Global fields and their L-functions

Solomatin, P.

Global Fields and Their L-functions

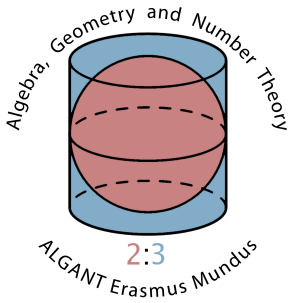
Proefschrift
ter verkrijging van
de graad van doctor aan de Universiteit Leiden
op gezag van rector magnificus prof.dr.ir. H.Bijl,
volgens besluit van het college voor promoties
te verdedigen op 2 maart 2021
klokke 16:15 uur

door

Pavel Solomatin
geboren te Moskou, Russische Federatie, in 1991

Promotor: Prof. dr. Bart de Smit
Promotor: Prof. dr. Karim Belabas (Université de Bordeaux)

Samenstelling van de promotiecommissie:
Dr. Elisa Lorenzo García (Université de Rennes 1)
Prof.dr. Frank van der Duijn Schouten
Prof.dr. Marc Hindry (Université Paris VII)
Prof.dr. Michael A. Tsfasman (Laboratoire de Mathématiques de Versailles)
Prof.dr. Ronald van Luijk



université de BORDEAUX

This work was funded by Erasmus Mundus ALGANT-DOC and it was carried out at Leiden University and University of Bordeaux

THÈSE EN COTUTELLE PRÉSENTÉE
POUR OBTENIR LE GRADE DE
DOCTEUR
DE L'UNIVERSITÉ DE BORDEAUX
ET DE L'UNIVERSITÉ DE LEYDE

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE
INSTITUT DES MATHÉMATIQUES DE L'UNIVERSITÉ DE LEYDE

SPÉCIALITÉ Mathématiques Pures

Par Pavel Solomatin

Corps globaux et leurs fonctions L

Sous la direction de Bart de Smit et Karim Belabas
Soutenue le 2 mars 2021

Membres du jury:

Marc Hindry	Professeur, Université de Paris	Examinateur
Michael A. Tsfasman	Directeur de recherche, Université de Versailles Saint-Quentin-en-Yvelines	Examinateur
Bart de Smit	Professeur, Universiteit Leiden	Directeur
Karim Belabas	Professeur, Université de Bordeaux	Directeur

Summary of the Thesis

In the first chapter of the present thesis we provide a brief step by step introduction to the topic as well as a survey of the main results of the thesis. During the process we focus primarily on the discussion about *arithmetically equivalent number fields*, also known as *isospectral number fields*. This discussion leads to numerous related notions which are central in this dissertation. Among them the following concepts will play a crucial role: *Artin L-functions, absolute Galois groups, class field theory, representation theory of finite and pro-finite groups*. The principal result behind the theory is the famous Theorem 1.23 which goes back to Gassmann. Together with its corollaries this result provides a powerful framework which illustrates nicely how beautiful the interaction between the notions mentioned above can be. We also recall connections of the topic with the so-called *Grothendieck's Anabelian Geometry*. Among other subjects this theory studies properties of the absolute Galois group $\mathcal{G}_K = \mathrm{Gal}(\overline{K} : K)$ of a number field K as well as the structure of the maximal abelian quotient $\mathcal{G}_K^{ab} = \mathrm{Gal}(K^{ab} : K)$ of $\mathcal{G}_K$. We state our main results in section 1.7. Note that while this part of the dissertation served as an introduction and contains no original results, other chapters represent the original work of the author and have corresponding references to preprint versions available on the Arxiv website: arxiv.org.

In chapter two we extend methods of the framework mentioned above and provide some interesting applications of the theory. In particular, we formulate a bit less-known, but still remarkable Theorem 2.4 due to Professor Bart de Smit. Roughly speaking, this Theorem states that the isomorphism class of a number field K is uniquely determined by the collection of Artin L-functions of abelian characters of the absolute Galois group $\mathcal{G}_K$ of K; see section 2.3. In the section 2.4 of this chapter we also generalise Theorem 2.4 in a way which allows us to produce an alternative approach towards a proof of the famous Neukirch-Uchida theorem for the case of non-normal extensions of number fields. This part of the dissertation occurred in [49].

Then in chapters three and four we provide two different approaches in a direction of a function field analogue of Theorem 2.4. The difference between the two treatments is the following: chapter three regards function fields from an *algebraic point of view*, i.e., function fields as finite extensions of the field $\mathbb{F}_q(X)$. In contrast, in chapter four we consider a more geometric setting such as field of functions on a smooth projective curve defined over a finite field $\mathbb{F}_q$. Despite the fact that the two notions are extremely related, the results we proved seem to be opposite. Chapter three has a large intersection with the pre-print [48], while chapter four is based on [47].

Finally, in chapters five and six we shift our focus towards the description of the isomorphism class of the abelianized absolute Galois group $\mathcal{G}_K^{ab}$ associated to a global function field and an imaginary quadratic number field respectively. In the case of global function fields we obtained a complete description and classified all possible isomorphism classes of $\mathcal{G}_K^{ab}$ in terms of more

elementary invariants attached to K. For the imaginary quadratic field case we improved results of [1]. In particular we proved that there are infinitely many isomorphism types of pro-finite abelian groups which occur as $\mathcal{G}_K^{ab}$ for some imaginary quadratic field K. These parts of the thesis correspond to preprints [11] and [12].

For the sake of coherence, along the way towards our main results we occasionally will discuss some additional questions, lemmas and remarks. At the first sight those might seem to be a little aside from the topic, but actually together with the core content they form essential basis needed for understanding the whole picture. We will also provide many concrete examples as well as scripts written in the language of the computational algebra system called Magma. These scripts can be used by anybody who is curious about constructing more sophisticated instances and checking statements of some of the theorems.

Dedication

Dedicated to the memory of my Friend, Advisor and Teacher,
Professor Alexey Ivanovich Zykin(13 June 1984 — 22 April 2017).

Contents

Part I

Number Fields and Their L-functions

Chapter 1

Introduction

1.1 Motivation

Let $f(x)$ be a monic irreducible polynomial in one variable with integer coefficients. An interesting question to ask is the following: which prime numbers divide values of $f(x)$ when x runs over all integer numbers? In other words, for which prime numbers p does a solution of the equation $f(x) = 0 \mod p$ exist? Let us call the set of such primes $\mathcal{A}_{f(x)}$. Note that the case where $f(x)$ is of degree one is not interesting since then $f(x)$ is a bijection $\mathbb{Z} \to \mathbb{Z}$ and therefore each prime number occurs as a divisor of some element of the set $\{f(x)|x \in \mathbb{Z}\}$.

The answer for polynomials of degree two is given by the Legendre symbol and the famous *quadratic reciprocity law*. Let $\mathcal{P}$ denote the set of all prime numbers. Consider for example the case where $f(x) = x^2 + 1$. Then it is well-known since Fermat's time that for every odd prime number p the above equation has a solution modulo p if and only if $(-1)^{\frac{p-1}{2}} = 1$, i.e., if and only if $p = 1 \mod 4$. Obviously the equation $f(x) = 0 \mod 2$ also has a solution and hence we obtain a complete description:

$$\mathcal{A}_{x^2+1} = \{2\} \cup \{p \in \mathcal{P}|p = 1 \mod 4\}.$$

A remarkable fact is the *Dirichlet's Theorem on primes in arithmetic progressions* which implies that in this case exactly half of the primes occur in the set $\mathcal{A}_{x^2+1}$ in the sense that:

$$\lim_{x\to\infty} \frac{\#\{p \in \mathcal{A}_{x^2+1}|p \leq x\}}{\#\{p \in \mathcal{P} \leq x\}} = \frac{1}{2}.$$

