \leq l+1$ and $\Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_i = 0$ for $i \geq l+1$ and this implies $l+1 > j_2$, but $l \leq j_2$ since $G_l = N \times \mathbf{Z}/p$ therefore $l = j_2$. By lemma $l+1 \leq d$. In particular $d > j_2$. By Herbrand's theorem

$$G_{j_2+1}G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') = (0 \times \mathbf{Z}/p)(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0)$$

$$\begin{aligned} &\simeq \mathbf{Z}/p \\ &= \left(G/G(\mathbf{L}/\mathbf{K}')\right)_{\varphi_{\mathbf{L}/\mathbf{K}'}(j_2+1)} \\ &= \left(G/G(\mathbf{L}/\mathbf{K}')\right)_{j_1+\frac{j_2-j_1}{p}+\frac{1}{p^2}} \\ &= \left(G/G(\mathbf{L}/\mathbf{K}')\right)_{j_1+\frac{j_2-j_1}{p}+1}. \end{aligned}$$

The above identities imply

$$\varphi_{\mathbf{L}\mathbf{K}'}(l+1) = j_1 + \frac{j_2-j_1}{p} + \frac{1}{p^2} \leq d.$$

Since $0 \times \mathbf{Z}/p$ does not have a proper subgroup, then we can assume $G_{j_2+r} = 0 \times \mathbf{Z}/p$ and $G_{j_2+r+1} = (0,0)$ for some $r > 1$. We have

$$\begin{aligned} \varphi_{\mathbf{L}/\mathbf{K}}(j_2+r) &= j_1 + \frac{j_2-j_1}{p} + \frac{r}{p^2} \leq d \\ \varphi_{\mathbf{L}/\mathbf{K}}(j_2+r+1) &= j_1 + \frac{j_2-j_1}{p} + \frac{r+1}{p^2} > d. \end{aligned}$$

If we put together the above information we get

$$d = j_1 + \frac{j_2-j_1}{p} + \frac{r}{p^2}.$$

If we solve for r we get $r = (d-j_1)p^2 - p(j_2-j_1)$, then

$$l + r = p(p-1)(d-j_1-j_2) + dp.$$

We have the following filtration of G

$$G_0 = \cdots G_{j_1} \supset G_{j_1+1} = \cdots G_{j_2} \supset G_{j_2+1} = \cdots = G_{p(p-1)(d-j_1-j_2)+dp} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_{j_1+1} = N \times \mathbf{Z}/p$ and $G_{j_2+1} = 0 \times \mathbf{Z}/p$. This filtration of G is the fourth case of theoren 1.18.

Subcase 4. Let $G_{l+1} = M_y$.

If $G_{l+1} = M_y$, then $G(\mathbf{L}/\mathbf{K})_{l+1} = (0,0) = G(\mathbf{L}/\mathbf{K}')_{l+1}$. By lemma 1.17 we have $l+1 > d$. Since $G(\mathbf{L}/\mathbf{K})_l = 0 \times \mathbf{Z}/p$, we have $l \leq d$, therefore $l = d$. By Herbrand's theorem

$$\begin{aligned} G_{d+1}G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= M_y(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq \mathbf{Z}/p \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(d+1)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{j_1+\frac{d-j_1}{p}+\frac{1}{p^2}} \end{aligned}$$

and

$$\begin{aligned} G_{d+1}G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= M_y(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq N \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(d+1)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{d+\frac{1}{p}} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{d+1}. \end{aligned}$$

Note that

$$\varphi_{\mathbf{L}/\mathbf{K}}(l+1) = j_1 + \frac{d-j_1}{p} + \frac{1}{p^2} \leq d \tag{1.3}$$

and

$$j_1 < d+1 \leq j_2.$$

If we solve in (1.3) for d, we get

$$j_1 + \frac{1}{p(p-1)} \leq d.$$

Since M_y does not contain a proper subgroup, then we can assume that $G_{d+r} = M_y$ and $G_{d+r+1} = 0$ for $r > 1$. By Herbrand's theorem we have

$$\begin{aligned} G_{d+r}G(\mathbf{L}/\mathbf{K}')/G(\mathbf{L}/\mathbf{K}') &= M_y(\mathbf{Z}/p^2 \times 0)/(\mathbf{Z}/p^2 \times 0) \\ &\simeq \mathbf{Z}/p \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(d+r)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{j_1+\frac{d-j_1}{p}+\frac{r}{p^2}} \end{aligned}$$

and

$$\begin{aligned} G_{d+r}G(\mathbf{L}/\mathbf{K})/G(\mathbf{L}/\mathbf{K}) &= M_y(0 \times \mathbf{Z}/p)/(0 \times \mathbf{Z}/p) \\ &\simeq N \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(d+r)} \\ &= \Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{d+\frac{r}{p}}. \end{aligned}$$

We have

$$\Big(G/G(\mathbf{L}/\mathbf{K})\Big)_{\varphi_{\mathbf{L}/\mathbf{K}}(d+r+1)} = \Big(G/G(\mathbf{L}/\mathbf{K}')\Big)_{\varphi_{\mathbf{L}/\mathbf{K}'}(d+r+1)} = 0$$

where $\varphi_{\mathbf{L}/\mathbf{K}'}(d+r+1) = j_1 + \frac{d-j_1}{p} + \frac{r+1}{p^2}$ and $\varphi_{\mathbf{L}/\mathbf{K}}(d+r+1) = d + \frac{r+1}{p}$. Therefore, we have

$$j_1 + \frac{d-j_1}{p} + \frac{r}{p^2} \leq d < j_1 + \frac{d-j_1}{p} + \frac{r+1}{p^2}$$

and

$$d + \frac{r}{p} \leq j_2 < d + \frac{r+1}{p}.$$

We can conclude $d = j_1 + \frac{d-j_1}{p} + \frac{r}{p^2}$ and $j_2 = d + \frac{r}{p}$. If we solve for r, we get the following $r = p(p-1)(d-j_1)$ and $r = (j_2 - d)p$. Therefore,

$$l + r = d + p(p-1)(d-j_1) = d + (j_2 - d)p.$$

We obtain the following filtration of G in this case

$$G_0 = \cdots G_{j_1} \supset G_{j_1+1} = \cdots = G_d \supset G_{d+1} = \cdots = G_{d+(j_2-d)p} \supset (0,0),$$

where $G_0 = \mathbf{Z}/p^2 \times \mathbf{Z}/p$ and $G_{j_1+1} = N \times \mathbf{Z}/p$ and $G_{d+1} = M_y$. This filtration of G is the fifth case of theorem 1.18.

This completes the proof of the theorem 1.18.

Given a nontrivial representation χ of G, it is easy to give a bound for the conductor $\mathcal{F}(\chi)$ using theorem 1.18. For example, if G has a filtration as case 1 in theorem 1.18 and the representation is trivial on $\mathbf{Z}/p^2 \times 0$, then $\mathcal{F}(\chi) = d + 1$.

Note that if $G(\mathbf{K}/\mathbf{k})$ is a cyclic group of order p^n, then the above situation is more complicated since $G(\mathbf{K}/\mathbf{k}) \times G(\mathbf{K}'/\mathbf{k})$ has many subgroups. The

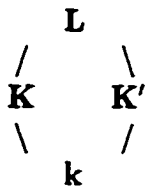
amounts of subgroups of $G(\mathbf{K}/\mathbf{k}) \times G(\mathbf{K}'/\mathbf{k})$ increases exponentially when n increases.

1.4 Ramification Groups of the Composite Field of the an Artin-Schreier and a Kummer Extension

In this section, we compute the filtration of the ramification groups of the composite field of an Artin-Schreier and a Kummer extension. As an application, we give a bound for mixed exponential sums in one variable which depend on a multiplicative and additive characters.

Let $\mathbf{k}$ be a local field of characteristic p. Let $\mathbf{K}$ be an Artin-Schreier extension of $\mathbf{k}$, i.e., $\mathbf{K}/\mathbf{k}$ is a separable field of degree p. Recall that the Galois group $G(\mathbf{K}/\mathbf{k})$ of the extension $\mathbf{K}/\mathbf{k}$ is isomorphic to $\mathbf{Z}/p$. Like we did before, we identify $G(\mathbf{K}/\mathbf{k})$ with $\mathbf{Z}/p$. Let $\mathbf{K}'$ be a Kummer extension of $\mathbf{k}$ of degree n, i.e., $\mathbf{K}/\mathbf{k}$ is a cyclic extension of degree n where n is relatively prime to p. Note that $\mathbf{k}$ has to contain a primitive n-th root of unity. Recall that the Galois group $G(\mathbf{K}'/\mathbf{k})$ is isomomorphic to $\mathbf{Z}/n$. We use this identification through this section. The fields $\mathbf{K}$ and $\mathbf{K}'$ are linearly disjoint. We assume that the extensions $\mathbf{K}/\mathbf{k}$ and $\mathbf{K}'/\mathbf{k}$ ramify at the same prime. Let $\mathbf{L} = \mathbf{K}\mathbf{K}'$ be the composite field of $\mathbf{K}$ and $\mathbf{K}'$ and let G be the Galois group of the field

extension $\mathbf{L}/\mathbf{k}$. We can identify $G \simeq G(\mathbf{K}/\mathbf{k}) \times G(\mathbf{K}'/\mathbf{k})$ with $\mathbf{Z}/p \times \mathbf{Z}/n$.



We can identify the Galois group of the field extension $\mathbf{L}/\mathbf{K}$ with $0 \times \mathbf{Z}/n$ and the Galois group of the field extension $\mathbf{L}/\mathbf{K}'$ with $\mathbf{Z}/p \times 0$. We can assume that $\mathbf{K}'/\mathbf{k}$ is totally ramified. Therefore, $\mathbf{L}/\mathbf{k}$ is a totally ramified extension of degree np.

Let $G(\mathbf{K}/\mathbf{k})_0 = \cdots = G(\mathbf{K}/\mathbf{k})_j \supset 0$ be the filtration groups of $G(\mathbf{K}/\mathbf{k})$ and let $G(\mathbf{K}'/\mathbf{k})_0 \supset 0$ be the filtration of the ramification groups of $G(\mathbf{K}'/\mathbf{k})$. We suppose that $G_0 \supset \cdots \supset G_i \supset 0$ is the filtration of the ramification groups of G.

Theorem 1.19. *The filtration of the ramification groups of G is equal to*

$$G_0 \supset G_1 = \cdots = G_{nj} \supset 0,$$

where $G_0 = \mathbf{Z}/p \times \mathbf{Z}/n$ and $G_1 = \mathbf{Z}/p \times 0$.

Proof. We have that $G_0 = G(\mathbf{K}/\mathbf{k}) \times G(\mathbf{K}'/\mathbf{k})$ and G_1 is a p-group, therefore $G_1 = G(\mathbf{K}/\mathbf{k}) = \mathbf{Z}/p \times 0$. We assume that $G_l = \mathbf{Z}/p \times 0$ and $G_{l+1} = (0,0)$ for $l > 1$. Then $G(\mathbf{L}/\mathbf{K})_l = (0,0)$. Therefore

$$\varphi_{\mathbf{L}/\mathbf{K}}(l) = \frac{1}{n}(\overbrace{1 + \cdots + 1}^{l})$$

and

$$\varphi_{\mathbf{L/K}}(l+1) = \frac{1}{n}(\overbrace{1+\cdots+1+1}^{l+1}).$$

Now, we use Herbrand's theorem.

$$\begin{aligned} G_l G(\mathbf{L/K})/G(\mathbf{L/K}) &\simeq (\mathbf{Z}/p \times 0)(0 \times \mathbf{Z}/n)/(0 \times \mathbf{Z}/n) \\ &\simeq \mathbf{Z}/p \\ &\simeq \Big(G/G(\mathbf{L/K})\Big)_{\varphi_{\mathbf{L/K}}(l)} \\ &= \Big(G/G(\mathbf{L/K})\Big)_{\frac{l}{n}}. \end{aligned}$$

Therefore $\frac{l}{n} \leq j$.

$$\begin{aligned} G_l G(\mathbf{L/K})/G(\mathbf{L/K}) &\simeq 0 \\ &\simeq \Big(G/G(\mathbf{L/K})\Big)_{\varphi_{\mathbf{L/K}}(l)} \\ &= \Big(G/G(\mathbf{L/K})\Big)_{\frac{l}{n}+\frac{1}{n}}. \end{aligned}$$

Therefore $\frac{l}{n} + \frac{1}{n} > j$. If we put together the two inequalities we get

$$\frac{l}{n} \leq j < \frac{l}{n} + \frac{1}{n}. \tag{1.4}$$

By Hasse-Arf's theorem

$$\varphi_{\mathbf{L/k}}(l) = \frac{1}{pm}(g_1 + \cdots + g_l) = \frac{l}{n}$$

is an integer. Therefore n divide l. Hence, the first inequality of (1.4) becomes equality, i.e., $j = \frac{l}{n}$. If we solve for l, we get $l = nj$. This proves the theorem.

Our next step is to apply the theorem 1.19 to mixed exponential sums in one variable. Let ψ be an additive character of the field $\mathbf{F}_q$, we can assume that

$$\psi(x) = e^{2\pi i Tr_{\mathbf{F}_q/\mathbf{F}_p}(x)/p}$$

and let χ be a multiplicative character of $\mathbf{F}_q^*$, we assume the order of χ is n.

Let X be a complete non-singular curve of genus g', defined over $\mathbf{F}_q$. Let k be its function field, and let $\mathbf{kF}_q^{sep}$ be the function field of X considered as a curve over the algebraic closure $\mathbf{F}_q^{sep}$ of $\mathbf{F}_q$. Let $f, g \in \mathbf{k}$ be a rational functions on X, satisfying the condition

(1.5) $$f \neq h^p - h \text{ for } h \in \mathbf{kF}_q^{sep}$$

(1.6) $$g \neq h^n \text{ for } h \in \mathbf{kF}_q^{sep}$$

Recall that we can identity f, g with rational maps

$$f, g : X \longrightarrow \mathbf{A}^1$$

of X into the affine line defined over $\mathbf{F}_q$. Let X_m be the set of points of X defined $\mathbf{F}_{q^m}$, and let

(1.7) $$S_m(f, g, X) = \sum_{x \in X_m} \chi(N(g(x)))e^{(2\pi i Tr(f(x))/p)},$$

where the summation is over the points of X_m except the poles of f, g and Tr is the trace map from $\mathbf{F}_{q^m}$ to $\mathbf{F}_p$ and N is the norm map from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$.

This exponential sum is related to the composite field of an Artin-Schreier and a Kummer extension. Before we give a bound for $S_m(f, g, X)$, we need

some notation. Let $(f)_\infty$ be the divisor of the poles of f on X, and write

$$(f)_\infty = \sum_{i=1}^{l} a_i P_i,$$

let (g) be the divisor corresponding to g, and write

$$(g) = \sum_{i=1}^{s} b_i Q_i.$$

Perel'muter on [17, theorem 1] gives the following bound for $S_m(f,g)$,

$$|S_m(f,g)| \leq (2g' - 2 + s + l + deg((f)_\infty))q^{m/2}.$$

Let r be the number of closed points of X that $(f)_\infty$ and (g) have in common. We are ready to state the second theorem of this section.