In this case we say that $\mathcal{A}_{x^2+1}$ has a *natural density* $\frac{1}{2}$. In general, let $\mathcal{S}$ be any subset of $\mathcal{P}$. Suppose the following limit exists:

$$\delta(\mathcal{S}) = \lim_{x\to\infty} \frac{\#\{p \in \mathcal{S}|p \leq x\}}{\#\{p \in \mathcal{P}|p \leq x\}},$$

then we call the number $\delta(\mathcal{S})$ a *natural density* of $\mathcal{S}$. Sometimes, it is easier to work with a weaker definition of density. In the above setting suppose the following limit exists:

$$\omega(\mathcal{S}) = \lim_{s\to 1+} \frac{\sum_{p\in\mathcal{S}} \frac{1}{p^s}}{\sum_{p\in\mathcal{P}} \frac{1}{p^s}},$$

then we call the number $\omega(\mathcal{S})$ the Dirichlet density of $\mathcal{S}$. Note that the series $\sum_{p\in\mathcal{P}} \frac{1}{p^s}$ absolutely converges for the real $s > 1$ and the limit in the definition of $\omega(\mathcal{S})$ is taken as $s \to 1$ from the right. At first sight it might seem that the Dirichlet density is more artificial and complicated notion to work with. But for many different interesting sets $\mathcal{S}$ we can obtain some information about $\omega(\mathcal{S})$ via the theory of the so-called L-functions. The fundamental relation between the two notions is given by the following:

Theorem 1.1. *Suppose that the natural density $\delta(\mathcal{S})$ of the set $\mathcal{S}$ exists. Then also the Dirichlet density $\omega(\mathcal{S})$ exists and two densities coincide: $\delta(\mathcal{S}) = \omega(\mathcal{S})$. The converse statement is false: there exists an example of a set $\mathcal{S}$ such that the Dirichlet density of $\mathcal{S}$ exists and the natural density does not.*

Proof. See [36], paragraph 13 of chapter VII. □

In the case where $\delta(\mathcal{S})$ exists we simply say that it is *the density* of $\mathcal{S}$.

The case of a general polynomial of $\deg(f) = 2$ is quite parallel: the answer is also given in terms of some linear congruences modulo the number $M_{f(x)} = 4 \cdot \mathrm{Disc}(f)$, where $\mathrm{Disc}(f)$ stands for the discriminant of the polynomial $f(x)$. Moreover we also have that exactly half of the primes occur in $\mathcal{A}_{f(x)}$ in the sense of the above density : $\delta(\mathcal{A}_{f(x)}) = \frac{1}{2}$.

Surprisingly the question about the description of the set $\mathcal{A}_{f(x)}$ in the case where the degree $\deg(f)$ is three or higher is extremely complicated in general and relates to a huge variety of topics in modern mathematics. For some class of polynomials which we call *abelian*, the set $\mathcal{A}_{f(x)}$ still can be characterised in terms of linear congruences modulo an integer $M_{f(x)}$ which depends on $f(x)$ and usually called *the conductor of* $f(x)$. Investigations of properties of the set $\mathcal{A}_{f(x)}$ for this case of abelian polynomials form the main topic of the *class field theory* – one of the central branches of number theory developed in 20th-century. This is already quite a complex and sophisticated subject which took decades of thorough work to develop necessary techniques for establishing its main results. For the present thesis class field theory itself and these techniques will play a crucial role. Note that for a general polynomial there is no such $M_{f(x)}$ and an answer is way more mysterious. Below we consider a few well-know instances of this phenomenon.

If the degree $\deg(f)$ is three then the polynomial $f(x)$ is abelian if and only if the absolute value of the discriminant of f is a square. For instance the polynomial $f(x) = x^3 - 3x + 1$ has discriminant 81 and therefore is abelian. In this abelian case the famous *Kronecker–Weber Theorem* which is itself a partial case of the *Artin reciprocity law* provides us with the following description of $\mathcal{A}_{x^3-3x+1}$. Let $H \subset (\mathbb{Z}/81\mathbb{Z})^\times$ be the subgroup generated by $\langle 8 \rangle$. Then $p \in \mathcal{A}_{x^3-3x+1}$ if and only if either $p = 3$ or $(p \mod 81) \in H$ and as before the Dirichlet's Theorem ensures us that:

$$\delta(A_{x^3-3x+1}) = \frac{1}{3}.$$

In contrast, consider $f(x) = x^3 - x - 1$ of discriminant -23. This is an example of a non-abelian polynomial, but one can still describe the set $\mathcal{A}_{x^3-x-1}$ using the so-called *theory of modular forms*. Let $N_p(f(x))$ denote the number of distinct roots of the equation $f(x) = 0 \mod p$. In particular $p \in \mathcal{A}_{f(x)}$ if and only if $N_p(f(x))$ is positive. Let us consider the following

formal power series:

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \sum_{n=1}^{\infty} a_n q^n = q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} + \dots$$

and compare coefficients a_n for $n = p$ a prime number with $N_p(x^3 - x - 1)$:

Table 1.1: $N_p(f)$ and coefficients a_p

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$N_p(f)$	0	0	1	1	1	0	1	1	2	0	0	1	0	1
a_p	-1	-1	0	0	0	-1	0	0	1	-1	-1	0	-1	0

The non-trivial fact which one could easily check for the first few primes given in the table above is:

$$a_p + 1 = N_p(f). \tag{1.1}$$

In particular this means that $p \in \mathcal{A}_{x^3-x-1}$ if and only if $a_p \geq 0$. This identity is an example of *non-abelian reciprocity* which leads to the so-called *Langlands program*, one of the central research parts of modern number theory. Note also that the far reaching generalisation of the Dirichlet's Theorem mentioned above, the *Chebotarev density Theorem*, implies:

$$\delta(A_{x^3-x-1}) = \frac{5}{6}.$$

It is also remarkable that formula 1.1 helps us to establish some properties of a_p. For instance looking at the definition of a_p, $p \in \mathcal{P}$ it is by no means obvious that $a_p \in \{-1, 0, 1, 2\}$ and the equality $a_p = 1$ implies $p = 23$.

In order to convince the reader that the above identity is not an accident, but rather a part of extremely impressive pattern we state one more example with $f(x) = x^3 - 2$. This polynomial has discriminant equal to -108 and hence is not abelian. In this case we also have a relation which is quite similar to 1.1. Namely $b_p + 1 = N_p(x^3 - 2)$, where the coefficients b_n are given by the following expression:

$$q\prod_{n=1}^{\infty}(1-q^{6n})(1-q^{18n}) = \sum_{n=1}^{\infty} b_n q^n = q - q^7 - q^{13} - q^{19} + q^{25} + 2q^{31} + \dots$$

Except for cases which in some sense resemble those discussed above there are not so many instances where the set $\mathcal{A}_{f(x)}$ could be given more or less explicitly, but it does not mean that we cannot prove anything about them. In contrast, the problem gives rise to a lot of astonishing discoveries and there is a lot of interesting theory behind it. For instance, mentioned above: algebraic and analytic number theory, class field theory, modular forms etc. All these topics have something to do with the title of the present thesis: *"Global fields and their L-functions"*. Our goal in the next section is to introduce relations between the above question and the title more accurately. A reader interested in more *explicit examples of reciprocity laws* can consult a well written expository article [60], as well as [46] or [53]. Identity 1.1 and the next one are well-known and were taken from these materials.

Slightly generalising the main question stated above one could also ask: given a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$, how does this polynomial factor into irreducible polynomials considered modulo a prime number p for different prime numbers? More concretely, for each such $f(x)$ and a prime number p, let $f(x) = g_1^{a_1}(x) \dots g_m^{a_m}(x) \mod p$ where $g_i \in \mathbb{F}_p[x]$, $1 \leq i \leq m$ are distinct monic irreducible polynomials of degree $\deg(g_i) = f_i$ ordered by ascending: $f_1 \leq f_2 \leq \cdots \leq f_m$. Note that $a_i \geq 2$ for some $1 \leq i \leq m$ if and only if $f(x) \mod p$ has a double root in the algebraic closure $\overline{\mathbb{F}_p}$ which happens if and only if p divides the discriminant of $f(x)$. In particular, there are only finitely many prime numbers such that $a_i \geq 2$ for some i. In this terminology our problem can be stated as follows: for a given f and p determine the set of pairs $\{(f_1, a_1), (f_2, a_2), \dots, (f_n, a_n)\}$. How does this set behave where f is fixed and p runs over the set of prime numbers $\mathcal{P}$? It turned out that it is convenient to rephrase this question in the language of algebraic number theory.

1.1.1 Side remark: Checking examples by using Magma

According to one popular opinion, there is only one way to do and understand mathematics: experimenting with objects and their properties as much as possible. This approach helps mathematicians not only to discover new material, but also to grasp the existing one and sometimes even to detect mistakes in it. In order to do these experiments one often needs to have special computational software. The computational algebra system Magma is especially handy for doing number theory, though there are still some analogues, among them are systems called Sage and PARI/GP. The author used Magma quite a lot while working on the content of the present thesis. He has created many interesting scripts which he would like to share with the reader. The example given below is of course quite elementary and by no means interesting, but assists us to illustrate how we can use Magma to check statements and claims occurring in the text.

```
// Testing Artin reciprocity and Chebotarev density for f(x) = x^3 - 3*x + 1
U, g := ResidueClassRing(81);
x := (g(2))^3;
H := { x^i : i in [1..18]};
U, "H = ", H;
numberOfFactorsByPrediction := 0;
counter := 0;
bound := 250;
for i in [1..bound] do
    p := NthPrime(i);
    k := GF(p);
    R<x> := PolynomialRing(k);
    f<x> := x^3 - 3*x + 1;
    if g(p) in H then
        numberOfFactorsByPrediction := 3;
        counter := counter+1;
    else
        numberOfFactorsByPrediction := 1;
```

```
    end if;
    p, numberOfFactorsByPrediction, #Factorization(f);
end for;
"The density of A_f is approximately", (counter/bound);
```

The reader can run the script in a freely-available online calculator located at the address: `http://magma.maths.usyd.edu.au/calc/` or use it on any other machine with preinstalled Magma. The output should look like this:

```
Residue class ring of integers modulo 81
H =  { 17, 35, 1, 53, 19, 37, 71, 55, 73, 8, 26, 44, 10, 28, 62, 46, 80, 64 }
2 1 1
3 1 1
...
...
1579 1 1
1583 3 3
The density of A_f is approximately 8/25
```

The given output allows us to convince ourselves that at least for the first 250 primes the predicted reciprocity law holds. At the same time we can see that the proportion of those primes lying in A_f is $\frac{8}{25}$ which is quite close to the predicted limit value given by the Chebotarev density Theorem. For any issues related to the syntax of Magma and its current functionality we definitely recommend to consult the Magma manual disposed at the same link. Another good reference is [4].

1.2 Splitting of Ideals in Number Fields

Let K be a number field, i.e., a finite field extension of the field of rational numbers $\mathbb{Q}$. This extension is given by adjoining to $\mathbb{Q}$ an element α satisfying a polynomial relation $f(\alpha) = 0$, where $f(x)$ is as before a monic irreducible polynomial with integer coefficients. Let $\mathcal{O}_K$ denote the ring of integers of K, i.e., the integral closure of $\mathbb{Z}$ in K. Note that $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, but usually $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$. On the other hand $\mathbb{Z}[\alpha]$ is not that far from $\mathcal{O}_K$, in the sense that it has finite index inside $\mathcal{O}_K$, i.e., $|\mathcal{O}_K/\mathbb{Z}[\alpha]| < \infty$. In contrast to $\mathbb{Z}$, the ring $\mathcal{O}_K$ is not in general a unique factorization domain, but is a Dedekind domain and therefore admits a unique factorization of ideals into a product of prime ideals. Each prime ideal of $\mathbb{Z}$ is principal and generated by a prime number $(p) = p\mathbb{Z}$, but the ideal $p\mathcal{O}_K$ may not be prime in $\mathcal{O}_K$. Let $p\mathcal{O}_K = \mathfrak{p}_1^{\mathfrak{e}_1} \dots \mathfrak{p}_m^{\mathfrak{e}_m}$ be the factorization of the ideal $p\mathcal{O}_K$ in $\mathcal{O}_K$. In this situation we will say that a prime ideal $\mathfrak{p}_i$ lies over $p\mathbb{Z}$, or that $\mathfrak{p}_i$ divides $p\mathbb{Z}$. The number $\mathfrak{e}_i$ is called the *ramification index* of $\mathfrak{p}_i$. A prime ideal $p\mathbb{Z}$ is unramified if $\mathfrak{e}_i = 1$ for $1 \leq i \leq m$ and ramified otherwise. Note that in each number field K there are only finitely many ramified primes. The quotient $\mathcal{O}_K/\mathfrak{p}_i$ is an $\mathbb{F}_p$-vector space and its dimension is called the *inertia index* of $\mathfrak{p}_i$ and usually denoted by $\mathfrak{f}_i$. If for all $1 \leq i \leq m$ we have $\mathfrak{e}_i = \mathfrak{f}_i = 1$ then we say that $p\mathbb{Z}$ *splits completely in* $\mathcal{O}_K$. We denote by $\mathrm{Spl}(K)$ the set of all prime numbers p in $\mathcal{P}$ such that $p\mathbb{Z}$ splits completely in $\mathcal{O}_K$. If $m = 1$

and $\mathfrak{e}_1 = 1$ then $p\mathbb{Z}$ is *inert in* $\mathcal{O}_K$. In what follows, for every commutative ring R we denote by (p) the principal ideal generated by an element $p \in R$. In particular $(p) = p\mathcal{O}_K$ as an ideal of $\mathcal{O}_K$.

The following classical result provides a connection between factorization of the ideal (p) in $\mathcal{O}_K$ and the question about factorization of $f(x)$ modulo p :

Theorem 1.2 (Kummer-Dedekind)**.** *In the above setting suppose that a prime number p does not divide the index $|\mathcal{O}_K/\mathbb{Z}[\alpha]|$. Let $f(x) = g_1^{a_1}(x)\dots g_n^{a_m}(x) \mod p$ be a factorization of $f(x)$ into distinct monic irreducible polynomials in $\mathbb{F}_p[x]$. Let $\tilde{g}_i(x)$ be any lift of $g_i(x)$ to characteristic zero, i.e., $\tilde{g}_i(x) \in \mathbb{Z}[x]$, $\tilde{g}_i(x)$ is monic and $\tilde{g}_i(x) = g_i(x) \mod p$. For $1 \le i \le m$ define an ideal $\mathfrak{p}_i = (\overline{g_i}(\alpha), p)$. Then $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$, moreover $(p) = \mathfrak{p}_1^{\mathfrak{e}_1}\dots\mathfrak{p}_m^{\mathfrak{e}_m}$ and for all $1 \le i \le m$ we have $\mathfrak{e}_i = a_i$, $\mathfrak{f}_i = \deg(g_i)$.*

Proof. See [33], chapter IV. □

Now the main problem we are interested in can be stated as follows: *given a number field K, find the factorizations of the ideal $(p) \subset \mathcal{O}_K$ into prime ideals, for all prime numbers p.*

To any ideal $\mathfrak{a} \in \mathcal{O}_K$ one associates its norm $\mathcal{N}(\mathfrak{a})$ which is defined as the number of elements in the quotient $\mathcal{O}_K/\mathfrak{a}$: $\mathcal{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. The norm is multiplicative: if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in $\mathcal{O}_K$ then $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.

Remark 1.3. *Given a prime ideal $\mathfrak{p}$ one has $\mathcal{N}(\mathfrak{p}) = p^{\mathfrak{f}}$. In particular, one could recover from $\mathcal{N}(\mathfrak{p})$ the prime number p such that $(p) = \mathfrak{p}\cap\mathbb{Q}$ and its inertia index $\mathfrak{f}$. This circumstance plays a crucial role in the whole story we will discuss later. Note that the analogue of this statement in the function field case is completely wrong and that is the reason why the present thesis has been written.*

Obviously, for almost all except finitely many ramified primes our question is equivalent to know how many prime ideals of a given norm there are. We give two examples related to polynomials discussed above:

Example 1.4. *Let $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$ and therefore the splitting behaviour (p) is equivalent to the consideration $f(x) = x^2 + 1$ modulo p. The discriminant of $f(x)$ is (-4) therefore (2) is the only ramified prime in $\mathcal{O}_K$. We have $x^2 + 1 = (x+1)^2 \mod 2$ and hence $(2) = \mathfrak{p}^2$, where $\mathfrak{p} = (2, 1+i)$. If $p = 1 \mod 4$ then (p) splits in two primes $(p) = \mathfrak{p}_1\mathfrak{p}_2$ each of norm $\mathcal{N}(\mathfrak{p}_1) = \mathcal{N}(\mathfrak{p}_2) = p$. Finally if $p = 3 \mod 4$ then (p) is a prime ideal of norm $\mathcal{N}(p) = p^2$.*