Theorem 1.20. *Let X be a complete non-singular curve over $\mathbf{F}_q$ of genus g' and let f and g be two rational functions on X satisfying condition (1.5) and (1.6). Then*

$$|S_m(f,g)| = |\sum_{x \in X_m} \chi(N(g(x)))e^{(2\pi i Tr(f(x))/p)}| \leq (2g'-2+s+l+deg((f)_\infty)-r)q^{m/2}.$$

Proof. Let $\mathbf{K}$ be the splitting field of $y^p - y = f$, this is an Artin-Schreier extension of $\mathbf{k}$. Let $\mathbf{K}'$ be the splitting field of $y^n = g$, this is a Kummer extension of k(We assume that the field of constant of $\mathbf{K}'$ contains a primitive n-th root of unity). Finally, let $\mathbf{L} = \mathbf{K}\mathbf{K}'$ be the composite field of $\mathbf{K}$ and

$\mathbf{K}'$. We need to compute the exponential conductor of $\psi\chi$. We know that if D is the exponential conductor of $\psi\chi$, then

$$|S_m(f,g)| = |\sum_{x\in X_m} \chi(N(g(x)))e^{2\pi\imath Tr(f(x))/p}| \leq (2g' - 2 + D)q^{m/2}.$$

We are going to prove that $D \leq s + l + deg((f)_\infty) - r$. The question here is local, therefore we work in completion of $\mathbf{k}$. The field extension $\mathbf{L}/\mathbf{k}$ can ramify at closed points that appear in $(f)_\infty$ and (g). If P_i does not divide g, then the local exponential conductor less than or equal $d_i + 1$. If Q_i does not divide $(f)_\infty$, then the local exponential conductor is less than or equal to 1. If P_i is a closed point of X that divide $(f)_\infty$ and (g), by the theorem 1.19 the local exponential conductor is less than or equal $d_i + 1$. If we put together all the contribution from the closed points appearing in $(f)_\infty$ and (g), we get what we want. If $gcd(a_i, p) = 1$ for $i = 1, \ldots, l$, where p is the characteristic of $\mathbf{F}_q$ and $gcd(b_i, n) = 1$, then $D = l + s + deg((f)_\infty) - r$.

Now we discuss some examples.

Example 3.

Let $\psi(x) = e^{2\pi\imath Tr_{\mathbf{F}_q/\mathbf{F}_p}(x)/p}$ and $\chi(x)$ be a multiplicative character of $\mathbf{F}_q^*$. Note we are taking $X = \mathbf{A}^1$.

1. If we take $f(x) = x$ and $g(x) = x$, then we get a Gauss sum

$$|S_m(f,g)| = |\sum_{x\in\mathbf{F}_{q^m}} \chi(N_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))e^{2\pi\imath Tr_{\mathbf{F}_{q^m}/\mathbf{F}_p}(x)/p}| \leq (2 + 2 - 1 - 2)q^{m/2}$$

2. If we take $f(x) = x^7 + at$, where $a \in \mathbf{F}_q$, and $g(x) = x$, then we get

$$|S_m(f,g)| = \sum_{x \in \mathbf{F}_{q^m}} \chi(N_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)) e^{2\pi i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_p}(x^7+ax)/p}| \leq (8+2-1-2)q^{m/2}.$$

Using theorem 1.20, we compute some L-functions.

Example 4.

We compute the L-function of this sum

$$S_m(x^7 - ax, x) = \sum_{x \in \mathbf{F}_{p^m}} (\frac{N_{\mathbf{F}_{p^m}/\mathbf{F}_p}(x)}{p}) e^{2\pi i Tr(x^7-ax)/p}$$

for $p = 3$. Therefore, the L-function is defined by

$$L(t, x^7 - ax) = \exp\{\sum_{m=1}^{\infty} \frac{S_m(x^7 - ax, x)}{m} t^m\}.$$

By theorem 1.20 the degree of L-functions is ≤ 7.

1. $L(t, x^7 - x, p = 3) = (9t^4 + 3t^2 + 1)(3\sqrt{3}it^3 + 1)$

2. $L(x^7 + x, x, p = 3) = (1 + \sqrt{3}it)$. Note that the degree is one, therefore there exists a transformation such that the sum becomes a Gauss sum.

3. $L(t, x^7, x, p = 3) = 1 + \sqrt{3}it + 27t^6 + 27\sqrt{3}it^7$

Chapter 2

L-functions of Singular Curves over Finite Fields

In this chapter we introduce a definition for L-functions associated to an abelian covering of algebraic curves with singularities. The main result, theorem 2.5, is a proof that this definition is compatible with the definition given by Stöhr for the zeta function of a singular curve. We also include applications to exponential sums.

2.1 The Zeta functions of Singular Curves

In this section we give some definitions and facts about singular curves and recall some results of Karl-Otto Stöhr that are needed in the following sections. In some of the results that we present in this section, we will give an outline of the proof. We follow closely the presentation of Stöhr on [23] and [24].

Let X be a complete irreducible algebraic curve with constant field $\mathbf{k}$

and let $\mathbf{K}$ be the function field of X. Therefore $\mathbf{K}$ is a function field in one variable with field of constant $\mathbf{k}$, i.e., $\mathbf{K}$ is a finite algebraic extension of $\mathbf{k}(x)$ for some element $x \in \mathbf{K}$, which is transcendental over $\mathbf{k}$ and X is the set $\{\mathcal{O}_P\}_{P \in X}$ of local $\mathbf{k}$-algebras, properly contained in $\mathbf{K}$ with quotient field $\mathbf{K}$, satisfying the following two conditions:

1. For almost all P[1], the local ring $\mathcal{O}_P$ is a discrete valuation ring.

2. For each discrete valuation ring $\mathbf{B}$ of $\mathbf{K}$ there is an unique $P \in X$ such that $\mathcal{O}_P \subseteq \mathbf{B}$.

Recall that

$$\mathcal{O}_P = \{ z \in \mathbf{K} \mid z \text{ is a regular function at } P \}.$$

By a **singular point**, we understand a point P for which $\mathcal{O}_P$ is not a discrete valuation ring. The property 1 means that the number of singular points of X is finite, we denote this set by X_{sing}. The property 2 implies that we have a surjective morphism

$$\pi : \tilde{X} \longrightarrow X$$

where $\tilde{X}$ is the smooth model of X. Note that π is a birational morphism. The pair $(\tilde{X}, \pi)$ is unique in the following sense: given another non-singular curve $\tilde{X}'$ and a birational morphism $\pi' : \tilde{X}' \longrightarrow X$, there exists a unique isomorphism $\pi'' : \tilde{X} \longmapsto \tilde{X}'$ such that $\pi = \pi' \circ \pi''$. Recall that the function

[1]That is, for all except a finite number.

field of X and $\tilde{X}$ are the same. For each point $P \in X$, the elements of the fiber $\pi^{-1}(P)$ are called the branches of X centered at P. By the extension theorem of valuation theory, there exists at least one branch centered at P. Note that the set of branches centered at P is a finite set.

By a divisor of X we mean a formal product

$$\mathbf{a} = \prod_{P \in X} \mathbf{a}_P$$

where $\mathbf{a}_P$ is a (non-zero fractional) ideal of $\mathcal{O}_P$ for each $P \in X$ and $\mathbf{a}_P = \mathcal{O}_P$ for almost all P. A divisor $\mathbf{a}$ is called locally principal (or Cartier divisor) if each component $\mathbf{a}_P$ is a principal ideal. For two divisors $\mathbf{a}$ and $\mathbf{b}$ we define the product $\mathbf{a} \cdot \mathbf{b}$ and the quotient $\mathbf{a} : \mathbf{b}$ by setting:

- $(\mathbf{a} \cdot \mathbf{b})_P := \mathbf{a}_P \cdot \mathbf{b}_P = \{ \sum a_i b_j \mid a_i \in \mathbf{a}_P \text{ and } b_j \in \mathbf{b}_P \}$
- $(\mathbf{a} : \mathbf{b})_P := \mathbf{a}_P : \mathbf{b}_P = \{ z \in \mathbf{K} \mid z\mathbf{b}_P \subseteq \mathbf{a}_P \}$.

Note that the locally principal divisors form a multiplicative group whose identity is the structure divisor

$$\mathcal{O} := \prod_{P \in X} \mathcal{O}_P.$$

We define $\mathbf{a} \geq \mathbf{b} \iff \mathbf{a}_P \supseteq \mathbf{b}_P$ for each $P \in X$ and call a divisor $\mathbf{a}$ positive if $\mathbf{a} \geq \mathcal{O}$. The degree of a divisor is defined by the following two properties:

1. $deg(\mathcal{O}) = 0$

2. $deg(\mathbf{a}) - deg(\mathbf{b}) = \sum_{P \in X} dim_{\mathbf{k}}(\mathbf{a}_P/\mathbf{b}_P)$ whenever $\mathbf{a} \geq \mathbf{b}$.

For each non-zero rational function $z \in \mathbf{K}^*$ we define the principal divisor as follows:

$$div(z) := \prod_{P \in X} z^{-1}\mathcal{O}_P.$$

Recall that $z \in \mathcal{O}_P$ for almost all $P \in X$. Let

$$\mathbf{L}(\mathbf{a}) := \bigcap_{P \in X} \mathbf{a}_P = \{ z \in \mathbf{K} \mid \mathrm{div}(z) \cdot \mathbf{a} \geq \mathcal{O} \}$$

be the $\mathbf{k}$-vector space of global sections of $\mathbf{a}$. Note that the product formula extends to the singular case:

$$deg(div(z)) = 0 \text{ for each } z \in \mathbf{K}^*.$$

Since $\mathbf{K}$ is a field in one variable with constant field $\mathbf{k}$, each integral $\mathbf{k}$-algebra A with quotient field $\mathbf{K}$ has finite $\mathbf{k}$-codimension in its integral closure $\tilde{A}$. The integer

$$\delta_P := dim_{\mathbf{k}}(\tilde{\mathcal{O}}_P/\mathcal{O}_P)$$

is called the **singularity degree** of P. The **total singularity degree** is denoted by

$$\delta := \sum_P \delta_P.$$

If we denote by $Q_1, \ldots, Q_m \in \tilde{X}$ the branches centered at P, then the integral closure

$$\tilde{\mathcal{O}}_P = \mathcal{O}_{Q_1} \bigcap \cdots \bigcap \mathcal{O}_{Q_m}$$

of $\mathcal{O}_P$ is a principal ideal domain whose maximal ideals correspond bijectively to the branches $Q_1,\ldots,Q_m$. Therefore, the divisors of the non-singular model correspond bijectively to the $\tilde{\mathcal{O}}_P$-divisors of X defined as the divisors whose P-components are $\tilde{\mathcal{O}}_P$-ideals. We assign to $Q_i \in \tilde{X}$ the ideal $m_{Q_i}^{-1}$ where m_{Q_i} is a maximal ideal of $\tilde{\mathcal{O}}_P$. The structure divisor of $\tilde{X}$ corresponds to the $\tilde{\mathcal{O}}$-divisor

$$\tilde{\mathcal{O}} := \prod_{P \in X} \tilde{\mathcal{O}}_P.$$

If $\mathfrak{a}$ is a $\tilde{\mathcal{O}}$-divisor of X corresponding to a divisor $\mathcal{A}$ of $\tilde{X}$, then

$$deg(\mathfrak{a}) = deg(\mathcal{A}) + deg(\tilde{\mathcal{O}}) = deg(\mathcal{A}) + \sum_{P \in X} \delta_P.$$

The **arithmetic genus** of X satisfies the following relation:

$$g = \tilde{g} + \sum_{P \in X} \delta_P,$$

where $\tilde{g}$ is the **geometric genus** of X defined to be the genus of the non-singular model $\tilde{X}$. From now on, we assume that the field of constants of $\mathbf{K}$ is a finite field, i.e., $\mathbf{F}_q$ where $q = p^n$. If x is a separating element, then $z \in \mathbf{K}$ can be written in a unique way as

$$z = z_0^p + z_1^p x + \cdots + z_{p-1}^p x^{p-1} \text{ where } z_0, \ldots, z_{p-1} \in \mathbf{K}.$$

The operator $\mathcal{C}$ on the differential forms is defined by setting:

$$\mathcal{C}(z\,dx) := z_{p-1}\,dx.$$

It can be proved that $\mathcal{C}(z\,dx) := -(\frac{d^{p-1}z}{dx^{p-1}})^{1/p}dx$ for each $z \in \mathbf{K}$ and each separating variable x of $\mathbf{K}/\mathbf{k}$. $\mathcal{C}$ is called the Cartier operator on the space of differential forms. $\mathcal{C}$ acts on $\Omega(\mathcal{O})$ and $\Omega(\tilde{\mathcal{O}})$, where $\Omega(\mathcal{O})$ is the space of regular differential[2] (in the sense of Stöhr, see [23, section 2]) on X and $\Omega(\tilde{\mathcal{O}})$ is the space of regular differential (in the sense of Stöhr, see [23, section 2]) on $\tilde{X}$, respectively.

Theorem 2.1. (Stöhr) *With the above notation, we have*

$$det(Id - tC^n_{\Omega(\mathcal{O})/\Omega(\tilde{\mathcal{O}})}) = \prod_{P \in X_{\text{sing}}} \frac{\prod_{Q|P}(1 - t^{deg(Q)})}{1 - t^{deg(P)}},$$

where P varies in the finite set X_{sing} of singular points of X and Q ranges over all branches centered at P and $\Omega(\mathcal{O})$ is the space of regular differentials on X and $\Omega(\tilde{\mathcal{O}})$ is the space of regular differentials on $\tilde{X}$.

In the proof of theorem 2.1, the two main results used are the following:
1. $\Omega(\mathcal{O})/\Omega(\tilde{\mathcal{O}}) \simeq \oplus_{P \in X_{\text{sing}}} \Omega(\mathcal{O}_P)/\Omega(\tilde{\mathcal{O}}_P)$, where $\Omega(\mathcal{O}_P)$ is the space of the differentials regular at P and $\Omega(\tilde{\mathcal{O}}_P)$ is the space of differentials regular at the branches centered at P.

2. If $\mathfrak{r}_P$ is the Jacobson radical of $\tilde{\mathcal{O}}_P$ and

$$\Omega(\mathcal{O}_P + \mathfrak{r}_P) = \{\, \mu \in \Omega(\mathcal{O}_P) \,|\, \text{ord}_{Q_i}(\mu) \geq -1 \text{ for each } i = 1, \ldots, m \,\}$$

[2]There is a slightly difference between the regular differential used by Stöhr and the general concept of killer differential.

and $\mathbf{k}_{Q_i}$ is the residue field of $\mathbf{K}$ at Q_i, then there exists an isomorphism

$$\Omega(\mathcal{O}_P + \mathfrak{r}_P)/\Omega(\tilde{\mathcal{O}}_P) \simeq \{(a_1, \ldots, a_m) \in \oplus_{i=1}^m \mathbf{k}_{Q_i} \mid \sum_{i=1}^m Tr_{\mathbf{k}_{Q_i}/\mathbf{k}}(a_i) = 0\}$$

defined by

$$\mu + \Omega(\tilde{\mathcal{O}}_P) \mapsto (res_{Q_1}(\mu), \ldots, res_{Q_m}(\mu)).$$

The Cartier operator induces on the vectors on right hand side the action

$$(a_1, \ldots, a_m) \mapsto (a_1^{1/p}, \ldots, a_m^{1/p})$$

The proof of 1 and 2 can be found in [23, corollary 4.1] and [24, theorem 4.3]. We will call

$$\prod_{P \in X_{sing}} \frac{\prod_{Q|P}(1 - t^{deg(Q)})}{1 - t^{deg(P)}},$$

the **Stöhr factor** of the singular curve X.