Example 1.5. *Let $K = \mathbb{Q}(\alpha)$, where α is the real root of $f(x) = x^3 - x + 1$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and the only ramified prime is 23. We have $(23) = \mathfrak{p}_1\mathfrak{p}_2^2$, where $\mathfrak{p}_1 = (23, 3+\alpha)$, $\mathfrak{p}_2 = (23, 13+\alpha)$. For each prime number p different from 23 there are the following possibilities: if $f(x)$ has no roots modulo p then above (p) there is only one prime ideal $\mathfrak{p}$ with norm p^3, if $f(x)$ has only one root then over (p) there are two prime ideals one with norm p and another one with norm p^2, finally if $f(x)$ has three roots modulo p then there are three prime ideals lying above (p) each of norm p.*

All notions of this paragraph are easy to generalise to the case of arbitrary extensions of number fields L/K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, similarly to the case of extensions of the rational numbers $\mathbb{Q}$, the ideal $\mathfrak{p}\mathcal{O}_L$ may not be necessarily prime in $\mathcal{O}_L$. Suppose we have a factorization of the ideal $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$ as $\mathfrak{q}_1^{\mathfrak{e}_1} \dots \mathfrak{q}_m^{\mathfrak{e}_m}$. We translate all notions word by word replacing the prime ideal (p) in $\mathbb{Z}$ by a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. Only the notation of the *inertia index* needs some comment. It the general setting we have that $\mathcal{O}_L/\mathfrak{q}_i$ is a vector space over $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. The dimension of this vector space is called the inertia index of $\mathfrak{q}_i$ over $\mathfrak{p}$ and is denoted by $\mathfrak{f}_i$. As before we have the relation $\mathcal{N}(\mathfrak{q}_i) = \mathcal{N}(\mathfrak{p})^{\mathfrak{f}_i}$.

1.3 Dedekind zeta-function

In order to work with norms of prime ideals it is convenient to assemble all of them in one object which is called the *Dedekind zeta-function* of K. This object is not only a crucial tool in the study of distribution properties of prime ideals, but also has a lot of remarkable properties interesting by themselves. We will briefly recall these properties but first, let us start from the Riemann zeta-function $\zeta(s)$ which is the *Dedekind zeta-function* of the field $\mathbb{Q}$ of rational numbers. A good reference is chapter VII from [36] and [30], [31].

1.3.1 Riemann zeta-function

Let $K = \mathbb{Q}$. In order to study distribution properties of prime numbers p among all integer numbers $\mathbb{Z}$ one considers the famous Riemann zeta-function:

$$\zeta(s) = \prod_{i=1}^{\infty} \frac{1}{1-p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

A priori this function is defined only for complex numbers s with $\Re(s) > 1$, where $\Re(s)$ denotes the real part of s. But one can show that it has an analytic continuation as a meromorphic function on the whole complex plane $\mathbb{C}$ with only one pole at $s = 1$. Moreover this pole is simple and the residue of $\zeta(s)$ at $s = 1$ is one:

$$\lim_{s\to 1}(s-1)\zeta(s) = 1.$$

A standard way to get the meromorphic continuation to $\mathbb{C}$ is to consider the function $\widehat{\zeta}(s) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$ which is defined for all s with $\Re(s) > 0$ and show the identity $\zeta(s) = \widehat{\zeta}(s)\frac{1}{1-2^{1-s}}$ which allows to define $\zeta(s)$ for s with $\Re(s) > 0$, $s \neq 1$. Then using the functional equation discussed below one extends $\zeta(s)$ as analytic function to the whole complex plane without one point $s = 1$.

Many issues about distribution of primes become more accessible after rephrasing in terms of analytic properties of $\zeta(s)$. For example, consider the famous *prime number Theorem* conjectured by Gauss in 1793 which states that:

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1,$$

where $\pi(x) = \#\{p \in \mathcal{P} | p \leq x\}$ is the prime-counting function. Riemann showed in 1859 that this statement is equivalent to the statement that $\zeta(s)$ has no zeros on the line $s = 1+it$, $t \in \mathbb{R}$. Finally the last claim was proved independently by Jacques Hadamard and Charles Jean de la Vallee-Poussin in 1896, see [30].

This function has also some other remarkable properties. For instance, it satisfies the following *functional equation* mentioned above:

$$\zeta(s) = \zeta(1-s)2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s),$$

where $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$ is the gamma function.

Another remarkable point is the phenomena of the so-called *special values* of $\zeta(s)$:

$$\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6},\ \zeta(4) = \sum_{n=1}^{\infty}\frac{1}{n^4} = \frac{\pi^4}{90},\ \zeta(6) = \sum_{n=1}^{\infty}\frac{1}{n^6} = \frac{\pi^6}{945},$$

and more generally:

$$\zeta(2n) = \frac{(-1)^{n+1}(2\pi)^{2n}B_{2n}}{2(2n)!},$$

where B_{2n} denotes the famous Bernoulli number defined as coefficients of the Todd Series:

$$\frac{e^x x}{e^x - 1} = \sum \frac{B_n x^n}{n!}.$$

1.3.2 Dedekind zeta-Function

For a general number field K one defines $\zeta_K(s)$ as

$$\zeta_K(s) = \prod_{\mathfrak{p}}\frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} = \sum_{\mathfrak{a}\subset\mathcal{O}_K}\frac{1}{\mathcal{N}(\mathfrak{a})^s},$$

where the product is taken over all non-zero prime ideals and sum is taken over all ideals of $\mathcal{O}_K$. This function has a lot of similarities with $\zeta(s)$. It also has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$. But now the residue at $s = 1$ is given by the *class number formula*:

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{h_K \operatorname{Reg}_K 2^{r_1}(2\pi)^{r_2}}{w_K\sqrt{|\mathcal{D}_K|}}. \tag{1.2}$$

Here r_1 and r_2 stand for the number of real and complex places of K respectively, h_K denotes the class number of K, i.e., the order of the class group $\mathrm{Cl}(K)$ of K, Reg_K is the regulator of K, i.e., the co-volume of the lattice obtained from the image of $\mathcal{O}_K^\times$ in $\mathbb{R}^{r_1+r_2-1}$ after the logarithmic embedding, w_K is the number of roots of unity in K and $\mathcal{D}_K$ is the discriminant of K.

Similarly to $\zeta(s)$, this function is also a very useful tool in the study of the number of ideals with given norm. The *Landau prime ideal Theorem* proved in 1903 states:

$$\lim_{x\to\infty}\frac{\pi_K(x)}{\frac{x}{\log(x)}} = 1,$$

where $\pi_K(x) = \#\{\mathfrak{p}|\mathcal{N}(\mathfrak{p}) \leq x\}$ is the prime ideal counting function.

The Dedekind zeta-function also satisfies the functional equation, see [36] :

$$\Lambda_K(s) = \Lambda_K(1-s),$$

where $\Lambda_K(s) = |\mathcal{D}_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}^{r_1}(s)\Gamma_{\mathbb{C}}^{r_2}(s)\zeta_K(s)$. Here $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$ and $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$.

By using the functional equation we can state the class number formula as follows:

$$\lim_{s\to 0} s^{-r}\zeta_K(0) = -\frac{h_K \operatorname{Reg}_K}{w_K}, \tag{1.3}$$

where $r = r_1 + r_2 - 1$ is the rank of the unit group $\mathcal{O}_K^{\times}$. Moreover, there are a lot of interesting theorems and conjectures concerning special values of $\zeta_K(s)$ at integer numbers, but even a correct formulation of these is far from the scope of the present thesis.

Example 1.6. *If $K = \mathbb{Q}(i)$, then we know from example 1.4 that there exists exactly one prime ideal over (2) and it has norm 2, if $p = 1 \mod 4$ then there are exactly two prime ideals over (p) each has norm p, and if $p = 3 \mod 4$ then there exists only one ideal over (p) with norm p^2. Therefore:*

$$\zeta_K(s) = \frac{1}{1-2^{-s}} \prod_{p=1 \mod 4} \frac{1}{(1-p^{-s})^2} \prod_{p=3 \mod 4} \frac{1}{(1-p^{-2s})} = \zeta_{\mathbb{Q}}(s) \prod_{p\neq 2} \frac{1}{1-(-1)^{\frac{p-1}{2}}p^{-s}}.$$

We have $h_k = 1$, $\operatorname{Reg}_K = 1$, $\mathcal{D}_K = 4$, $r_1 = 0$, $r_2 = 1$, $w_K = 4$. The class number formula reads as:

$$\frac{\pi}{4} = \lim_{s\to 1}(s-1)\zeta_K(s) = \prod_{p\neq 2} \frac{1}{1-(-1)^{\frac{p-1}{2}}p^{-1}} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \dots$$

Example 1.7. *Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 - x + 1$. We have $r_1 = 1$, $r_2 = 1$, $\operatorname{Reg} = \log(|\alpha|)$, $\mathcal{D}_K = -23$, $w_K = 2$, $h_k = 1$. The class number formula reads as:*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \lim_{s\to 1}\left(\frac{1-2^{-s}}{1-2^{-3s}} \cdot \frac{1-3^{-s}}{1-3^{-3s}} \cdot \frac{1}{1-5^{-2s}} \cdot \frac{1}{1-7^{-2s}} \cdots\right) = \frac{2\pi \log(|\alpha|)}{\sqrt{23}} \simeq 0.3684\dots$$

1.4 Arithmetical Equivalence

Now given a number a field K one could ask what kind of information about K can be recovered from $\zeta_K(s)$. For example, using the analytic class number formula it follows immediately that the right-hand side $\frac{h_K \operatorname{Reg}_K}{w_K}$ of the formula 1.3 is invariant. Surprisingly much more is true. For example if K over $\mathbb{Q}$ is normal then actually $\zeta_K(s)$ determines the field K. In the general case it is a theorem of Gassmann (Theorem 1.23 from the section 1.4.3) which provides an interesting connection between number fields sharing the same zeta-function and the theory of finite groups. This connection gives rise to many surprising theorems. Good references for the topic are the expository book [27], [44], and well-written lecture notes [52]. In the next two sections we extensively use the ideas from these materials.

1.4.1 The Galois Case

We start from the case of Galois extensions. Suppose K is a normal, i.e., $|\operatorname{Aut}(K:\mathbb{Q})| = n$, where n is the degree of K. The Galois group of K then fixes each rational prime p and therefore acts on the set of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ lying above $(p) \in \mathcal{O}_K$. This action is transitive and therefore one has $\mathfrak{e}_1 = \mathfrak{e}_2 = \cdots = \mathfrak{e}_m$, $\mathfrak{f}_1 = \mathfrak{f}_2 = \cdots = \mathfrak{f}_m$ and $\mathfrak{e}_i\mathfrak{f}_i = \frac{n}{m}$ for all $1 \leq i \leq m$. In particular this means that if there exists one $\mathfrak{p}_i$ over (p) such that $\mathfrak{f}_i = \mathfrak{e}_i = 1$ then $n = m$ and each $\mathfrak{p}_j$ has norm p.

Remark 1.8. *The converse of the above statement is also true. Given a number field K, suppose that every unramified ideal (p) splits completely in $\mathcal{O}_K$ if it has at least one prime ideal $\mathfrak{p}_1$ above it with $\mathfrak{f}_1 = 1$. Then K is normal.*

This observation and some analytic estimates of the residue of $\zeta_K(s)$ at $s = 1$ lead to the following:

Theorem 1.9. *Let K be a normal extension of $\mathbb{Q}$ of degree n. Then the density of primes which split completely in $\mathcal{O}_K$ exists and is equal to $\frac{1}{n}$, i.e., $\delta(\mathrm{Spl}(K)) = \frac{1}{n}$.*

Proof. See [36], section 13 chapter VII. □

Theorem 1.9 is a crucial point in the investigation of the present thesis and has a big impact on what we are going to discuss. We illustrate the power of this theorem with a few corollaries:

Corollary 1.10. *If K is normal then the set $\mathrm{Spl}(K)$ coincides up to finitely many primes with $\mathcal{A}_{f(x)}$ introduced in the first section, and hence in the case of normal extensions $\delta(\mathcal{A}_{f(x)})$ always exists and is equal to $\frac{1}{\deg(f)}$.*

Corollary 1.11. *Let K and L be two normal number fields such that for all except possibly finitely many primes we have $p \in \mathrm{Spl}(K)$ if and only $p \in \mathrm{Spl}(L)$. Then $K = L$.*

Proof. Let N be a common normal closure of K and L. A prime p splits completely in $\mathcal{O}_N$ if and only if (p) splits completely in both $\mathcal{O}_K$ and $\mathcal{O}_L$ and therefore $\mathrm{Spl}(N) = \mathrm{Spl}(K) \cap \mathrm{Spl}(L)$. We have:

$$\frac{1}{\deg(N:\mathbb{Q})} = \delta(\mathrm{Spl}_N) = \delta(\mathrm{Spl}_K) = \frac{1}{\deg(K:\mathbb{Q})}$$

which implies that $K = N$, and hence L is contained in K. Interchanging the role of K and L one also has that K is contained in L. □

Corollary 1.12. *Let K and L be two normal fields such that $\zeta_K(s) = \zeta_L(s)$. Then $K = L$.*

Proof. The key idea is to determine the set $\mathrm{Spl}(K)$ from $\zeta_K(s)$ and then use the above corollary. For each natural number m consider the number r_m of ideals in $\mathcal{O}_K$ with norm m: $r_m = \#\{\mathfrak{a} | \mathcal{N}(\mathfrak{a}) = m\}$. Combining all primes with given norm in one term in the definition of the Dedekind zeta-function we get:

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{\mathcal{N}(\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{r_n}{n^s}.$$

We know that r_p is positive if and only if over p there is an ideal with norm p. This ideal is necessarily prime since the only ideal with norm one is $\mathcal{O}_K$. But then omitting finitely many ramified primes we have that p splits completely in $\mathcal{O}_K$ since K is normal. Therefore up to finitely many primes the set $\mathrm{Spl}(K)$ coincides with $\#\{p \in P | r_p > 0\}$ and hence if $\zeta_K(s) = \zeta_L(s)$ then $\mathrm{Spl}(K)$ matches with $\mathrm{Spl}(L)$ up to finitely many primes and therefore $K = L$. □

Corollary 1.13. *Let K be a finite not necessarily normal extension of $\mathbb{Q}$. The Galois closure N of K is determined by the set $\mathrm{Spl}(K)$, i.e., if K' is another field such that $\mathrm{Spl}(K) = \mathrm{Spl}(K')$ then K and K' have the same Galois closure N. In particular, given K there are at most finitely many fields K' such that $\mathrm{Spl}(K) = \mathrm{Spl}(K')$.*

Proof. A prime ideal (p) splits completely in $\mathcal{O}_K$ if and only if it splits completely in $\mathcal{O}_N$. Therefore the condition $\mathrm{Spl}(K) = \mathrm{Spl}(K')$ implies $\mathrm{Spl}(N) = \mathrm{Spl}(N')$, where N(respectively N') denotes the normal closure of K (of K'). But the previous corollary shows that $N = N'$. The last statement follows from the fact that each number field has only finitely many subfields. □

Corollary 1.14. *For every integer $n > 1$ and every monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ there exist infinitely many prime numbers p such that: $p = 1 \mod n$ and $f(x)$ splits completely modulo p.*

Proof. Given n as above, consider n-th cyclotomic field K_n which is generated by the n-th primitive roots of unity. Let us denote by L the field obtained by adjoining to $\mathbb{Q}$ a root of $f(x)$. Consider a common normal closure N of L and K_n. As before, because of Theorem 1.9 we know that there are infinitely many primes p which split completely in $\mathcal{O}_N$. But p splits completely in $\mathcal{O}_N$ if and only if it splits completely in both $\mathcal{O}_L$ and $\mathcal{O}_{K_n}$. Finally we note that p splits completely in $\mathcal{O}_{K_n}$ if and only if $p = 1 \mod n$ and therefore there are infinitely many primes $p = 1 \mod n$ such that $f(x)$ splits completely modulo p. □

The last corollary is somewhat surprising: it implies for example that we cannot construct a quadratic extension K of $\mathbb{Q}$ such that almost all primes p with $p = 3 \mod 4$ split completely in $\mathcal{O}_K$ and almost all primes with $p = 1 \mod 4$ stay inert, because then it would contradict to the splitting behaviour of principal ideals generated by rational primes in $\mathbb{Z}[i]$. Somehow the fact of existence of one polynomial implies non-existence of other polynomials!

Before we state the main theorem about number fields sharing the same zeta-function in the general case it is convenient to introduce some group-theoretical notions.