Definition 2.2. *The Zeta function of X is defined to be the Euler product*

$$Z(X, s) := \prod_{P \in X} (1 - q^{-s\,deg(P)})^{-1}, \text{ where } \Re(s) > 1.$$

With the substitution $t = q^{-s}$, (2.1) becomes

$$Z(X, t) = \prod_{P \in X} (1 - t^{deg(P)})^{-1}.$$

Therefore, we have the following relation between the zeta function of the curve X and the zeta function of the curve $\tilde{X}$:

$$M(X, t) = \frac{Z(X, t)}{Z(\tilde{X}, t)} := \prod_{P \in X_{sing}} \frac{\prod_{Q|P}(1 - t^{deg(Q)})}{1 - t^{deg(P)}}.$$

Formally, this is the same expression as in theorem 2.1; but now we are in characteristic zero. Note that the degree of P divides the degree of Q when Q is centered at P, therefore $M(X,t)$ is a monic polynomial in $\mathbf{Z}[t]$ and its zeros are roots of unity. The degree of the polynomial $M(X,t)$ is equal to

$$\deg(M(X,t)) = dim(\Omega(\mathcal{O}+\mathfrak{r})) - \tilde{g},$$

where $\mathfrak{r} = \prod_{P\in X} \mathfrak{r}_P$. By the Riemann hypothesis for non-singular curves we can write

$$Z(\tilde{X},t) = \frac{L(\tilde{X},t)}{(1-t)(1-qt)}, \tag{2.1}$$

where $L(\tilde{X},t)$ is a polynomial with integer coefficients in t, degree $2\tilde{g}$, whose zeros have absolute value $q^{1/2}$. If we put together (2.1) and (2.2) we get

$$Z(X,t) = \frac{L(X,t)}{(1-t)(1-qt)},$$

where $L(X,t) = L(\tilde{X},t)M(X,t)$ and $deg(L(X,t)) = \tilde{g} + dim(\Omega(\mathcal{O}+\mathfrak{r}) \leq 2g$.

Let $Z(\mathcal{O},s)$ be the Dirichlet series defined by:

$$Z(\mathcal{O},s) := \sum_{\mathfrak{a}\geq\mathcal{O}} q^{-s\,deg(\mathfrak{a})},$$

where the sum is taken over all positive divisors $\mathfrak{a}$ of X. $Z(\mathcal{O},s)$ converges absolutely for $\Re(s) > 1$.

Theorem 2.3. *The function $q^{s(g-1)}Z(\mathcal{O},s)$ is invariant under the substitution $s \mapsto 1-s$.*

The proof of theorem 2.3 follows from Riemann-Roch's theorem for singular curves [7, theorem 5.4]. As in the non-singular case, in the proof of theorem 2.3 one studies the divisors of degree greater than $2g-2$ and the divisors of degree less than or equal to $2g-2$.

We can write $Z(\mathcal{O},s)$ as product of local factors:

$$Z(\mathcal{O},s)=\prod_{P\in X} Z(\mathcal{O}_P,t),$$

where

$$Z(\mathcal{O}_P,s)=\sum_{\mathfrak{a}_P\supseteq\mathcal{O}_P} q^{-s\,dim_{\mathbf{k}}(\mathfrak{a}_P/\mathcal{O}_P)}.$$

Since $Z(\mathcal{O}_P,s)=(1-q^{-s\,deg(P)})^{-1}$ when P is non-singular, then we have

$$\frac{Z(\mathcal{O},s)}{Z(X,s)}=\prod_{P\in X_{sing}}(1-q^{-s\,deg(P)})Z(\mathcal{O}_P,s).$$

The local factor $Z(\mathcal{O}_P,s)$ satisfies a local functional equation, the function

$$q^{s\delta_P}Z(\mathcal{O}_P,s)\prod_{Q|P}(1-q^{-s\,deg(Q)})$$

is invariant under substitution $s\mapsto 1-s$.

In the following section we give some examples to illustrate the results of Stöhr.

2.2 Examples

In this section we analyze three examples of singular curves over a finite field. In some of the examples we use the following two results:

1. If X is a singular plane curve of degree d, then its arithmetic genus $g = \frac{1}{2}(d-1)(d-2)$.

2. If X is a curve that has only ordinary singularities, then δ is simply the number of these singular points.

In the examples below we use the following notation. Let X be an affine singular curve over $\mathbf{F}_p$. The function field of X is denoted by $\mathbf{K}(X)$. Let X' be the homogenization of X.

Example 1.

Let X be the curve defined by the equation $x^2y^2+x^2+y^2-1=0$ over $\mathbf{F}_p$. X has two singular points $P_1 = (1,0,0)$ and $P_2 = (0,1,0)$. The geometric genus of X is 1 since the P_1 and P_2 are ordinary singular points. The curve $\tilde{X}$ is defined by an equation of the form $y^2 = f(x) \in \mathbf{F}_p[x]$, where $f(x)$ is a square-free polynomial of degree 3 since the geometric genus of X is 1(see [22, chapter 6.1]). Therefore, the function field $\mathbf{K}(\tilde{X})$ of $\tilde{X}$ is a Kummer extension of $\mathbf{F}_p(x)$ of degree 2.

If $p \equiv 1 \bmod 4$, then we can write p in the form a^2+b^2 with a odd and b even. The zeta function of X' over $\mathbf{F}_p$ is

$$Z(X',t) = \frac{(1-2at+pt^2)(1-t)^2}{(1-t)(1-pt)},$$

where if $4|b$, we choose $a \equiv 1 \bmod 4$ and if $4 \nmid b$, we choose $a \equiv -1 \bmod 4$.

The calculation of the zeta function of X' can be found in [10, chapter 11.5]. Using Stöhr's theorem we have

$$\frac{Z(X,t)}{Z(\tilde{X},t)} = \left(\frac{\prod_{Q|P_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\right)\left(\frac{\prod_{Q'|P_2}(1-t^{deg(Q')})}{1-t^{deg(P_2)}}\right) = (1-t)^2.$$

If $p \equiv 3 \bmod 4$, then the zeta function of X' over $\mathbf{F}_p$ is

$$Z(X,t) = \frac{(1+pt^2)(1+t)^2}{(1-t)(1-pt)}.$$

The calculation of the zeta function of X' can be found in [10, chapter 11.5]). Using Stöhr's theorem we have

$$\frac{Z(X,t)}{Z(\tilde{X},t)} = \left(\frac{\prod_{Q|P_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\right)\left(\frac{\prod_{Q'|P_2}(1-t^{deg(Q')})}{1-t^{deg(P_2)}}\right) = (1+t)^2.$$

Example 2.

Let X be the projective curve defined by the equation $y^4+z^2y^2+z^2x^2 = 0$ over $\mathbf{F}_p$ where $p = 3$ or 5. X has two singular points $P_1 = (0,0,1)$ and $P_2 = (1,0,0)$. P_1 is an ordinary singular point and P_2 is a double singular point. The arithmetic genus of X is 3. Recall that $deg(Z(X,t)) \leq 2g$. Using the computer program Maple, we computed the number of solutions of X over $\mathbf{P}^2(\mathbf{F}_{3^i})$ and $\mathbf{P}^2(\mathbf{F}_{5^i})$ for $i = 1,\ldots,6$. These are given in the following table:

n	$\lvert V(y^4+z^2y^2+z^2x^2, p=3)\rvert$	$\lvert V(y^4+z^2y^2+z^2x^2, p=5)\rvert$
1	6	4
2	8	24
3	30	124
4	80	624
5	246	3124
6	728	15,625

Therefore, we have

$$Z(X,t,3)=\frac{(1+t)^2}{(1-t)(1-3t)},$$

and

$$Z(X,t,5)=\frac{(1-t)^2}{(1-t)(1-5t)}.$$

Using Stöhr's theorem for $p=3$ we obtain

$$\frac{Z(X',t)}{Z(\mathbf{P}^1(\mathbf{F}_p),t)}=\frac{\prod_{Q|P_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\frac{\prod_{Q'|P_2}(1-t^{deg(Q')})}{1-t^{deg(P_2)}}=(1+t)^2.$$

Stöhr's theorem also gives for $p=5$

$$\frac{Z(X',t)}{Z(\mathbf{P}^1(\mathbf{F}_p),t)}=\frac{\prod_{Q|P_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\frac{\prod_{Q'|P_2}(1-t^{deg(Q')})}{1-t^{deg(P_2)}}=(1-t)^2.$$

The above expression implies that the geometric genus of X is 0. Therefore, $\tilde{X}$ is isomorphic to $\mathbf{P}^1$.

Example 3.

Let X be the curve defined by the equation $y^2+x^4+1=0$ over $\mathbf{F}_p$. $P=(0,0,1)$ is the only singular point of X'. The arithmetic genus of X is 3. Using the Hurwitz genus formula, it can be proved that the geometric genus of

X is 1. The curve $\tilde{X}$ is defined by an equation of the form $y^2 = f(x) \in \mathbf{F}_p[x]$, where $f(x)$ is a square-free polynomial of degree 3 since the geometric genus of X is 1. Therefore, the function field $\mathbf{K}(\tilde{X})$ of $\tilde{X}$ is a Kummer extension of $\mathbf{F}_p(x)$ of degree 2. If $p \equiv 1 \bmod 4$, then the zeta function of X over $\mathbf{F}_p$ is

$$Z(X,t) = \frac{(1-at+pt^2)(1-t)}{(1-t)(1-pt)},$$

where $a \in \mathbf{Z}[x]$. This is an application of theorem 5 of chapter 8 on [10]. Using Stöhr's theorem we get

$$\frac{Z(X,t)}{Z(\mathbf{P}^1,t)} = \frac{\prod_{Q|P}(1-t^{deg(Q)})}{1-t^{deg(P)}} = (1-t).$$

If $p \equiv 3 \bmod 4$, then the zeta function of X over $\mathbf{F}_p$ is

$$Z(X,t) = \frac{(1+pt^2)(1+t)}{(1-t)(1-pt)}.$$

This is followed by an application of theorem 5 of chapter 8 on [10]. Using Stöhr's theorem, we have

$$\frac{Z(X,t)}{Z(\mathbf{P}^1,t)} = \frac{\prod_{Q|P}(1-t^{deg(Q)})}{1-t^{deg(P)}} = (1+t).$$

2.3 Definition of L-functions over $\mathbf{F}_q$

In this section we are going to define the L-function for any curve that is an abelian covering of the projective line. It is well known that if the curve over the finite field is non-singular, then the L-functions associated to the curve are polynomials. We prove that if the singular curve defined over a finite

field is an abelian covering of the projective line, then the zeta function of the singular curve factors as product of L-functions where the factors are not necessarily rational functions.

Let X be a curve over a finite field $\mathbf{F}_q$. We are going to assume that the geometric genus $\tilde{g}$ of X is greater than zero. Let $\mathbf{K}$ be the function field of X and let $\mathbf{F}_q$ be its field of constants. Let $\pi : \tilde{X} \longrightarrow X$ be a morphism, where $\tilde{X}$ is the smooth model of X and let $\pi_0 : \tilde{X} \longrightarrow \mathbf{P}^1$ be a covering of the projective line. We assume that π_0 is an abelian covering of degree n, i.e., $\mathbf{K}$ is an abelian extension of $\mathbf{F}_q(x)$ of degree n for some $x \in \mathbf{K}$. Let G be the Galois group of the extension $\mathbf{K}/\mathbf{F}_q(x)$. Let χ be a character of G. Let $\mathcal{O}_P$ be the ring of regular function at $P \in X$ and let $\tilde{\mathcal{O}}_P$ be the integral closure of $\mathcal{O}_P$ in $\mathbf{K}$. We assume that X has at least one singular point. Let P be a singular point of X and let $Q_1,\ldots,Q_m \in \tilde{X}$ be the branches centered at P, i.e., $\pi^{-1}(P) = \{Q_1,\ldots,Q_m\}$. We have the following: diagram

$$\begin{array}{ccccc} Q_1,\cdots Q_m & \tilde{\mathcal{O}}_P & \mathbf{K} & \tilde{\mathcal{O}}_P/Q \\ \backslash/ & | & & | \\ P & \mathcal{O}_P & & \mathcal{O}_P/P \\ | & | & & | \\ p & \mathcal{O}_p & \mathbf{F}_q(x) & \mathcal{O}_p/p \end{array}$$

For each $p \in \mathbf{P}^1$ we have $n = f(p)g(p)e(p)$, where $f(p)$ is the degree of any point of $\tilde{X}$ lying above p, $g(p)$ is the cardinality of $\pi_0^{-1}(p)$ and $e(p)$ is the ramification of p in $\tilde{X}$. Let $D(p)$ be the decomposition group of Q, let $I(p)$

be the inertia group of Q, where Q is a branch centered at P. Let

$$N(P|p) = \{\, \sigma \in D(p) \,|\, \sigma(x) \equiv x \bmod P \text{ for every } x \in \mathcal{O}_P \,\}.$$

Let $f'(p)$ be equal to the cardinality of $D(P|p)/N(P|p)$. Note that $f'(p)$ divides $f(p)$. For $P \in X_{\text{sing}}$ we have two cases: $m = g(p)$ and $m \neq g(p)$. If $m \neq g(p)$, then there exists $P_1,\ldots,P_l$ distinct singular points in X including P such that $g(p) = \sum_{i=1}^{l} |\pi^{-1}(P_i)|$, where $|\pi^{-1}(P_i)|$ is the cardinality of $\pi^{-1}(P_i)$. We say $P_1, P_2 \in X_{\text{sing}}$ are equivalent if P_1 and P_2 lie above the same point in $\mathbf{P}^1$. This is an equivalence relation on the set X_{sing}. We will denote the set of all equivalence classes of X_{sing} by $\overline{X}_{\text{sing}}$. If $P_1,\ldots,P_l$ are singular points of X lie above p in $\mathbf{P}^1$, then they will count as one point with multiplicity l and we will denote the multiplicity of $P|p$ by $l(p)$. Let F_p be Frobenius automorphism.

Definition 2.4. *Let X be a singular curve defined over $\mathbf{F}_q$ and let $\pi_0 : \tilde{X} \longrightarrow \mathbf{P}^1$ be an abelian covering of $\mathbf{P}^1$, then the* **L-function** *of X is given by*

$$L(X/\mathbf{P}^1, t, \chi) = L(\tilde{X}/\mathbf{P}^1, t, \chi) \prod_{\substack{P \in \overline{X}_{\text{sing}} \\ P|p}} \frac{(1 - \chi(F_p) t^{deg(p)})^{r(p)}}{\left(1 - \chi(F_p^{\frac{f(p)}{f'(p)}}) t^{deg(p)}\right)^{\frac{l(p) f'(p) r(p)}{f(p) g(p)}}},$$

where $L(\tilde{X}, t, \chi)$ is the ordinary L-function of $\tilde{X}$ associated to χ and

$$r(p) = \begin{cases} 1 & \text{if } \chi(I(p)) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Remark. Note that $r(p)$ depends on χ.

The next theorem, which is our principal result, gives the relation between the L-functions of the singular curve X and the Stöhr zeta function:

Theorem 2.5. *Let X be a curve over $\mathbf{F}_q$ and let $\pi_0 : \tilde{X} \longrightarrow \mathbf{P}^1$ be an abelian covering of $\mathbf{P}^1$, then with notation as above, we have*

$$Z(X,t) = \prod_{\chi \in \widehat{G}} L(X/\mathbf{P}^1, t, \chi).$$

Proof. In the proof of theorem 2.5, we are going to factor the Stöhr factor into a product of functions where the product runs over all the character of G. We can assume that X has at least one singular point since the theorem 2.5 is true for non-singular curves. Let P be a singular point of X, then P lies above a point $p \in \mathbf{P}^1$. Let $Q_1,\ldots,Q_m$ branches centered at P. We have two cases $g(p) = m$ and $g(p) \neq m$. First we prove the theorem when $g(p) = m$ and then the other case will follow easily.