1.4.2 Gassmann Triples

We start from a purely group theoretical definition of the so-called Gassman triples and then we briefly cover the main properties of such triples. Given a finite group G and two subgroups H, H' we will call a triple (G, H, H') a *Gassmann triple* if for every conjugacy class $[c]$ in G we have $|[c] \cap H| = |[c] \cap H'|$. In other words if there is a bijection between elements of H to elements of H' which preserves G-conjugacy. This can also be phrased in terms of representations of a finite group G: (G, H, H') is a Gassmann triple if and only we have an isomorphism of induced representations:

$$\mathrm{Ind}_H^G(1_H) \simeq \mathrm{Ind}_{H'}^G(1_{H'}),$$

where 1_H (and $1_{H'}$) denotes the trivial representation of H (of H' respectively). The equivalence between these two definitions is easy to establish after recalling that the character χ_ρ of the representation $\rho = \mathrm{Ind}_H^G(1_H)$ evaluated on an element $g \in G$ is:

$$\chi_\rho(g) = \frac{|[c] \cap H||C_G(g)|}{|H|},$$

where $C_G(g)$ is the centraliser of the element g and $[c]$ denotes the conjugacy class of g. Since two complex representations of a finite group are isomorphic if and only if their characters are equal we have: $\mathrm{Ind}_H^G(1_H) \simeq \mathrm{Ind}_{H'}^G(1_{H'})$ if and only if $\frac{|[c]\cap H|}{|H|} = \frac{|[c]\cap H'|}{|H'|}$ for all $[c]$. Finally one shows that both definitions imply $|H| = |H'|$ and therefore they are equivalent.

We will call a Gassmann triple (G, H, H') *non-trivial* if H and H' are not conjugate inside G. We will also say that a Gassmann triple (G, H, H') has index n, where $n = \frac{|G|}{|H|} = \frac{|G|}{|H'|}$. Here one classical example is:

Example 1.15. *Fix a prime number $p > 2$. Let G be $\mathrm{Gl}_2(\mathbb{F}_p)$ and let $H = \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \in G \right\}$ and $H' = \left\{ \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix} \in G \right\}$. Then the triple (G, H, H') is a non-trivial Gassmann triple.*

Indeed, the map ϕ from G to G defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} d & b \\ c & a \end{bmatrix}$ satisfies $\phi(AB) = \phi(B)\phi(A)$ and hence provides us with a bijection from H to H' which preserves G-conjugacy. At the same time it is not difficult to see by the direct computations that H and H' are not conjugate inside G.

One natural question to ask is: *what kind of properties do the groups H and H' share*? Are they necessarily have to be isomorphic as abstract groups? The answer to this problem is given by Theorem 1.3 from [52]:

Lemma 1.16. *If (G, H, H') form a Gassmann triple, then there exists an order-preserving bijection between the elements of H and elements of H'. Moreover, given isomorphism classes of abstract groups H_1, H_2 and an order-preserving bijection between their elements, there exist a group G and a Gassmann-triple (G, H, H') with $H \simeq H_1$ and $H' \simeq H_2$.*

Proof. The first claim is entirely obvious, because all elements in the same conjugacy class share the same order. In order to prove the second part one needs to consider groups H, H' as subgroups of the permutation group S_n with $n = \#H$, where the embedding H to S_n is given by the action of H on itself by multiplication. For every element $h \in H$ the cycle type of the corresponding permutation is a union of disjoint cycles of the same length which is equal to the order of h. But two elements of S_n are conjugate if and only if they share the same cycle type and hence order preserving bijection between H and H' provides us with a bijection which preserves G-conjugacy. □

Remark 1.17. *It was also mentioned in [52] that the above Lemma shows that for a given prime number p it is possible to construct a non-trivial Gassmann triple with H isomorphic to the abelian group $(C_p)^3$ and H' isomorphic to the Heisenberg group H_p over $\mathbb{F}_p$, since both these groups have p^3 elements and are of exponent p. Because they are not isomorphic they cannot be conjugate and therefore the triple $(S_{p^3}, H_p, (C_p)^3)$ is a non-trivial Gassmann triple.*

Gassmann triples have a lot of remarkable properties which are interesting not only by themselves, but also because they can be applied to number theoretical statements. Here is an example of one of such properties proved in [44]:

Theorem 1.18. *Let G be a finite group and $H \subset G$ a subgroup of index n. Suppose one of the following conditions holds:*

1. *$n \leq 6$;*
2. *H is cyclic;*
3. *$G = \mathbb{S}_n$ the full symmetric group of order n;*
4. *$n = p$ is prime and $G = \mathbb{A}_p$ is the alternating group of order p.*

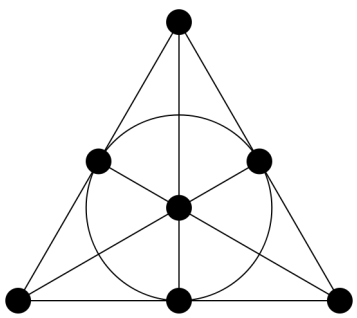
then any Gassmann triple (G, H, H') is trivial.

We also state another interesting fact from [14] which we later apply to our problem:

Theorem 1.19. *If a finite group G admits a non-trivial Gassmman triple (G, H, H') then the order of G is divisible by the product of at least five not necessarily distinct primes.*

One could address another purely group theoretical matter: for which natural number n does there exist a finite group G with two subgroups H, H' of index n such that (G, H, H') is a non-trivial Gassmann triple? For $n \leq 15$ these groups were classified by Wieb Bosma and Bart de Smit in [5]. An important series of examples consists of groups of Gl-type, for instance: $\mathrm{PSL}_2(\mathbb{F}_7)$, $\mathrm{Gl}_2(\mathbb{F}_3)$, $\mathrm{PGL}_3(\mathbb{F}_2)$. These groups are especially interesting because torsion points on elliptic curves defined over $\mathbb{Q}$ allow us *to construct explicitly Galois-extensions with such Galois groups*. As we will see later, this construction together with Theorem 1.23 from the next section supply us with a natural way to produce non-isomorphic number fields sharing the same zeta-function, see article [9] and section 2.2.1 for the details.

Some instances of Gassmann triples can be obtained by geometric methods. Let us illustrate this in the case of $G = \mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{PGL}_3(\mathbb{F}_2)$. The famous Fano plane is the projective plane over the field $\mathbb{F}_2$ of two elements. The group G acts on the Fano plane via linear transformations and this action can be described in terms of the automorphisms of the following graph:



One picks two subgroups: H which stabilises some fixed vertex and H' which stabilises some fixed edge. Note that they are both of index seven. One can show that (G, H, H') form a non-trivial Gassmann triple and moreover the following is true:

Remark 1.20. *The triple (G, H, H') is the unique non-trivial Gassmann triple of index seven.*

Intently considering above examples one can suspect that Gassmann triples arise from some kind of duality and hence it should be difficult to produce a group G with three (or more) pairwise non-conjugate subgroups H_i, $1 \leq i \leq 3$ such that $\mathrm{Ind}_{H_i}^G(1_{H_i}) \simeq \mathrm{Ind}_{H_j}^G(1_{H_j})$ for $i, j \in \{1, 2, 3\}$. Actually that is not the case as shown by the following proposition:

Lemma 1.21. *If (G, H_1, H_2), (G', H_1', H_2') are two non-trivial Gassmann triples then inside the group $\mathcal{G} = G \times G'$ the four subgroups $A_{i,j} = H_i \times H_j'$, $i, j \in \{1, 2\}$ are pairwise non-conjugate and share the same isomorphism class of the permutation representations $\mathrm{Ind}_{A_{i,j}}^{\mathcal{G}}(1_{A_{i,j}})$.*

Proof. The groups $A_{i,j}$ are pairwise non-conjugate because conjugation in $\mathcal{G}$ provides (via projection) a conjugation in G and G' and hence we obtain a contradiction with the fact that the above triples are non-trivial. The second part of the statement follows from the observation that $\mathrm{Ind}_{A_{i,j}}^{\mathcal{G}}(1_{A_{i,j}}) \simeq \mathrm{Ind}_{H_i}^G(1_{H_i}) \otimes \mathrm{Ind}_{H_j'}^{G'}(1_{H_j'})$ and the fact that $\mathrm{Ind}_{H_1}^G(1_{H_1}) \simeq \mathrm{Ind}_{H_2}^G(1_{H_2})$ and $\mathrm{Ind}_{H_1'}^{G'}(1_{H_1'}) \simeq \mathrm{Ind}_{H_2'}^{G'}(1_{H_2'})$ because (G, H_1, H_2), (G', H_1', H_2') are Gassmann triples. □

Finally, using Lemma 1.21 and the construction from example 1.15 one obtains the following:

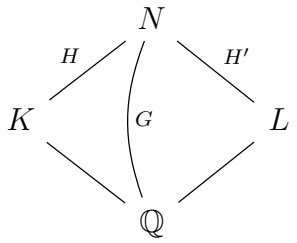
Lemma 1.22. *For a given natural number n there exists a group G with a sequence of at least 2^n pairwise non-conjugate subgroups sharing the same isomorphism class of the permutation representations.*

Proof. Fix a natural number n. Let $p_1, \ldots, p_n$ be n pairwise distinct odd prime numbers. Then the following group satisfies conditions of the Lemma:

$$G = \prod_{i=1}^{n} \mathrm{Gl}_2(\mathbb{F}_{p_i}).$$ □

1.4.3 On Perlis Theorem

Now let K and L be two number fields, not necessarily normal. We will say that they *split equivalently* if for all except possibly finitely many prime numbers $p \in \mathcal{P}$ there exists a bijection ϕ_p from the set of primes in $\mathcal{O}_K$ lying above (p) to the set of those primes in $\mathcal{O}_L$. We will say that they are *arithmetically equivalent* if for all except possibly finitely many p the bijection ϕ_p can be chosen to be degree preserving, i.e., $\mathfrak{f}_i = \mathfrak{f}_{\phi_p(\mathfrak{p}_i)}$. Let N denote the common Galois closure of K and L over $\mathbb{Q}$ and let $G = \mathrm{Gal}(N/\mathbb{Q})$, $H = \mathrm{Gal}(N/K)$, $H' = \mathrm{Gal}(N/L)$. See the diagram below.



In the above setting we have the following famous result, see [44] and [51]:

Theorem 1.23. *The following statements are equivalent:*

1. $\zeta_K(s) = \zeta_L(s)$;
2. *K and L are arithmetically equivalent;*
3. *K and L split equivalently;*
4. *(G, H, H') is a Gassmann triple.*

Moreover, if one of the above conditions holds then K and L have the same degree, the same discriminant, the same normal closure, the same number of real and complex embeddings and the groups of units of their rings of integers are isomorphic.

Remark 1.24. *If K and L are arithmetically equivalent then a priori $\zeta_K(s) = \zeta_L(s)$ up to finitely many factors. The above Theorem then says that actually their zeta-functions are equal, i.e., that one could omit the condition "except finitely many primes" in the definition of arithmetical equivalence, but then it becomes slightly more tricky to show that two fields are arithmetically equivalent: sometimes it is convenient to omit finitely many primes.*

It follows directly from the definition that the triple (G, H, H') is non-trivial if and only if K is not isomorphic to L, as an abstract field or equivalently as extension of $\mathbb{Q}$. Theorem 1.23 allows us to use group theory to study arithmetical properties of number fields. For instance:

Corollary 1.25. *Suppose K is a number field and N is its normal closure. Let $G = \mathrm{Gal}(N/\mathbb{Q})$, $H = \mathrm{Gal}(N/K)$ and suppose one of the conditions from Theorem 1.18 holds. Then $\zeta_K(s)$ determines the field K up to isomorphism, i.e. if for any other number field L one has $\zeta_K(s) = \zeta_L(s)$, then $K \simeq L$.*

Here is another application which now follows directly from Theorem 1.19:

Corollary 1.26. *Let K be a number field with the degree of the normal closure N of K strictly less than 32. Then $\zeta_K(s)$ determines K up to isomorphism.*

Now let us consider some classical constructions of arithmetically equivalent number fields. Observe fist that since the degree of K over $\mathbb{Q}$ is the index of H in G we get that if the degree of K does not exceed 6, then equality $\zeta_K(s) = \zeta_L(s)$ implies $K \simeq L$. On the other hand there are infinitely many non-isomorphic pairs (K_α, L_α) of (isomorphism classes of) fields of degree seven such that $\zeta_{K_\alpha}(s) = \zeta_{L_\alpha}(s)$. Moreover because of remark 1.20 each pair (K, L) of non-isomorphic number fields of degree seven with $\zeta_K(s) = \zeta_L(s)$ occurs as subfields of some normal field N with $\mathrm{Gal}(N : \mathbb{Q}) = \mathrm{PSL}_2(\mathbb{F}_7)$, $\mathrm{Gal}(N : K) = H$ and $\mathrm{Gal}(N : L) = H'$.

Example 1.27. *Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^7 - 7x + 3$ and let $K' = \mathbb{Q}(\beta)$, where β is a root of $g(x) = x^7 + 14x^4 - 42x^2 - 21x + 9$. Then K and K' are arithmetically equivalent fields occurring in the triple with $G = \mathrm{PSL}_2(\mathbb{F}_7)$ discussed above.*

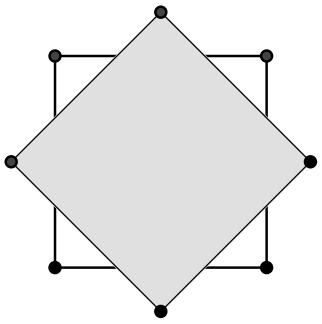
It is more convenient to provide another example of such a family for degree eight.

Example 1.28. *Let a be any integer such that both $|a|$ and $|2a|$ are not squares. Then the two fields $\mathbb{Q}(\sqrt[8]{a})$ and $\mathbb{Q}(\sqrt[8]{16a})$ are arithmetically equivalent.*

Proof. Consider two polynomials $f(x) = x^8 - a$ and $g(x) = x^8 - 16a$. The conditions above insure that these polynomials are irreducible. We claim that for almost all except finitely many primes p these polynomials split in the same way modulo p. Indeed if either $\sqrt{2} \in \mathbb{F}_p$ or $\sqrt{-2} \in \mathbb{F}_p$ then 16 is an eighth power. If both $\sqrt{2}$ and $\sqrt{-2}$ are not in $\mathbb{F}_p$ then $i = \sqrt{-1} \in \mathbb{F}_p$ and hence $(1+i)^8 = 16$. It means in both cases that $f(x)$ and $g(x)$ considered modulo p are related by the linear change of the variable and therefore the degree of irreducible factors of the decomposition $f(x)$ and $g(x)$ modulo a prime p coincide for almost all $p \in \mathcal{P}$. Therefore the fields $\mathbb{Q}(\sqrt[8]{a})$ and $\mathbb{Q}(\sqrt[8]{16a})$ are arithmetically equivalent and hence share the same zeta-function. □

Remark 1.29. *The simplicity of the above example is in some sense exceptional:* Theorem 1, chapter 9 *from* [2] *states that if for some fixed odd number m there exists $a \in \mathbb{Z}$ such that for all except possibly finitely many primes the equation $x^m = a \mod p$ has a solution then the equation $x^m = a$ has a solution in $\mathbb{Z}$.*

The Galois group G of the normal closure of the field $\mathbb{Q}(\sqrt[8]{a})$ mentioned above is isomorphic to a semi-direct product $C_8 \rtimes V_4$ where C_8 is a cyclic group of order eight, V_4 is the Klein group and the action of V_4 on C_8 given via the isomorphism $V_4 \simeq \mathrm{Aut}(C_8)$. As pointed out by the authors the group G could be obtained as a subgroup of the automorphism group of the following graph:



It has two subgroups: H which stabilises a given vertex and H' which stabilises a given edge. The triple (G, H, H') is exactly the Gassmann triple corresponding to the fields from example 1.28 stated above. Both examples 1.28 and 1.27 already occurred in [44].