1. If $g(p) = m$, then we can assume that X has only one singular point P since the question is local. To simplify the notation let $n = gfe$ and $r = r(p)$ and let $N(P|p) = N$. In this case we have

$$\frac{Z(X,t)}{Z(\tilde{X},t)} = \frac{(1-t^{deg(Q)})^g}{1-t^{deg(P)}} = \frac{\prod_{Q|p}(1-t^{deg(Q)})}{1-t^{deg(P)}}.$$

In this case, the L-function becomes

$$L(X/\mathbf{P}^1,t,\chi)=L(\tilde{X}/\mathbf{P}^1,t,\chi)\frac{(1-\chi(F_p)t^{deg(p)})^r}{(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'r}{fg}}}.$$

We need to prove the following

$$\begin{aligned} Z(X,t) &= \prod_{\chi\in\widehat{G}} L(X/\mathbf{P}^1,t,\chi) \\ &= \Big(\prod_{\chi\in\widehat{G}} L(\tilde{X}/\mathbf{P}^1,t,\chi)\frac{(1-\chi(F_p)t^{deg(p)})^r}{(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'r}{fg}}}\Big) \end{aligned}$$

or equivalently

$$\frac{Z(X,t)}{\prod_{\chi\in\widehat{G}} L(\tilde{X}/\mathbf{P}^1,t,\chi)}=\prod_{\chi\in\widehat{G}}\frac{(1-\chi(F_p)t^{deg(p)})^r}{(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'r}{fg}}}.$$

Using the following identity between zeta and L-functions for non-singular curves

$$Z(\tilde{X}/\mathbf{P}^1)=\prod_{\chi\in\widehat{G}} L(\tilde{X}/\mathbf{P}^1,\chi).$$

We get

$$\frac{Z(X,t)}{Z(\tilde{X},t)}=\prod_{\chi\in\widehat{G}}\frac{(1-\chi(F_p)t^{deg(p)})^r}{(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'r}{fg}}}.$$

Therefore, we need to prove that the right side of the last equation is equal to the Stöhr factor:

$$\prod_{\chi\in\widehat{G}}\frac{(1-\chi(F_p)t^{deg(p)})^r}{(1-\chi(F_p)t^{deg(p)})^{\frac{f'r}{fg}}}=\frac{(1-t^{deg(Q)})^g}{1-t^{deg(P)}}.$$

Now, we are going to prove

$$\prod_{\chi\in\widehat{G}}(1-\chi(F_p)t^{deg(p)})^r=(1-t^{deg(Q)})^g$$

and

$$\prod_{\chi\in\widehat{G}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'r}{fg}}=1-t^{deg(P)}.$$

We consider two cases: p ramifies in $\mathbf{K}$ and p does not ramify in $\mathbf{K}$.

A. If p is unramified in $\mathbf{K}$, then we need to prove

$$\prod_{\chi\in\widehat{G}}\frac{(1-\chi(F_p)t^{deg(p)})}{(1-\chi(F_p)t^{deg(p)})^{\frac{f'r}{fg}}}=\frac{(1-t^{deg(Q)})^g}{1-t^{deg(P)}}.$$

Claim. If p is unramified in $\mathbf{K}$, then

$$\prod_{\chi\in\widehat{G}}(1-\chi(F_p)t^{deg(p)})=(1-t^{deg(Q)})^g, \tag{2.2}$$

where F_p is the generator of $D(p)$, i.e., the Frobenius automorphism.

Proof. Note that $\chi(1)=\chi(F_p^f)=\chi^f(F_p)=1$, therefore $\chi(F_p)$ is an f-root of unity.

Subclaim. There exists $\chi\in\hat{G}$ such that $\chi(F_p)$ is an f-th primitive root of unity.

We prove the subclaim by contradiction. We suppose that there exists a n such that $\chi^n(F_p)=1$ for every $\chi\in\hat{G}$ and $0<n<f$. This implies that $\chi(F_p^n)=1$ for every $\chi\in\hat{G}$. Then $F_p^n=1$. This is a contradiction since the order of F_p is f. This proves the subclaim.

Let $\widehat{H}=\{\chi\in\hat{G}\,|\,\chi(F_p)=1\}=\{\chi\in\hat{G}\,|\,\chi(D(p))=1\}$. We can identify the characters of G trivial on $D(p)$ with $\widehat{G/D(p)}$ where $G/D(p)$ is the group

of characters of $G/D(p)$. This implies that $|\widehat{H}| = g$. Let χ be the character of G such that satisfies the following: $\chi(F_p)$ is an f-th primitive root of unity. Note

$$\chi\psi(F_p) = \chi(F_p)$$

for every $\psi \in \widehat{H}$. We consider $\widehat{H}, \chi\widehat{H}, \ldots, \chi^{f-1}\widehat{H}$, note that each one is an equivalence class of $\widehat{G}/\widehat{H}$. Let χ_i be a representative of the class $\chi^i\widehat{H}$, then

$$\prod_{i=0}^{f-1}(1 - \chi_i(F_p)t^{deg(p)}) = 1 - t^{fdeg(p)} = 1 - t^{deg(Q)}.$$

If we repeat the above for all the elements of each equivalence class, we get

$$\prod_{\psi\in\widehat{H}}\prod_{i=0}^{f-1}(1 - \chi_i\psi(F_p)t^{deg(p)}) = \prod_{j=1}^{g}\prod_{i=0}^{f-1}(1 - \chi_i\psi(F_p)t^{deg(p)}) = (1 - t^{deg(Q)})^g.$$

This proves the claim.

Claim. If p is unramified, then

$$1 - t^{deg(P)} = \prod_{\chi\in\widehat{G}}(1 - \chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}}, \tag{2.3}$$

where $f' = |D(p)/N|$ and F_p is the Frobenius automorphism. Recall that $deg(P) = deg(\mathcal{O}_P/P/\mathcal{O}_p/p) \times deg(p)$. Since $\widehat{D(p)}$ is a cyclic group, then we can write

$$\prod_{\chi\in\widehat{D(p)}}(1 - \chi(F_p)t^{deg(p)}) = \prod_{i=1}^{f}(1 - \psi^i(F_p)t^{deg(p)}),$$

where $\psi(F_p)$ is an f-th root of unity . Note f' divide f and $\frac{deg(P)}{deg(p)} = f'$. We have that $\psi(F_p^{\frac{f}{f'}})$ is an f'-th primitive root of unity. Therefore, we can substitute F_p by $F_p^{\frac{f}{f'}}$ in the last equation. We get

$$\begin{aligned}
\prod_{x\in\widehat{D(p)}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}} &= \prod_{i=1}^{f}(1-\psi^i(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}} \\
&= \prod_{j=1}^{\frac{f}{f'}}\prod_{i=1}^{f'}(1-\psi^i(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}} \\
&= \prod_{i=1}^{f'}(1-\psi^i(F_p^{\frac{f}{f'}})t^{deg(p)}) \\
&= 1-t^{f'deg(p)} \\
&= 1-t^{deg(P)}.
\end{aligned}$$

We can extend $\prod_{x\in\widehat{D(p)}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}}$ to a product over all $\hat{G}$ by setting

$$\prod_{x\in\widehat{D(p)}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}} = \prod_{x\in\hat{G}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}}$$

since there are g characters trivial on $\widehat{D(p)}$. This proves the claim. If we put together (2.2) and (2.3), we get

$$\frac{Z(X,t)}{Z(\tilde{X},t)} = \frac{(1-t^{deg(Q)})^g}{1-t^{deg(P)}} = \prod_{x\in\hat{G}}\frac{(1-\chi(Fr_p)t^{deg(p)})}{(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}}}.$$

This proves the theorem 2.5 is true when $g=m$ and p is unramified.

B. If p ramifies in $\mathbf{K}$, we need to prove

$$\prod_{x\in\hat{G}}\frac{(1-\chi(F_p)t^{deg(p)})^r}{(1-\chi(F_p)t^{deg(p)})^{\frac{f'r}{fg}}} = \frac{(1-t^{deg(Q)})^g}{1-t^{deg(P)}}.$$

Claim. If p ramifies in $\mathbf{K}$, then

$$\prod_{\chi\in\widehat{G}}(1-\chi(F_p)t^{deg(p)})^r=(1-t^{deg(Q)})^g \tag{2.4}$$

where F_p is a representative of the Frobenius equivalence class and

$$r=\begin{cases}1 & \text{if } \chi(I(p))=1\\ 0 & \text{otherwise.}\end{cases}$$

We identify the characters of $G/D(p)$ with the characters of G trivial on $D(p)$. Therefore, there are g characters χ of G such that $\chi(D(p))=1$. $\chi(Fr_p)$ is an f-th primitive root of unity for some $\chi\in\widehat{G}$. It was proved in case **A**.

Let χ be a character of G such that $\chi(F_p)$ is an f-th primitive root of unity. Then, we have

$$\begin{aligned}\prod_{\substack{\chi\in\widehat{G}\\ \chi(I(p))=1}}(1-\chi(F_p)t^{deg(p)}) &= \prod_{\chi\in\widehat{G/I(p)}}(1-\chi(F_p)t^{deg(p)})\\ &= \prod_{\substack{\psi\in\widehat{G/I(p)}\\ \psi(D(p)/I(p))=1}}\prod_{i=1}^{f}(1-\chi^i\psi(F_p)t^{deg(p)})\\ &= \prod_{\substack{\psi\in\widehat{G/I(p)}\\ \psi(D(p)/I(p))=1}}(1-t^{f\,deg(p)})\\ &= (1-t^{deg(Q)})^g.\end{aligned}$$

We can write the above as

$$(1-t^{deg(Q)})^g=\prod_{\chi\in\widehat{G}}(1-\chi(F_p)t^{deg(p)})^r,$$

where

$$r = \begin{cases} 1 & \text{if } \chi(I(p)) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Claim. If p ramifies, then

$$1 - t^{deg(P)} = \prod_{\chi \in \widehat{G}} (1 - \chi(F_p^{\frac{f}{f'}}) t^{deg(p)})^{\frac{f'r}{fg}}, \tag{2.5}$$

where F_p is a representative of the Frobenius conjugacy class and $f' = |G/N|$.

Subclaim. $I(p) \subseteq N$.

Proof. If $\sigma \in I(p)$, then $\sigma(x) \equiv x \bmod Q$ for every $x \in \tilde{\mathcal{O}}_P$. Therefore, if $x \in \mathcal{O}_P$ and $\sigma(x) - x \notin P$, then $\sigma(x) - x$ is a unit in $\mathcal{O}_P$. Therefore $\sigma(x) - x \notin Q$, this is a contradiction, hence we can conclude that

$$\sigma(x) \equiv x \bmod P$$

for every $x \in \mathcal{O}_P$. This proves that $\sigma \in N$.

We have

$$\prod_{\substack{\chi \in \widehat{D(p)} \\ \chi(I(p))=1}} (1 - \chi(F_p) t^{deg(p)}) = \prod_{i=1}^{f} (1 - \psi^i(F_p) t^{deg(p)}),$$

where $\psi \in \widehat{D(p)}$ and $\psi(F_p)$ is a primitive f-th root of unity. The last statement is true since $D(p)/I(p)$ is a cyclic of order f. Therefore, we can substitute F_p by $F_p^{\frac{f}{f'}}$ in the last equation. We get

$$\prod_{\substack{\chi \in \widehat{D(p)} \\ \chi(I(p))=1}} (1 - \chi(F_p^{\frac{f}{f'}}) t^{deg(p)})^{\frac{f'}{f}} = \prod_{i=1}^{f} (1 - \psi^i(F_p^{\frac{f}{f'}}) t^{deg(p)})^{\frac{f'}{f}},$$

where $\psi(F_p^{\frac{f}{f'}})$ is a primitive f'-th root of unity. Therefore, we have

$$\begin{aligned}\prod_{\substack{\chi\in\widehat{D(p)}\\ \chi(I(p))=1}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}} &= \prod_{j=1}^{\frac{f}{f'}}\prod_{i=1}^{f'}(1-\psi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}}\\ &= \prod_{i=1}^{f'}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})\\ &= 1-t^{f'deg(p)}\\ &= 1-t^{deg(P)}.\end{aligned}$$

This proves the claim. We need to extend the above product to all $\hat{G}$. The next step is to prove the following:

Subclaim.

$$\prod_{\substack{\chi\in\widehat{D(p)}\\ \chi(I(p))=1}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}} = \prod_{\substack{\chi\in\widehat{G}\\ \chi(I(p))=1}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}}$$

Proof. We have

$$\begin{aligned}\prod_{\substack{\chi\in\widehat{G}\\ \chi(I(p))=1}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}} &= \prod_{\chi\in\widehat{G/I(p)}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}}\\ &= \prod_{\substack{\chi\in\widehat{G/I(p)}\\ \chi(D(p)/I(p))=1}}\prod_{i=1}^{f}(1-\psi^i\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}},\end{aligned}$$

where $\psi(F_p)$ is a primitive f-th root of unity. Then

$$\prod_{\substack{\chi\in\widehat{G}\\ \chi(I(p))=1}}(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}} = \prod_{i=1}^{f}(1-\psi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}},$$

since there are g characters of G trivial on $D(p)$. Therefore, we have proved that

$$\prod_{\substack{\chi\in\widehat{G}\\ \chi(I(p))=1}} (1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{fg}} = \prod_{\substack{\chi\in\widehat{D(p)}\\ \chi(I(p))=1}} (1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'}{f}}.$$

This proves the subclaim. We extend the above product to all $\hat{G}$ by setting

$$1-t^{deg(P)} = \prod_{\chi\in\hat{G}} (1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'r}{fg}},$$

where

$$r = \begin{cases} 1 & \text{if } \chi(I(p)) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

If we put together (2.4) and (2.5) we get

$$\frac{Z(X,t)}{Z(\tilde{X},t)} = \frac{(1-t^{deg(Q)})^g}{1-t^{deg(P)}} = \prod_{\chi\in\hat{G}} \frac{(1-\chi(Fr_p)t^{deg(p)})^r}{(1-\chi(F_p^{\frac{f}{f'}})t^{deg(p)})^{\frac{f'r}{fg}}},$$

where

$$r = \begin{cases} 1 & \text{if } \chi(I(p)) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

This proves **B**, i.e., p ramifies in **K**. We have proved the theorem 2.5 when $g(p) = m$.

2. If $g(p) \neq m$ then we can assume that there are only two singular points P_1 and P_2 lying above p and these are the only two singular points of X. Then $|\pi^{-1}(P_1)| + |\pi^{-1}(P_2)| = g(p)$. Let $Q_1,\ldots,Q_m,Q_{m+1}\ldots,Q_{g(p)}$ be the prime ideals of **K** lying above p. Let $Q_1,\ldots,Q_m$ be the prime ideals of $\tilde{\mathcal{O}}_{P_1}$ and let

$Q_{m+1},\ldots,Q_{g(p)}$ be the prime ideals of $\tilde{\mathcal{O}}_{P_2}$. Recall that G acts transitively on the ideals of $\mathbf{K}$ lying above p.

Claim. $|\pi^{-1}(P_1)| = |\pi^{-1}(P_2)|$

Proof. There exists a $\sigma \in G$ such that $\sigma(P_1) = P_2$ since G acts transitively on the ideals of $\mathbf{K}$ lying above p. It proves the claim since $P_1 = Q_1 \cdots Q_m$.

Claim. $\mathcal{O}_{P_1}/P_1 \simeq \mathcal{O}_{P_2}/P_2$

Proof. Since there exists a $\sigma \in G$ such $\sigma(P_1) = P_2$, then we can define a map η from

$$\mathcal{O}_{P_1}/P_1 \longrightarrow \mathcal{O}_{P_2}/P_2$$

by setting

$$x + P_1 \mapsto \sigma(x) + P_2.$$

This is an isomorphism since σ is a automorphism of $\mathbf{K}$. In particular, this implies that $deg(P_1) = deg(P_2)$. Therefore,

$$\begin{aligned} \frac{Z(X,t)}{Z(\tilde{X},t)} &= \left(\frac{\prod_{Q|P_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\right)\left(\frac{\prod_{Q|P_2}(1-t^{deg(Q)})}{1-t^{deg(P_2)}}\right) \\ &= \frac{\prod_{Q|p}(1-t^{deg(Q)})}{(1-t^{deg(P_1)})^2}. \end{aligned}$$

We have reduced case two, i.e., $g(p) \neq m$ to the first case, therefore we have proved the theorem 2.5.

The L-functions associated to X satisfy the following:

Theorem 2.6. *Let X be a curve over $\mathbf{F}_q$ and let $\pi_0 : \tilde{X} \longrightarrow \mathbf{P}^1$ be an abelian covering of the projective line. Let $\mathbf{K}/\mathbf{F}_q(x)$ be the separable extension associated to the covering π_0 and let G be the Galois group of the extension $\mathbf{K}/\mathbf{F}_q(x)$. If χ_1 and χ_2 are characters of G, then*

$$L(X, t, \chi_1 + \chi_2) = L(X, t, \chi_1)L(X, t, \chi_2)$$

Proof. Since

$$\begin{aligned}\log(L(X,t,\chi_1)) &= \log(L(\tilde{X},t,\chi_1)) + \sum_{P|p\in\overline{X}_{sing}} r(p)\log(1-\chi_1(F_p)t^{deg(p)}) \\ &\quad -\frac{l(p)f'(p)r(p)}{f(p)g(p)}\log(1-\chi_1(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)}),\end{aligned}$$

we only need to prove that

$$\sum_{P|p\in\overline{X}_{sing}} r(p)(1-(\chi_1(F_p))t^{deg(p)})^{r(p)} - \frac{l(p)f'(p)r(p)}{f(p)g(p)}\log(1-\chi_1(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)})$$

satisfies the theorem 2.6. Using the Taylor expansion of log, we get

$$\begin{aligned}\sum_{P|p\in\overline{X}_{sing}} -r(p)\Big((1+\chi_1(F_p)t^{deg(p)} + \chi_1(F_p^2)t^{2\,deg(p)} + \cdots) - \\ \frac{l(p)f'(p)}{f(p)g(p)}(1+\chi_1(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)} + \cdots)\Big).\end{aligned}$$

The above expression is clearly additive. This proves the theorem 2.6.

Corollary 2.7. (Funtional Equation) *Let X be a curve over $\mathbf{F}_q$ and let $\pi_0 : \tilde{X} \longrightarrow \mathbf{P}^1$ be an abelian covering of the projective line. Let $\mathbf{K}/\mathbf{F}_q(x)$ be*

the abelian extension associated to the covering π_0 and let G be the Galois group of the extension $\mathbf{K}/\mathbf{F}_q(x)$. Let χ a character of G, then

$$\frac{L(1/qt, X, \overline{\chi})}{L(t, X, \chi)} = \epsilon(\chi)(\sqrt{q}/t)^{2\tilde{g}-2+\mathcal{F}} \prod_{\substack{P \in \overline{X}_{sing} \\ P|p}} \left(\frac{(1-\chi(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)})}{(1-\overline{\chi}(F_p^{\frac{f(p)}{f'(p)}})(tq)^{-deg(p)})} \right)^{\frac{l(p)f'(p)r(p)}{f(p)g(p)}} \times$$
$$\left(\frac{(1-\overline{\chi}(F_p)(tq)^{-deg(p)})}{1-\chi(F_p)t^{deg(p)}} \right)^{r(p)},$$

where $|\epsilon(\chi)| = 1$ and $\mathcal{F}$ is the degree of the conductor of χ and $\tilde{g}$ is the geometric genus of X.

Proof. The last corollary is a direct consequence of the definition of L-function for singular curve and the functional equation of the L-functions of non-singular curves, i.e.,

$$L(\tilde{X}, \frac{1}{qt}, \chi^{-1}) = \epsilon(\chi)(\sqrt{q}/t)^{2\tilde{g}-2+\mathcal{F}} L(\tilde{X}, t, \chi).$$

Now we are ready to compute the L-functions associated to the curves of the examples 1 and 3 of the section 2.3. We continue using the notation of the examples of section 2.2.

Examples of L-functions.

1. **(Gauss' Last Entry)** Let X be the curve defined by the equation $x^2y^2 + x^2 + y^2 - 1 = 0$ over $\mathbf{F}_p$. Recall that the function field $\mathbf{K}(X)/\mathbf{F}_q(x)$ has degree 2. The points $P_1 = (1,0,0)$ and $P_2 = (0,1,0)$ in X lie above two points p_1

and p_2 in $\mathbf{P}^1$. Note that $p_1 \neq p_2$ since this contradicts the form of the zeta function. Therefore $g(p_i) = |\pi^{-1}(P_i)|$ for $i = 1, 2$.

A. If $p \equiv 1 \bmod 4$, then by Stöhr's theorem we have

$$\begin{aligned}\frac{Z(X,t)}{Z(\tilde{X},t)} &= \Big(\frac{\prod_{Q|P_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\Big)\Big(\frac{\prod_{Q|P_2}(1-t^{deg(Q)})}{1-t^{deg(P_2)}}\Big) \\ &= \Big(\frac{\prod_{Q|p_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\Big)\Big(\frac{\prod_{Q|p_2}(1-t^{deg(Q)})}{1-t^{deg(P_2)}}\Big) \\ &= (1-t)^2.\end{aligned}$$

The above implies

$$\frac{\prod_{Q|p_i}(1-t^{deg(Q)})}{1-t^{deg(P_i)}} = 1-t \text{ for } i = 1, 2.$$

Therefore, $f(p_i) = 1, e(p_i) = 1$ and $g(p_i) = 2$ for $i = 1, 2$. This implies that $F_{p_i} = 1$ for $i = 1, 2$. Let χ and 1 be the characters of G. The L-functions of associated to the curve X are the following:

a. The L-function associated to the non-trivial character χ is

$$\begin{aligned}L(X,t,\chi) &= L(\tilde{X},t,\chi)\Big(\frac{1-\chi(F_{p_1})t}{(1-\chi(F_{p_1})t)^{1/2}}\Big)\Big(\frac{1-\chi(F_{p_2})t}{(1-\chi(F_{p_2})t)^{1/2}}\Big) \\ &= L(\tilde{X},t,\chi)\frac{1-t}{(1-t)^{1/2}}\frac{1-t}{(1-t)^{1/2}} \\ &= (1-2a+pt^2)(1-t).\end{aligned}$$

In particular,

- $L(X,t,\chi,p=5) = (1+2t+5t^2)(1-t)$

- $L(X,t,\chi,p=13)=(1-6t+13t^2)(1-t)$
- $L(X,t,\chi,p=17)=(1-3t+17t^2)(1-t)$.

We have found a factorization of the zeta function corresponding to the Gauss' Last Entry.

b. The L-function associated to the trivial character 1 is

$$\begin{aligned} L(X,t,1) &= L(\tilde{X},t,1)\Big(\frac{1-t}{(1-t)^{1/2}}\Big)\Big(\frac{1-t}{(1-t)^{1/2}}\Big) \\ &= L(\mathbf{P}^1,t,1)(1-t) \\ &= (1-pt). \end{aligned}$$

B. If $p \equiv 3 \bmod 4$, then by Stöhr's theorem we have

$$\begin{aligned} \frac{Z(X,t)}{Z(\tilde{X},t)} &= \Big(\frac{\prod_{Q|P_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\Big)\Big(\frac{\prod_{Q|P_2}(1-t^{deg(Q)})}{1-t^{deg(P_2)}}\Big) \\ &= \Big(\frac{\prod_{Q|p_1}(1-t^{deg(Q)})}{1-t^{deg(P_1)}}\Big)\Big(\frac{\prod_{Q|p_2}(1-t^{deg(Q)})}{1-t^{deg(P_2)}}\Big) \\ &= (1+t)^2. \end{aligned}$$

This implies

$$\frac{\prod_{Q|p_i}(1-t^{deg(Q)})}{1-t^{deg(P_i)}} = 1+t \text{ for } i=1,2.$$

Therefore, $f(p_i)=2$, $e(p_i)=2$, $g(p_i)=1$ and $f'(p_i)=1$ for $i=1,2$. Let χ and 1 be the characters of G. The L-functions associated to the curve X are

a. The L-function associated to the non-trivial character χ is

$$\begin{aligned} L(X,t,\chi) &= L(\tilde{X},t,\chi)\Big(\frac{1-\chi(F_{p_1})t}{(1-\chi(F_{p_1}^2)t)^{1/2}}\Big)\Big(\frac{1-\chi(F_{p_2})t}{(1-\chi(F_{p_2}^2)t)^{1/2}}\Big) \\ &= L(\tilde{X},t,\chi)\frac{1+t}{(1-t)^{1/2}}\frac{1+t}{(1-t)^{1/2}} \\ &= \frac{(1+t)^2(1+pt^2)}{1-t}. \end{aligned}$$

b. The L-function associated to the trivial character 1 is

$$\begin{aligned} L(X,t,1) &= L(\tilde{X},t,1)\Big(\frac{1-t}{(1-t)^{1/2}}\Big)\Big(\frac{1-t}{(1-t)^{1/2}}\Big) \\ &= L(\mathbf{P}^1,t,1)(1-t) \\ &= \frac{1}{(1-pt)}. \end{aligned}$$

2. Let X be a curve defined by the equation $y^2+x^4+1=0$ over $\mathbf{F}_p$. Recall that the field extension $\mathbf{K}(X)/\mathbf{F}_p(x)$ has degree 2. The point $P=(0,1,0)$ in X is lying above a point p in $\mathbf{P}^1$. This implies $g(p)=\pi^{-1}(P)$.

A. If $p \equiv 1 \bmod 4$, then by Stöhr's theorem we have

$$\begin{aligned} \frac{Z(X,t)}{Z(\tilde{X},t)} &= \frac{\prod_{Q|P}(1-t^{deg(Q)})}{1-t^{deg(P)}} \\ &= \frac{\prod_{Q|p}(1-t^{deg(Q)})}{1-t^{deg(p)}} \\ &= (1-t). \end{aligned}$$

Therefore, $f(p)=1$, $e(p)=1$ and $g(p)=2$. Let χ and 1 be the characters of the G. The L-functions associated to the curve X are

a. The L-function associated to the non-trivial character χ is

$$\begin{aligned} L(X,t,\chi) &= L(\tilde{X},t,\chi)\frac{(1-\chi(F_p)t)}{(1-\chi(F_p)t)^{1/2}} \\ &= L(\tilde{X},t,\chi)\frac{1-t}{(1-t)^{1/2}} \\ &= (1-at+pt^2)(1-t)^{1/2}. \end{aligned}$$

This example proves that $L(t,X,\chi)$ is not a polynomial in general. In particular,

- $L(X,t,p=5,\chi) = (1-2t+5t^2)(1-t)^{1/2}$
- $L(X,t,p=13,\chi) = (1+6t+13t^2)(1-t)^{1/2}$
- $L(X,t,p=17,\chi) = (1-2t+17t^2)(1-t)^{1/2}$.

b. The L-function associated to the trivial character 1 is

$$\begin{aligned} L(X,t,1) &= L(\tilde{X},t,1)\frac{1-t}{(1-t)^{1/2}} \\ &= L(\mathbf{P}^1,t,1)(1-t)^{1/2} \\ &= \frac{1}{(1-pt)(1-t)^{1/2}}. \end{aligned}$$

B. If $p \equiv 3 \bmod 4$, then by Stöhr's theorem we have

$$\begin{aligned} \frac{Z(X,t)}{Z(\tilde{X},t)} &= \frac{\prod_{Q|P}(1-t^{deg(Q)})}{1-t^{deg(P)}} \\ &= \frac{\prod_{Q|p}(1-t^{deg(Q)})}{1-t^{deg(p)}} \\ &= (1+t). \end{aligned}$$

Therefore, $f(p) = 2$, $e(p) = 1$ and $g(p) = 1$. Let χ and 1 be the characters of the G. The L-functions associated to the curve X are

a. The L-function associated to the non-trivial character χ is

$$\begin{aligned} L(X,t,\chi) &= L(\tilde{X},t,\chi)\frac{(1-\chi(F_p)t)}{(1-\chi(F_p^2)t)} \\ &= L(\tilde{X},t,\chi)\frac{1+t}{(1-t)^{1/2}} \\ &= \frac{(1-at+pt^2)(1+t)}{(1-t)^{1/2}}. \end{aligned}$$

The L-function associated to the trivial character 1 is

$$\begin{aligned} L(X,t,1) &= L(\tilde{X},t,1)\frac{1-t}{(1-t)^{1/2}} \\ &= L(\mathbf{P}^1,t,1)(1-t)^{1/2} \\ &= \frac{1}{(1-pt)(1-t)^{1/2}}. \end{aligned}$$

We can substitute in proof of theorem 2.5 the projective line by a non-singular curve since the argument in the proof is local. In the next section we associate to X an exponential sum in a natural way.

2.4 Exponential Sums associated to Singular Curves

In this section we define the exponential sums of a singular curve. This exponential sums consist of the exponential sum associated to the non-singular

model of the curve and some weight given by the singular points of the curve. The weight that will come from a singular point is of the form $a\zeta$, where $a \in \mathbf{Q}$ and ζ is a root of unity. We continue using the notation of the last section.

Let X be a curve over $\mathbf{F}_q$ that is an abelian covering of $\mathbf{P}^1$, then we apply logarithmic differentiation to

$$L(X,\mathbf{P}^1,t,\chi) = L(\tilde{X}/\mathbf{P}^1,t,\chi) \prod_{\substack{P\in\overline{X}_{sing}\\ P|p}} \frac{(1-\chi(F_p)t^{deg(p)})^{r(p)}}{(1-\chi(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)})^{\frac{l(p)f'(p)r(p)}{f(p)g(p)}}}$$

and multiplying by t, we get

$$\frac{t\,d\log(L(\chi,X/\mathbf{P}^1,t))}{dt} = \frac{t\,d\log(L(\chi,\tilde{X}/\mathbf{P}^1,t))}{dt} + \sum_{\substack{P\in\overline{X}_{sing}\\ P|p}} r(p)\Big(\frac{t\,d\log(1-\chi(F_p)t^{deg(p)}))}{dt}$$

$$-\frac{t\,d\log(1-\chi(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)}))^{\frac{f'(p)}{f(p)g(p)l(p)}}}{dt}\Big)$$

$$= \sum_{p\in\mathbf{P}^1} \frac{deg(p)\chi(F_p)t^{deg(p)}}{1-\chi(F_p)t^{deg(p)}} + \sum_{\substack{P\in\overline{X}_{sing}\\ P|p}} r(p)\Big(\frac{-deg(p)\chi(F_p)t^{deg(p)}}{1-\chi(Fr_p)t^{deg(p)}} + \frac{f'(p)l(p)deg(p)\chi(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)}}{f(p)g(p)(1-\chi(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)}}\Big)$$

$$= \sum_{p\in\mathbf{P}^1} deg(p)(\chi(F_p)t^{deg(p)} + \chi(F_p^2)t^{2deg(p)} + \cdots + \chi(F_p^n)t^{n\,deg(p)} + \cdots) -$$

$$\{\sum_{\substack{P\in X_{sing}\\ P|p}} r(p)deg(p)\Big((\chi(F_p)t^{deg(p)} + \chi(F_p^2)t^{2\,deg(p)} + \cdots) -$$

$$\frac{f'(p)l(p)}{f(p)g(p)}(\chi(F_p^{\frac{f(p)}{f'(p)}})t^{deg(p)} + \chi(F_p)^{\frac{2f(p)}{f'(p)}}t^{2deg(p)} + \cdots)\Big)\}$$

The first coefficient of the above series is

$$\sum_{\substack{p\in\mathbf{P}^1\\ deg(p)=1}} \chi(F_p) - \Big(\sum_{\substack{P\in X_{sing}\\ P|p\\ deg(p)=1}} r(p)(\chi(F_p) - \frac{f'(p)l(p)}{f(p)g(p)}\chi(F_p^{\frac{f(p)}{f'(p)}}))\Big).$$

This allow us to associate an exponential sum to X when X satisfies all the above conditions.

Definition 2.8. *Let X be a curve over $\mathbf{F}_q$ such that $\tilde{X}$ is an abelian covering of the projective line, then the* **exponential sum** $S(X, \mathbf{F}_q, \chi)$ *associated to the curve X is defined to be*

$$S(X, \mathbf{F}_q, \chi) = \sum_{\substack{p \in \mathbf{P}^1 \\ deg(p)=1}} \chi(F_p) - \Big(\sum_{\substack{P \in X_{sing} \\ P|p \\ deg(P)=1}} r(p)(\chi(F_p) - \frac{f'(p)l(p)}{f(p)g(p)} \chi(F_p^{\frac{f(p)}{f'(p)}})) \Big).$$

Note that this definition of exponential sums consist of the usual exponential sums and the contribution of the singular points. It is easy to obtain a bound for $S(X, \mathbf{F}_q, \chi)$.

Theorem 2.9. *With the above notation, we have*

$$|S(X, \mathbf{F}_q, \chi)| \leq (deg(\mathcal{F}) - 2)q^{1/2} + 2|\overline{X}_{\mathbf{sing}}|,$$

where $\mathcal{F}$ is the degree of the conductor of χ.

Proof. We have

$$\begin{aligned} |S(X, \mathbf{F}_q, \chi)| &\leq |\sum_{\substack{p \in \mathbf{P}^1 \\ deg(p)=1}} \chi(F_p)| + |(\sum_{\substack{P \in X_{sing} \\ P|p \\ deg(P)=1}} r(p)(\chi(F_p) - \frac{f'(p)l(p)}{f(p)g(p)} \chi(F_p^{\frac{f(p)}{f'(p)}}))| \\ &\leq |\sum_{\substack{p \in \mathbf{P}^1 \\ deg(p)=1}} \chi(F_p)| + 2|\overline{X}_{\mathbf{sing}}| \text{ since } \tfrac{f'(p)l(p)}{f(p)g(p)} \leq 1 \\ &\leq (deg(\mathcal{F}) - 2)q^{1/2} + 2|\overline{X}_{\mathbf{sing}}|. \end{aligned}$$

Examples of Exponential Sums.

1. Let X be a curve defined by the equation $x^2y^2 + y^2 + x^2 - 1 = 0$ over $\mathbf{F}_p$, where $p \equiv 1 \bmod 4$. Then, the L-function of $\tilde{X}$ associated to the non-trivial character χ of X is $1 - 2at + pt^2$. The exponential sum associated to X and χ is equal to:

$$\begin{aligned} S(X, \mathbf{F}_p, \chi) &= \sum_p \chi(F_p) - \sum_{P|p \in X_{sing}} (\chi(F_p) - \frac{1}{2}\chi(F_p)) \\ &= \sum_p \chi(F_p) - 1 \\ &= -2a - 1. \end{aligned}$$

In particular,

- If $p = 5$, then $S(X', \mathbf{F}_p, \chi) = 2 - 1 = 1$.
- If $p = 13$, then $S(X', \mathbf{F}_p, \chi) = -6 - 1 = -7$.
- If $p = 17$, then $S(X', \mathbf{F}_p, \chi) = -2 - 1 = -3$.

2. Let X be a curve defined by the equation $x^2y^2 + x^2 + y^2 - 1 = 0$ over $\mathbf{F}_p$, where $p \equiv 3 \bmod 4$. The exponential sum associated to X and χ is equal to:

$$\begin{aligned} S(X, \mathbf{F}_p, \chi) &= \sum_p \chi(F_p) - \sum_{\substack{P|p \in X_{sing} \\ deg(p)=1}} (\chi(F_p) - \frac{1}{2}\chi(F_p^2)) \\ &= \sum_p \chi(F_p) + 3. \end{aligned}$$

3. Let X be the curve defined by the equation $y^2+x^4+1=0$ over $\mathbf{F}_p$, where $p \equiv 1 \bmod 4$. The exponential sum associated to X and χ is equal to:

$$\begin{aligned} S(X, \mathbf{F}_p, \chi) &= \sum_p \chi(F_p) - \sum_{\substack{P \mid p \in X_{\text{sing}} \\ \deg(p)=1}} (\chi(F_p) - \frac{1}{2}\chi(F_p)) \\ &= \sum_p \chi(F_p) - \frac{1}{2}. \end{aligned}$$

In particular,

- $S(X, \mathbf{F}_5, \chi) = -2 - \frac{1}{2} = \frac{-5}{2}$
- $S(X, \mathbf{F}_{13}, \chi) = 6 - \frac{1}{2} = \frac{11}{2}$
- $S(X, \mathbf{F}_{17}, \chi) = -2 - \frac{1}{2} = \frac{-5}{2}$.

Chapter 3

Exponential Sums in Several Variables

This chapter deals with exponential sums in several variables. We make a detailed study of the Kloosterman sum in seven variables and prove some distribution results for its values.

3.1 Basic Definitions and Results on Constructible Sheaves

In this section we give some definitions that we need through this chapter. Furthermore, we will fix the notation that will be used throughout.

Let X be a connected, normal, and locally noetherian scheme. Let $\mathbf{K}$ be the function field of X, i.e., $\mathbf{K}$ is equal to the local ring $\mathcal{O}_\eta$ of the generic point η of X. Let $\mathbf{K}^{sep}$ be the separable closure of $\mathbf{K}$. Let $G(\mathbf{K}^{sep}/\mathbf{K})$ be the Galois group of the field extension $\mathbf{K}^{sep}/\mathbf{K}$. Let x be a closed point of X, then $\mathbf{K}_x$ denotes the completion of $\mathbf{K}$ at x. Let $\mathbf{k}$ be the residue field of $\mathbf{K}_x$.

We assume that $\mathbf{k}$ is a perfect field with characteristic $p > 0$. Let $\mathbf{K}_x^{sep}$ be the separable closure of $\mathbf{K}_x$ and put $D_x = G(\mathbf{K}_x^{sep}/\mathbf{K}_x)$, where $G(\mathbf{K}_x^{sep}/\mathbf{K}_x)$ is the Galois group of the field extension $\mathbf{K}_x^{sep}/\mathbf{K}_x$. We have the following exact sequences

$$1 \longrightarrow I_x \longrightarrow D_x \longrightarrow G(\mathbf{k}^{sep}/\mathbf{k}) \longrightarrow 1$$

and

$$1 \longrightarrow P_x \longrightarrow I_x \longrightarrow \prod_{l \neq p} \mathbf{Z}_l \longrightarrow 1,$$

where P_x is called the wild ramification group and is a maximal pro-p-group.

Now we define the étale fundamental group $\pi_1(X, \overline{x})$ of X. The following discussion is based on [16, chapter 1.5]. Let $\overline{x} \mapsto X$ be a geometric point of X. There exists a functor F from the categories

$$\mathcal{C} := \{X\text{-schemes finite and étale over} X\} \longrightarrow \{\text{Sets}\},$$

where $F(Y) := Hom_X(\overline{x}, Y)$. Hence to give an element of $F(Y)$ is to give a point $y \in Y$ lying over x and a $\mathbf{k}(x)$-homomorphism $\mathbf{k}(y) \longrightarrow \mathbf{k}(\overline{x}) = \mathbf{k}^{sep}$.

The functor F is strictly prorepresentable, i.e., there exists a directed set J, a projective system $(X_i, \phi_{ij})_{i \in J}$ in $\mathcal{C}$ for which the transition morphisms $\phi_{ij} : X_j \longrightarrow X_i$ for $i \leq j$ are epimorphism and the elements $f_i \in F(X_i)$ satisfy

1. $f_i = \phi_{ij} \circ f_j$

2. the natural map

$$\varinjlim Hom(X_i, Z) \longrightarrow F(Z)$$

induced by the f_i is an isomorphism for $Z \in \mathcal{C}$.

For an X-scheme Y, we denote by $Aut_X(Y)$ the X-automorphism of Y acting on the right. If $Y \in \mathcal{C}$, then for $g \in Y$, $\sigma \mapsto \sigma g : Aut_X(Y) \longrightarrow F(Y)$. The action of $Aut_X(Y)$ is bijective since Y is connected. We say Y is Galois over X. We have that for any $Y \in \mathcal{C}$, there exists a Y' that is Galois over X and a morphism $Y' \longrightarrow Y$. Therefore, we can assume that the X_i are Galois over X. Given $i \leq j$, we can define the map $\rho_{ij} : Aut_X(X_j) \longrightarrow Aut_X(X_i)$ by requiring that $\rho_{ij}(\sigma) = \phi_{ij} \circ \sigma \circ f_j$. We define

$$\pi_1(X, \overline{x}) = \varprojlim Aut_X(X_i).$$

Note that if $\overline{x}'$ is another geometric point of X, then $\pi_1(X, \overline{x}') \simeq \pi_1(X, \overline{x})$. This isomorphism is canonically determined up to an inner automorphism of $\pi_1(X, \overline{x})$.

Example 1.

If $X = Spec(\mathbf{k})$, $\mathbf{k}$ a field. The X_i may be taken to be the spectrum of all Galois extension $\mathbf{k}_i$ of $\mathbf{k}$ contained in $\mathbf{k}(\overline{x})$. Then, $\pi_1(X, \overline{x}) = G(\mathbf{k}^{sep}/\mathbf{k})$. Changing the geometric point $\overline{x}$ corresponds to choosing a different separable algebraic closure. If $\mathbf{k} = \mathbf{F}_q$, then $\pi_1(X, \overline{x}) = G(\mathbf{F}_q^{sep}/\mathbf{F}_q)$. This Galois group is a free profinite group on one canonical generator, namely the map $y \mapsto y^q$

on $\mathbf{F}_q^{sep}$, which is called the **arithmetic Frobenius**. The inverse of this generator is called the **geometric Frobenius.**

Example 2.

If $X = Spec(A)$ where A is strictly Henselian local ring, then $\pi_1(X, \overline{x}) = 1$ since $\mathcal{C}$ consists only of the direct sums of copies of X.

Example 3.

If $X = \mathbf{P}^1(\mathbf{k})$ where $\mathbf{k}$ is separable and closed, then $\pi_1(X, \overline{x}) = 1$ since $\mathbf{P}^1(\mathbf{k})$ does not admit a non-trivial étale covering.

Definition 3.1. *Let X be a connected scheme over a field* $\mathbf{k}$. *Then, the arithmetic fundamental group $\pi_1^{arith}(X)$ of X with base point $\overline{x}$ is $\pi_1(X, \overline{x})$ and the geometric fundamental group $\pi_1^{geom}(X)$ of X with base point $\overline{x}$ is $\pi_1(X \times_{\mathbf{k}} \mathbf{k}^{sep}, \overline{x})$.*

Example 4.

Let U be an open set of $\mathbf{P}^1(\mathbf{K})$, i.e., U is equal to

$$\mathbf{P}^1(\mathbf{K}) - \{\text{finite number of points}\}.$$

Then, $\pi_1^{arith}(U)$ can be viewed as the quotient of $G(\mathbf{K}^{sep}/\mathbf{K})$ by the smallest closed normal subgroup I_U containing all the I_x for $x \in U$. The geometric fundamental group $\pi_1^{geom}(U)$ can be viewed as the quotient of $G(\mathbf{K}^{sep}/\mathbf{K}\mathbf{k}^{sep})$

by I_U.

The functor π_1 is left exact and π_1 classifies the finite etale coverings of X. For X a schemes, and field $\mathbf{k}$, we can interpret a $\mathbf{k}$-valued point $x \in X(\mathbf{k})$ as a map of schemes $f : Spec(\mathbf{k}) \longrightarrow X$. By the covariance of π_1, we get a homomorphism $G(\mathbf{k}^{sep}/\mathbf{k}) \longrightarrow \pi_1^{arith}(X)$(well defined up to conjugation). If $\mathbf{k}$ is a finite field, we can attach to $\mathbf{k}$-valued point $x \in X(\mathbf{k})$ the image of the geometric Frobenius F_p in $\pi_1^{arith}(X)$, which we denote by $F_{p,x}$; it is well defined as a conjugacy class of $\pi_1^{arith}(X)$. $F_{p,x}$ is called the Frobenius conjugacy class associated to the pair $(\mathbf{k}, x)$.

Definition 3.2. *Let $\rho : G(\mathbf{K}^{sep}/\mathbf{K}) \longrightarrow Aut(V)$ be an l-adic representation of $\mathbf{K}$, and let $x \in X$. We say that ρ is unramified at x if $\rho(I_y) = 1$ for any $y \in \mathbf{K}^{sep}$ lying above x.*

If the represenation ρ is unramified at x, then the restriction of ρ to D_y factors through D_y/I_x for any $y|x$, i.e., y lies above x.

Now, we recall the definitions of constructible and lisse sheaves on X.

Definition 3.3. *Let $\overline{x}$ be a geometric point of X, a constructible sheaf $\mathcal{F}$ on X is a continous l-adic representation $\mathcal{F}_{\overline{x}}$ of $G(\mathbf{K}^{sep}/\mathbf{K})$ together with, for each closed point $x \in X$, a continous representation $\mathcal{F}_x$ of D_x/I_x and a D_x-equivariant map*

$$sp_x : \mathcal{F}_x \longrightarrow \mathcal{F}_{\overline{x}}$$

such that

1) I_x acts trivially for all but a finite number of closed points, that means, $\mathcal{F}_{\overline{x}}$ is unramified for all but a finite number of closed points.

2. sp_x is an isomorphism for almost all $x \in X$.

Definition 3.4. *The constructible sheaf $\mathcal{F}$ on X is lisse at $x \in X$ if sp_x is an isomorphism.*

Remark. If X is an algebraic variety over $\mathbf{F}_q$, then the Lefschetz trace formula gives the following:

$$|X_m| = \sum_i (-1)^i Tr(F_p^m \mid H_c^i(X \bigotimes \mathbf{F}_q^{sep}, \mathbf{Q}_l)),$$

where X_m be the set of points of X defined over $\mathbf{F}_{q^m}$, F_p is the geometric Frobenius, and $H_c^i(X \otimes \mathbf{Q}_l)$ is the i-th l-adic cohomology group with compact support ($char(\mathbf{F}_q) \neq l$). On [5], Deligne proves that for each eigenvalue α_i of F_p on $H_c^i(X \otimes \mathbf{Q}_l)$, there is an integer $w = w(\alpha_i)$, called its **weight**, such that

$$0 \leq w \leq i \ \ , |\text{every conjugate } \alpha_i| = q^{w/2}.$$

If, for given i, all the α_i have the same absolute value $w(\alpha_i)$, we say that $H_c^i(X \otimes \mathbf{Q}_l)$ is **pure of weight** w. It is well known that if X is proper and smooth, then $H_c^i(X \otimes \mathbf{Q}_l)$ is pure of weight i.

Let $x \in X$ be a closed point and let $\mathbf{K}_x$ be the completion of $\mathbf{K}$ at x. If

M is a $\mathbf{Z}[\frac{1}{p}]$-module on which P acts through a finite discrete quotient, i.e., there exists a representation $\rho : P \longrightarrow Aut_{\mathbf{Z}}(M)$ and a finite group G such that the diagram

$$\begin{array}{ccc} P & \longrightarrow & Aut_{\mathbf{Z}}(M) \\ & \searrow & \uparrow \\ & & G \end{array}$$

is commutative, then we have

1. M has a unique direct sum decomposition of $M = \bigoplus M(u)$ into P-stable submodules $M(u)$, indexed by real numbers $u \geq 0$, they satisfy the following:

A. $M(0) = M^P$

B. $(M(u))^{I^u} = 0$ for $u > 0$

C. $(M(u))^{I^v} = M(u)$ for $v > u$.

2. If $u > 0$, then $M(u) = 0$ for all but the finitely many values of u for which

$$\rho(I^u) \supset \bigcup_{v>u} \rho(I^v).$$

The construction of the $M(u)$ for $u > 0$ is based on "the projection onto the invariants". For the proof of the construction of $M(u)$ see [12, chapter 1.1]. The decomposition $M = \bigoplus M(u)$ is called the break-decomposition of M and the values of $u \geq 0$ for which $M(u) \neq 0$ are called the breaks of M.

Now we are ready to define the Swan Conductor of M.

Definition 3.5. *The Swan Conductor of M as I-representation is defined by*

$$Sw_\rho(M) := \sum_{u \geq 0} u\, dim(M(u)).$$

By Hasse-Arf, each product $u\, dim(M(u))$ is a nonnegative integer. If $M(u)^P = 0$, and we say that M is totally wild. If $M(u) = M(u)^P$ then P acts trivially on $M(u)$, we say M is tame. Now we define the Kloosterman sums.

Definition 3.6. *Let ψ be an additive character of $\mathbf{F}_q$ and let $\chi_1, \ldots, \chi_n$ be multiplicative characters of $\mathbf{F}_q^*$. Let $b_1, \ldots, b_n$ be positive integers, then the Kloosterman sum is defined by*

$$K_a(\psi, \chi_1, \ldots, \chi_n, b_1, \ldots, b_n)(\mathbf{F}_q) := \sum_{\substack{x_1^{b_1} \cdots x_n^{b_n} = a \\ x_i \in \mathbf{F}_q^*}} \psi(\sum_{i=1}^{n} x_i)\chi(x_1) \cdots \chi_n(x_n).$$

We are interested in the case when $\chi_1 = \cdots = \chi_n = 1$ and $b_1 = \cdots b_n = 1$. We denote this case by $K_a(\psi)$.

Definition 3.7. *Let ψ be an additive character of $\mathbf{F}_q$. Then the Kloosterman sum associated to ψ over $\mathbf{F}_{q^m}$ is defined by*

$$K_{a,m}(\psi) := \sum_{\substack{x_1 \cdots x_n = a \\ x_1, \ldots, x_n \in \mathbf{F}_{q^m}}} \psi(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\sum_{i=1}^{n} x_i)).$$

Now we will state the theorem that guarantees the existence of the Kloosterman sheaves. Let p be the characteristic of $\mathbf{F}_q$. Let $\mathbf{E}$ be a finite extension of $\mathbf{Q}$. Let $\psi : \mathbf{F}_q \longrightarrow \mathbf{E}^*$ be a non-trivial additive character, $n \geq 1$ an integer, $\chi_1,\ldots,\chi_n$ multiplicative characters $\chi_i : \mathbf{F}_q^* \mapsto \mathbf{E}^*$, and $b_1 = b_1' p^{n_1},\ldots,$ $b_n = b_n' p^{n_n}$ be positive integers where $gcd(b_i', p) = 1$ for $= 1,\ldots,n$. Let $l \neq p$ be a prime number and let $\mathbf{Q}_l$ be the completion of $\mathbf{Q}$ at l. Let E_λ be the composite field of $\mathbf{E}$ and $\mathbf{Q}_l$. Let $\mathcal{O}_\lambda$ be ring of integers of $\mathbf{E}_\lambda$. Now we are ready to state the theorem.

Theorem 3.8. *There exists a lisse sheaf of free $\mathcal{O}_\lambda$-modules of finite rank on $\mathbf{F}_q^* \otimes \mathbf{F}_q$, denoted*

$$K(\psi, \chi_1, \ldots, \chi_n, b_1, \ldots, b_n),$$

or simply K, with the following properties:

1. *$K(\psi, \chi_1, \ldots, \chi_n, b_1, \ldots, b_n)$ is lisse of rank $\sum_{i=1}^n b_i'$ and pure of weight $n-1$.*
2. *For any finite extension $\mathbf{F}_{q^m}$ of $\mathbf{F}_q$, and any $a \in \mathbf{F}_{q^m}^*$, we have the identity*

$$Tr(F_{a,\mathbf{F}_{q^m}} | K_{\overline{a}}) = (-1)^{n-1} K_a(\psi, \chi_1, \ldots, \chi_n, b_1, \ldots, b_n)(\mathbf{F}_{q^m})$$

where $\overline{a}$ is a geometric point lying above a and $F_{\overline{a},\mathbf{F}_{q^m}}$ is the inverse of the standard generator $y \mapsto y^{q^m}$ of $G(\mathbf{F}_q^{sep}/\mathbf{F}_q) \simeq \pi_1^{arith}(Spec(\mathbf{F}_q), \overline{a})$.

3. *K is totally wild at ∞, and $Sw_\infty(K) = 1$.*

4. K is tame at 0.

In [12, chapter 4.1], Katz proved the theorem for $n = 1$, via the sheaves $\mathcal{L}_\psi$ and $\mathcal{L}_\chi$. We will define $\mathcal{L}_\psi$ below. Katz develops the convolution of sheaves on $\mathbf{F}_q^* \otimes \mathbf{F}_q$, this allows him to construct the Kloosterman sheaves for $n > 1$.

Corollary 3.9. (Deligne) *For $a \in \mathbf{F}_q^*$, there exists n eigenvalues $\alpha_1, \ldots, \alpha_n$ of the Frobenius element with absolute value $q^{(n-1)/2}$ such that satisfy*

$$K_{a,m}(\psi) = \sum_{\substack{x_1 \cdots x_n = a \\ x_1, \ldots, x_n \in \mathbf{F}_{q^m}}} \psi(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\sum_{i=1}^{n} x_i)) = (-1)^{n-1}(\alpha_1^m + \cdots + \alpha_n^m).$$

Corollary 3.10. *With the above notation, if n is even, then for each eigenvalue α_i there exists an eigenvalue α_j such that*

$$\alpha_i \alpha_j = q^{n-1} \text{ or equivalently } \alpha_i = \overline{\alpha}_j.$$

Corollary 3.11. *With the above notation, we have*

$$|K_{a,m}(\psi)| \leq n q^{m(n-1)/2}.$$

Now we consider the affine line $\mathbf{A}^1 = Spec(\mathbf{F}_q[t])$. Let $\psi : \mathbf{A}^1 \mapsto \overline{\mathbf{Q}}_l$ be an additive character. The map $x \mapsto x^q - x$ on $\mathbf{A}^1$ corresponds a morphism of $\mathbf{A}^1 \longrightarrow \mathbf{A}^1$. This morphism is an Artin-Schreier covering of $\mathbf{A}(\mathbf{F}_q)$ and it is an étale covering. We have an exact sequence

$$0 \longrightarrow \mathbf{F}_q \longrightarrow \mathbf{A}^1 \xrightarrow{\pi} \mathbf{A}^1 \longrightarrow 0$$

where $\pi(x) = x^q - x$. Using the definition of the fundamental group, we have a map $\pi_1^{arith}(\mathbf{A}^1) \longrightarrow \mathbf{F}_q$. Therefore, we get a one dimensional continuous representation of $\pi_1^{arith}(\mathbf{A}^1)$,

$$\pi_1^{arith}(\mathbf{A}^1) \longrightarrow \mathbf{F}_q \longrightarrow \overline{\mathbf{Q}}_l.$$

We identify this representation with a lisse $\overline{\mathbf{Q}}_l$-sheaf of rank 1 denoted by $\mathcal{L}_\psi$ on $\mathbf{A}^1$. If $\mathbf{F}_{q^m}$ is a finite extension of $\mathbf{F}_q$ and $y \in \mathbf{F}_{q^m}$, then

$$Tr(\mathcal{L}_\psi)(\mathbf{F}_{q^m}, y) = \psi(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(y)).$$

If $f : X \longrightarrow \mathbf{A}^1$ is a morphism, we denote by $\mathcal{L}_{\psi(f)}$ the sheaf $f^*(\mathcal{L}_\psi)$ on X. If $y \in X(\mathbf{F}_{q^m})$, then

$$Tr(\mathcal{L}_{\psi(f)})(\mathbf{F}_{q^m}, y) = \psi(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(f(y))).$$

Given a constructible sheaf $\mathcal{F}$, the geometric monodromy group G_{geom} is defined by

$$G_{geom} := \text{the Zariski closure of the image } \rho(\pi_1^{geom}) \text{ in } \mathrm{GL}(n, \overline{\mathbf{Q}}_l),$$

where ρ is the representation associated to $\mathcal{F}$. If $\mathcal{F}$ is pure, then G_{geom} is semisimple algebraic group. If we choose an isomorphism $\overline{\mathbf{Q}}_l \simeq \mathbf{C}$, then we can view G_{geom} as a semisimple group over $\mathbf{C}$. From now on, when we talk about G_{geom}, we mean the complex semisimple Lie group $G_{geom}(\mathbf{C})$.

Now we state some definition that we will use in the next section.

Definition 3.12. *Let $f, g : \mathbf{C} \longrightarrow \mathbf{C}$ be two complex functions, we say*

$$f = o(g) \Longleftrightarrow \lim_{z \to \infty} \frac{f(z)}{g(z)} \to 0.$$

Definition 3.13. *Keeping the notation of definition 3.12. We say*

$$f \sim g \Longleftrightarrow f = g + o(z).$$

In the next section we analyze the Kloosterman sum in seven variables over the binary field. To simplify the notation, we denote this by $K_{a,n}(2,7)$.

3.2 Computation of the L-function associated to $K_{1,n}(2,7)$ and its Distribution of signs

In this section we analyze in detail the Kloosterman sum in seven variable over binary field. This sum is an exceptional cases since its geometric monodromy group is G_2. Now we define the Kloosterman sum in seven variables over the binary field.

Definition 3.14. *The Kloosterman sum $K_{1,n}(2,7)$ in seven varibles over $\mathbf{F}_{2^n}$ is defined by*

$$K_{1,n}(2,7) := \sum_{\substack{x_1 \cdots x_7 = 1 \\ x_i \in \mathbf{F}_{2^n}}} (-1)^{Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\sum_{i=1}^{7} x_i)}.$$

The L-function associated to $K_{1,n}(2,7)$ is defined by

$$L(t) = \exp\{\sum_{n=1}^{\infty} \frac{K_{1,n}(2,7)t^n}{n}\}. \tag{3.1}$$

Using Deligne's theorem we have

$$\begin{aligned} L(t) &= \exp\{\sum_{n=1}^{\infty} \frac{K_{1,n}(2,7)t^n}{n}\} \\ &= \exp\{\sum_{i=1}^{7}\sum_{n=1}^{\infty} \frac{(\alpha_i t)^n}{n}\} \\ &= \exp\{\sum_{i=1}^{7} \log(1-\alpha_i t)\} \\ &= \prod_{i=1}^{7}(1-\alpha_i t)^{-1}. \end{aligned}$$

Recall that the absolute value of the roots of $L(t)$ is 8. If we apply log to (3.1), we get the following

$$\sum_{n=1}^{\infty} \frac{K_{1,n}(2,7)t^n}{n} = -(\sum_{i=1}^{3} \log(1-(\alpha_i+\overline{\alpha_i})t+64t^2) + \log(1-\alpha t)),$$

where $\alpha = \overline{\alpha}$. Let a_i be equal to $\alpha_i + \overline{\alpha_i}$. We only need to compute $K_{1,n}(2,7)$ for $n = 1,\ldots,4$ since the L-function satisfies a functional equation. The values of those sums are given in the following table:

n	$K_{1,n}(2,7)$
1	-1
2	85
3	713
4	-6383

We have two possible values for α, i.e., 8 or -8 by Deligne's theorem. We are going to use $K_{1,4}(2,7)$ to find the correct value of α. Suppose α is equal to

8, then we get the following

$$-t+\frac{85}{2}t^2+\frac{713}{3}t^3-\frac{6383}{4}t^4+\cdots=-(\sum_{i=1}^{3}\log(1-(a_it-64t^2))+\log(1-8t))$$

Therefore, we have the following system of equations:

$$\begin{aligned} -9 &= a_1+a_2+a_3 \\ 405 &= a_1^2+a_2^2+a_3^2 \\ -1527 &= a_1^3+a_2^3+a_3^3. \end{aligned}$$

The solution of the above system of equations is

$$\begin{aligned} a_1 &= \Re(\xi^{1/3})-3 \\ a_2 &= -\Re(\xi^{1/3})-3-\sqrt{3}\,\Im(\xi^{1/3}) \\ a_3 &= -\Re(\xi^{1/3})-3+\sqrt{3}\,\Im(\xi^{1/3}) \end{aligned}$$

where $\xi = 326+\sqrt{143771}\,\imath$. The approximate values of the a_i's are

$$\{-14.50300692, -6.722704887, 12.2257118\}.$$

By a small computation, we found that

$$\begin{aligned} L(t) &= (1+t-42t^2-280t^3+2240t^4+21504t^5-32768t^6-2097152t^7)^{-1} \\ &= ((1+9t+30t^2-40t^3+1920t^4+36864t^5+262144t^6)(1-8t))^{-1}. \end{aligned}$$

If we expand $\log Z(t)$, we obtain $K_{1,4}(2,7) = -6383$. Therefore, α is equal 8. We now collect the above results in the following statement.

Theorem 3.15. *The L-function of the Kloosterman sum* $K_{1,n}(2,7)$ *is given by*

$$L(t) = \frac{1}{1 + t - 42t^2 - 280t^3 + 2240t^4 + 21504t^5 - 32768t^6 - 2097152t^7}.$$

Let

$$f(t) = 1 + 9t + 30t^2 - 40t^3 + 1920t^4 + 36864t^5 + 262144t^6. \tag{3.2}$$

Using the computer program Maple, we proved that $f(t)$ is irreducible over $\mathbf{Q}$ and its discriminant is $-(2)^{26}(3)^7(7)^2(109)^3(1319)^2$. The approximate values of the roots of $f(t)$ are

1. $.0955133736 \pm .08063619213\imath$
2. $-.05252113191 \pm .1134307309\imath$
3. $-.1133047416 \pm .05279238148\imath$.

Now we are ready to give a description of the reciprocal roots of $f(t)$. Let $\alpha_i = 8\,e^{2\pi\theta_i\imath}$ and $\overline{\alpha_i} = 8\,e^{-2\pi\theta_i\imath}$ be the reciprocal of the roots of $f(t)$. We want to prove that $e^{\pm 2\pi\theta_1\imath}$, $e^{\pm 2\pi\theta_2\imath}$, $e^{\pm 2\pi\theta_3\imath}$ are not roots of unity. We substitute $t = \frac{x}{8}$ in $f(t)$ and we get

$$f(\frac{x}{8}) = \frac{1}{64}(64 + 72x + 30x^2 - 5x^3 + 30x^4 + 72x^5 + 64x^6).$$

The roots of $f(\frac{x}{8})$ are $e^{\pm 2\pi\theta_i\imath}$ for $i = 1, 2, 3$. Let $g(x) = 64f(\frac{x}{8})$. $g(x)$ is irreducible over $\mathbf{Q}$.

Claim. $e^{\pm 2\pi\theta_i \imath}$ for $i = 1, 2, 3$ is not a root of unity.

Proof. Suppose that $e^{2\pi\theta_i \imath}$ is a root of the unity, then $e^{2\pi\theta_i \imath}$ is a root of a cyclotomic polynomial Φ. Since g and Φ are irreducible over $\mathbf{Q}$, then $-g = \Phi$ or $g = \Phi$. This is a contradiction. This proves the claim. Later, we will prove more precise result: If $\mathbf{K}$ is the splitting field of the polynomial $f(t)$, then $\mathbf{K}$ does not contain a cyclotomic subfield.

Theorem 3.16. *There exists a choice* $\epsilon_1, \epsilon_2, \epsilon_3 \in \{ \pm\theta_1, \pm\theta_2, \pm\theta_3 \}$ *such that*

$$\epsilon_1 + \epsilon_2 + \epsilon_3 \equiv 0 \bmod 1,$$

i.e., $\epsilon_1 + \epsilon_2 + \epsilon_3 \in \mathbf{Z}$ *and* $|\epsilon_i| \neq |\epsilon_j|$ *for* $i \neq j$.

Proof. Note that $f(t)$ factors over $\mathbf{Q}(\sqrt{327}\imath)$,

$$\begin{aligned} f(t) &= \frac{1}{4}(1024t^3 + 72t^2 - 8\sqrt{327}\imath t^2 - 9t - \sqrt{327}\imath t - 2) \times \\ &\quad (1024t^3 + 72t^2 + 8\sqrt{327}\imath t^2 - 9t + \sqrt{327}\imath t - 2). \end{aligned}$$

We know that $f(t) = \prod_{i=1}^{3}(1 - 8e^{2\pi\theta_i \imath} t) \prod_{i=1}^{3}(1 - 8e^{-2\pi\theta_i \imath} t)$, therefore there exists $\epsilon_1, \epsilon_2, \epsilon_3 \in \{ \pm\theta_1, \pm\theta_2, \pm\theta_3 \}$ such that $8^3 e^{\epsilon_1 + \epsilon_2 + \epsilon_3} = 512$. This implies $\epsilon_1 + \epsilon_2 + \epsilon_3 \equiv 0 \bmod 1$. It is clear that $|\epsilon_i| \neq |\epsilon_j|$ since $f(t)$ is irreducible over $\mathbf{Q}$. Using the aproximate values of the roots of $f(t)$, it can be seen that $\epsilon_1 + \epsilon_2 + \epsilon_3 = 1$. This completes the proof.

Let $\mathbf{K}$ be the splitting field of $f(t)$, then the Galois group of the field extension $\mathbf{K}/\mathbf{Q}$ is $D_6 =< \eta, \sigma \mid \eta^6 = \sigma^2 = 1, \eta^5\sigma = \sigma\eta >$. In particular, we

have $deg(\mathbf{K}/\mathbf{Q}) = 12$.

Theorem 3.17. $\mathbf{K}$ *does not contain cyclotomic subfields.*

Proof. Let $\mathbf{E}$ be a cyclotomic subfield of $\mathbf{K}$, then $deg(\mathbf{E}/\mathbf{Q})$ divides 12. Then $deg(\mathbf{E}/\mathbf{Q})$ is less than 12 since the roots of $f(\frac{t}{8})$ are not roots of unity. Therefore, $deg(\mathbf{K}/\mathbf{Q})$ can be equal to 2, 3, 4 and 6. By the theory of cyclotomic fields we know that $\mathbf{Q}(\zeta_l) = \mathbf{E}$ where $\zeta_l = e^{2\pi\iota/l}$ and $deg(\mathbf{Q}(\zeta_l)/\mathbf{Q}) = \phi(l)$ where $\phi(l)$ is the Euler function, i.e., $\phi(l)$ is defined to be the number of integers between 1 to l relatively prime l. In the following table we compute all the possible values of l such that $\phi(l)$ divides 12.

$\phi(l)$	l
2	3,4,6
3	
4	5,8,10,12
6	7,9,14,18

Using the computer program Maple, we found that $f(t)$ is irreducible over $\mathbf{Q}(\zeta_l)$ for all the l that are present in the previous table. Therefore, $\mathbf{K}$ does not contain $\mathbf{Q}(\zeta_l)$ as intermediate field for $\phi(l) > 2$ since we adjoint any root of $f(t)$ to $\mathbf{Q}(\zeta_l)$, we get an extension of degree bigger than 12. Now we are going to consider the case when $\phi(l) = 2$. For $\phi(l) = 2$, the possible cyclotomic subfields of $\mathbf{K}$ are $\mathbf{Q}(\zeta_3)$, $\mathbf{Q}(\zeta_4)$ and $\mathbf{Q}(\zeta_6)$.

Claim. $\mathbf{Q}(\zeta_4)$ is not contained in $\mathbf{K}$.

Proof. Suppose that $\mathbf{Q}(\zeta_4) = \mathbf{Q}(\imath)$ is a subfield of $\mathbf{K}$, then $\sqrt{327}\imath \cdot \imath \in \mathbf{K}$. Therefore, $\sqrt{327} \in \mathbf{K}$. $f(t)$ is irreducible over $\mathbf{Q}(\imath)$ and $\mathbf{Q}(\sqrt{327})$, then when we adjoint any root of $f(t)$ to $\mathbf{Q}(\imath)$ or $\mathbf{Q}(\sqrt{327})$, we get all $\mathbf{K}$. This is a contradiction. Hence we get the claim.

$$\begin{array}{c} \mathbf{Q}(e^{2\pi\theta_i\imath}, \imath) = \mathbf{Q}(e^{2\pi\theta_i\imath}, \sqrt{327}) \\ | \\ \mathbf{Q}(e^{2\pi\theta_i\imath}) \\ | \\ \mathbf{Q} \end{array}$$

The same argument applies for the other two cases. This completes the proof of the theorem 3.17.

Now we are ready to prove the main theorem of this section, but first we need some notation. Let

$$z = \mathcal{A}e^{2\pi\theta_1\imath} + \mathcal{B}e^{2\pi\theta_2\imath} + \mathcal{C}e^{2\pi\theta_3\imath}$$

where

1. $\theta_i - \theta_j$ is irrational for $i \neq j$.

2. $\theta_1 + \theta_2 + \theta_3 \equiv 0 \bmod 1$

3. $\mathcal{A} + \mathcal{B} > \mathcal{C}$.

We write

$$z = e^{2\pi\theta_3\imath}(\mathcal{A}e^{2\pi(\theta_1-\theta_3)\imath} + \mathcal{B}e^{2\pi(\theta_2-\theta_3)\imath} + \mathcal{C}).$$

Let

$$\mathcal{A}e^{2\pi(\theta_1-\theta_3)i} + \mathcal{B}e^{2\pi(\theta_2-\theta_3)i} + \mathcal{C} = r(\theta_1,\theta_2)e^{2\pi\sigma(n)i},$$

where $r(\theta_1,\theta_2)$ is a positive real number. Now we consider the triangle with length of the sides equal to $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$. Then, the triangle has angles $\pi\beta$, $\pi\gamma$, $\pi\tau$.

Theorem 3.18. *If we assume the above condition on the θ_1, θ_2, θ_3 and on the $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ then, we have*

$$\lim_{n\to\infty} \frac{\sigma(n)}{n} = a\beta + b\gamma,$$

where $a = \theta_1 - \theta_3$ and $b = \theta_2 - \theta_3$.

The proof can be found in [27, page 504–506] and [15].

We can conclude the following:

$$\begin{aligned} \sigma(n) &= (a\beta + b\gamma)n + o(n) \\ &\sim n(a\beta + b\gamma). \end{aligned}$$

If we apply the last result to $\mathcal{A}e^{2\pi(\theta_1-\theta_3)i} + \mathcal{B}e^{2\pi(\theta_2-\theta_3)i} + \mathcal{C}$, we get

$$\begin{aligned} \mathcal{A}e^{2\pi(\theta_1-\theta_3)i} + \mathcal{B}e^{2\pi(\theta_2-\theta_3)i} + \mathcal{C} &= r(\theta_1,\theta_2)e^{2\pi\sigma(n)i} \\ &= r(\theta_1,\theta_2)e^{2\pi((a\beta+b\gamma)n+o(n))i} \\ &\sim r(\theta_1,\theta_2)e^{2\pi n(a\beta+b\gamma)i} \end{aligned}$$

We want to apply the theorem 3.18 to our situation. Note that by theorem 3.16, we have $\theta_1+\theta_2+\theta_3 \equiv 0 \bmod 1$, we need to prove that $\theta_i-\theta_j$ is irrational for $i \neq j$.

Corollary 3.19. *$\theta_i - \theta_j$ is irrational for $i \neq j$.*

Proof. Suppose that $\theta_i-\theta_j = \frac{c}{d}$ is rational for $i \neq j$. Then $e^{2\pi(\theta_i-\theta_j)\imath} \in \mathbf{K}$ is a root of unity and this is a contradiction to the theorem 3.17. This completes the proof of the corollary 3.19.

We know that

$$K_{1,n}(2,7) = 8^n(e^{2\pi\theta_1 n\imath} + e^{2\pi\theta_2 n\imath} + e^{2\pi\theta_3 n\imath} + e^{-2\pi\theta_1 n\imath} + e^{-2\pi\theta_2 n\imath} + e^{-2\pi\theta_3 n\imath} + 1).$$

Let $K'_{1,n}(2,7) = \frac{K_n(2,7)-8^n}{8^n}$. We can write

$$\begin{aligned} K'_{1,n}(2,7) &= e^{2\pi\theta_1 n\imath} + e^{2\pi\theta_2 n\imath} + e^{2\pi\theta_3 n\imath} + e^{-2\pi\theta_1 n\imath} + e^{-2\pi\theta_2 n\imath} + e^{-2\pi\theta_3 n\imath} \\ &= e^{2\pi\theta_3 n\imath}(e^{2\pi(\theta_1-\theta_3)n\imath} + e^{2\pi(\theta_2-\theta_3)\imath} + 1) + e^{-2\pi\theta_3 n\imath}(e^{-2\pi(\theta_3-\theta_1)n\imath} + e^{-2\pi(\theta_3-\theta_2)n\imath} + 1) \\ &= r(\theta_1,\theta_2)e^{2\pi\theta_3 n\imath}e^{2\pi\sigma(n)\imath} + r(\theta_1,\theta_2)e^{-2\pi\theta_3 n\imath}e^{-2\pi\sigma(n)\imath}. \end{aligned}$$

Now we apply the theorem 3.18 to our case. Here we have $\mathcal{A} = \mathcal{B} = \mathcal{C} = 1$; therefore $\mathcal{A}+\mathcal{B} > \mathcal{C}$. In this case the triangle has angles equal to $\frac{\pi}{3}$. By theorem 3.18, we have $\pi\beta = \frac{\pi}{3}$ and $\pi\gamma = \frac{\pi}{3}$, therefore $\beta = \gamma = \frac{1}{3}$. Now we substitute the value of β and γ in the theorem 3.18 and we get

$$\sigma(n) \sim (a\beta + b\gamma)n$$

$$\sim \frac{(\theta_1-\theta_3)n}{3}+\frac{(\theta_2-\theta_3)n}{3}$$
$$\sim \frac{(\theta_1+\theta_2-2\theta_3)n}{3}$$

Therefore, we obtain

$$\begin{aligned} K'_{1,n}(2,7) &\sim r(\theta_1,\theta_2)(e^{2\pi\theta_3 nt}e^{\frac{2\pi n}{3}(\theta_1+\theta_2-2\theta_3)t}+e^{-2\pi\theta_3 nt}e^{\frac{-2\pi n}{3}(\theta_1+\theta_2-2\theta_3)t} \\ &\sim r(\theta_1,\theta_2)(e^{\frac{2\pi n}{3}(\theta_1+\theta_2+\theta_3)t}+e^{\frac{-2\pi n}{3}(\theta_1+\theta_2+\theta_3)t}) \\ &\sim r(\theta_1,\theta_2)(e^{\frac{2\pi nt}{3}}+e^{\frac{-2\pi nt}{3}}) \\ &\sim 2r(\theta_1,\theta_2)\cos(2n\pi/3) \end{aligned}$$

Note that

$$\cos(2n\pi/3)=\begin{cases} >0 & \text{if } n\equiv 0 \bmod 3 \\ <0 & \text{otherwise} \end{cases}$$

Therefore, we can conclude

$$|\{\, n\in[1,N]\,|\,sgn(K'_{1,n}(2,7))>0\,\}\sim\frac{N}{3}$$

and

$$|\{\, n\in[1,N]\,|\,sgn(K'_{1,n}(2,7))<0\,\}\sim\frac{2N}{3}.$$

We have proved the following theorem.

Theorem 3.20. *The distribution of the signs of* $K'_{1,n}(2,7)$ *is* $\frac{1}{3}$ *positive and* $\frac{2}{3}$ *negative.*

The theorem 3.20 proves that the distribution of positive value of $K_{1,n}(2,7)$ is greater than or equal to $\frac{1}{3}$.

Remark. Katz on [12, chapter 11, theorem 11.2], has shown that the monodromy group associated to $K_{1,n}(2,7)$ is G_2. The method we have developed here gives an alternative proof to the containment $G_2 \subset G_{geom}$ since $\theta_1, \theta_2, 1$ are linearly independent over $\mathbf{Q}$, i.e., $(e^{2\pi\theta_1 t}, e^{2\pi\theta_2 t})$ is dense in a maximal torus of G_2 (see [15, chapter 4, example 4.1]). Apparently, we need a more delicate argument to prove that $G_2 = G_{geom}$.

Bibliography

[1] Bombieri, E., On exponential sums in finite fields *Am. J. of Math.*, **88**(1966), 71-105.

[2] Borel, A., *Linear Algebraic Groups*, Springer-Verlag, New York, 1969.

[3] Curtis M. L., *Matrix Group*, Springer-Verlag, New York, 1984.

[4] Deligne, P., Applications de la formule des traces aux sommes trigonometriques, SGA 4.5, *Lectures Notes In Math.*, **569**,(1977), 168-232.

[5] Deligne, P., La conjecture de Weil II, *Publ. Math. I.H.E.S.* **52**(1981), 313-428.

[6] Fulton, W. and Harris, J., *Representation Theory*, Springer-Verlag, New York, 1991.

[7] Green B., On the Riemann-Roch theorem for orders in the ring of valuation vectors of a function field, *Manuscripta Math.*, **64**(1988), 259–276.

[8] Harstshorne, R., *Algebraic Geometry*, Springer, New York, 1977.

[9] Humphreys, J. E., *Conjugacy Classes in Semisimple Algebraic Groups*, Mathematical Survey and Monographs, Rhode Island, **43**, 1995.

[10] Ireland, K. and Rosen R., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1980.

[11] Moreno, C. J., *Algebraic Curves over Finite Fields,* Cambridge Tracts in Mathematics, **97**, Cambridge Univ, Press, Cambridge, 1991.

[12] Katz, N., Gauss sums, and Monodromy groups, *Ann. of Math. Studies*, Princeton, **116**, 1988.

[13] Katz, N., Exponential sums and differential equations, *Ann. of Math. Studies*, Princeton, **124**, 1990.

[14] Katz, N., *Exponential sums over finite fields and differential equations over the complex numbers: some interactions,* Bull. Amer. Mathematical Society, **23**(1990), 269-309.

[15] Kuipers, L. and Niederreiter, H. *Uniform Distribution of Sequences*, A Wiley-Interscience Series of Texts, Monographs and Tracts, New York, 1974.

[16] Milne, S., *Étale Cohomology*, Princeton University Press, Princeton, 1980.

[17] Perel'muter, G. I., Estimation of a sum along an algebraic curve, *Mat. Zametki*, **5**(1969), 373-380.

[18] Roquette P., Über den Riemann-Rochschen Satz in Funktionenkörpern vom Transzendenzgrad 1, *Math. Nachr.*, **19**(1958), 375-404.

[19] Rosenlicht M., Equivalence relations on algebraic curves, *Ann. of Math.* , **56**(1952), 169-191.

[20] Serre, J. P., *Local Fields*, Herman, Paris, 1968.

[21] Serre, J. P., *Groupes Algébriques et Corps de Classes*, Herman, Paris, 1959.

[22] Stichtenoth, H., *Algebraic Fields and Codes*, Universitext Springer-Verlag, New York, 1991.

[23] Stöhr K.-O, On the Poles of Regular Differentials of Singular Curves, *Boletim da Sociedade Brasileira de Matemática*,, **24**(1993), 105-236.

[24] Stöhr,K.-O., and Voloch,J.F., A formula for the Cartier Operator on Plane Algebraic Curves, *J. reine angew. Math.*, **377**(1987), 49-64.

[25] Sutor, R. S., The Calculation of Some Geometric Monodromy Groups, *IBM Research Division*, 1992(Preprint).

[26] Weil, A., On some exponential sums, *Proc. Nat. Acad. Sci. USA*, **34**(1948), 204-207.

[27] Weyl, H., Sur une application de la théorie des nombres á la mécanique statistique et la théorie des perturbations, *L'Enseignement mathématique*, **16**(1914), 455-467.