Magma Scripts

One can use the following Magma script to verify Theorem 1.23 using fields mentioned in the example 1.28:

```
R<x> := PolynomialRing(Integers());
f := x^8 - 15;
g := x^8 - 240;
K<y> := NumberField(f);
L<z> := NumberField(g);
"K is: ", K;
"L is: ", L;
"Are fields K, L isomorphic? Answer:", IsIsomorphic(K, L);
G, r, N := GaloisGroup(K);

"Degree of the normal closure N of K is", #G;
"The Galois Group of K is: ", G;

// Setting subgroups corresponding to x^8-15 and x^8-240
h := Subgroups(G: IndexEqual := 8);
H_1 := h[8]`subgroup;
H_2 := h[9]`subgroup;
"The group H_1 corresponds to the field extensions: ", GaloisSubgroup(N, H_1);

"The group H_2 corresponds to the field extensions: ", GaloisSubgroup(N, H_2);

//Checking that (G, H_1, H_2) is a non-trivial Gassmann triple
"Are H_1, H_2 conjugate inside G? Answer: ", IsConjugate(G, H_1, H_2);
"Permutation Character for G/H_1: ", PermutationCharacter(G, H_1);
"Permutation Character for G/H_2: ", PermutationCharacter(G, H_2);

"Testing that K and L are arithmetically equivalent: ";
for i in [1..10] do
    p := NthPrime(i);
    k := GF(p);
    R<x>:=PolynomialRing(k);
    f1 := x^8 - 15;
    f2 := x^8 - 240;
    "Factorization of x^8-15 mod", p, Factorization(f1);
    "Factorization of x^8-240 mod ", p, Factorization(f2);
end for;

"Verifying that values of zeta_K and zeta_L evaluated at 2 coincide: ";
zeta_K := LSeries(K);
zeta_L := LSeries(L);
```

```
"zeta_K(2) = ", Evaluate(zeta_K, 2);
"zeta_L(2) = ", Evaluate(zeta_L, 2);
```

The truncated output of the script shows:

```
K is:  Number Field with defining polynomial x^8 - 15 over the Rational Field
L is:  Number Field with defining polynomial x^8 - 240 over the Rational Field
Are fields K, L isomorphic? Answer: false
Degree of the normal closure N of K is 32
The Galois Group of K is:  Permutation group G acting on a set of cardinality 8
Order = 32 = 2^5
    (1, 6, 8, 3)(2, 5, 7, 4)
    (1, 2, 5, 3, 8, 7, 4, 6)
    (1, 8)(4, 5)
    (1, 4, 8, 5)(2, 6, 7, 3)
    (1, 8)(2, 7)(3, 6)(4, 5)
The group H_1 corresponds to the field extensions:  x^8 - 15
x2
The group H_2 corresponds to the field extensions:  x^8 - 240
(x1 + x4)
Are H_1, H_2 conjugate inside G? Answer:  false
Permutation Character for G/H_1:  ( 8, 0, 4, 2, 0, 2, 0, 0, 0, 0, 0 )
Permutation Character for G/H_2:  ( 8, 0, 4, 2, 0, 2, 0, 0, 0, 0, 0 )
Testing that K and L are arithmetically equivalent:
...
Factorization of x^8-15 mod 23 [
    <x^2 + 2*x + 17, 1>,
    <x^2 + 8*x + 17, 1>,
    <x^2 + 15*x + 17, 1>,
    <x^2 + 21*x + 17, 1>
]
Factorization of x^8-240 mod  23 [
    <x^2 + 6*x + 11, 1>,
    <x^2 + 10*x + 11, 1>,
    <x^2 + 13*x + 11, 1>,
    <x^2 + 17*x + 11, 1>
]
Factorization of x^8-15 mod 29 [
    <x^8 + 14, 1>
]
Factorization of x^8-240 mod  29 [
    <x^8 + 21, 1>
]

Verifying that values of zeta_K and zeta_L evaluated at 2 coincide:
```

```
zeta_K(2) =  1.669536050983038699624321276 86
zeta_L(2) =  1.669536050983038699624321276 86
```

Remark 1.30. Sometimes even highly sophisticated computer software produces mistakes. This also happened a few years ago when the author executed the above script: the last part of the script which evaluates values of ζ-functions wrongly suggested that ζ-functions should be different! It turned out that there was a problem with computing the values $\zeta_K(2)$ and $\zeta_L(2)$, but it took some time to actually realise it. The problem had been fixed quickly after the author informed the Magma development team.

1.4.4 Common Properties of Arithmetically Fields

Let us briefly discuss properties of arithmetically equivalent number fields. Despite the fact that the Dedekind zeta-function $\zeta_K(s)$ of K provides us with evidence about some numerical invariants of K it actually almost determines many other "non-numerical" invariants, for example the ideal class group. The reason for that is the existence of the so-called *arithmetical homomorphism* between multiplicative groups of arithmetically equivalent fields. An interested reader could consult the corresponding chapter in [27].

Class Groups

Because of the class number formula 1.3 and the fact that arithmetically equivalent number fields share the same number of roots of unity w_K one has the following implication:

$$\zeta_K(s) = \zeta_L(s) \Rightarrow h_K \operatorname{Reg}_K = h_L \operatorname{Reg}_L .$$

Surprisingly the class numbers of arithmetically equivalent number fields h_K and h_L may be different, see [10]. Nevertheless, there is a good bound on that difference. Namely, to each Gassmann triple (G, H, H') Perlis in [39] attached a natural number v, which divides the order of H. Suppose that K and K' are two number fields corresponding to the triple (G, H, H'). Then if a prime number l does not divide v, then the l-part of the class group of K and K' are isomorphic: $\mathrm{Cl}_l(K) \simeq \mathrm{Cl}_l(K')$.

His argument works in the following way: first for any Gassmann triple (G, H, H') let us fix an isomorphism α between two induced representations: $\mathrm{Ind}_H^G(1_H) \simeq \mathrm{Ind}_{H'}^G(1_{H'})$. Note that $\mathrm{Ind}_H^G(1_H)$ is a permutation representation and therefore this isomorphism can be considered as an isomorphism between $\mathbb{Q}[G]$-modules:

$$\alpha : \mathbb{Q}[G/H] \simeq_{\mathbb{Q}[G]} \mathbb{Q}[G/H'].$$

A triple (G, H, H') is non-trivial if these modules are not isomorphic as G-modules $\mathbb{Q}[G/H] \not\simeq_G \mathbb{Q}[G/H']$. Once an isomorphism α is fixed one can also pick a standard basis of the vector spaces $\mathbb{Q}[G/H]$, $\mathbb{Q}[G/H']$ and then α can be written as matrix M_α. Let $v_\alpha = \det(M_\alpha)$. Now given a Gassmann triple (G, H, H') he defined a natural number $v = \gcd_\alpha(|v_\alpha|)$, where α runs over all isomorphisms such that M_α has integral coefficients.

On the other hand, from this isomorphism α he constructed a homomorphism ϕ_α of multiplicative groups $\phi_\alpha : K^* \to (K')^*$. This map factors through fractional ideals and therefore induces morphism between ideal class groups. The map between class groups has a kernel and co-kernel and R. Perlis proved that primes dividing the order of these groups divide the natural number v_α associated to α. From this one easily deduces the argument about isomorphism of l-parts of class groups for l not dividing v. It was mentioned in [39] that for the Gassmann triple (G, H, H') with $G \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ and H of index seven one has $v = 8$ and therefore for each pair (K, K') of arithmetically equivalent number fields coming from this triple and each odd prime number l one has:

$$\mathrm{Cl}_l(K) \simeq \mathrm{Cl}_l(K').$$

Remark 1.31. *There exists an example of a non-trivial Gassmann triple (G, H, H') such that the invariant v is one, see* [40]*. The group G in this example is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{29})$, has order 12180 and contains two subgroups H, H' each isomorphic to the alternating group A_5 and of index 203. This triple has the property that not only $\mathbb{Q}[G/H] \simeq_{\mathbb{Q}[G]} \mathbb{Q}[G/H']$ but also $\mathbb{Z}[G/H] \simeq_{\mathbb{Z}[G]} \mathbb{Z}[G/H']$, while groups H and H' are still not conjugate inside G.*

Absolute Abelianized Galois Group

The main theorem of the class field theory produces an isomorphism between the Galois group of the maximal unramified abelian extension M_K of K and the class group of K, i.e., $\mathrm{Gal}(M_K : K) \simeq \mathrm{Cl}(K)$. Taking into account the previous discussion we have that arithmetically equivalent fields K, K' have similar groups $\mathrm{Gal}(M_K : K)$ and $\mathrm{Gal}(M_{K'} : K')$ in the following sense. For a given triple (G, H, H'), for all prime numbers l except finitely many which divide the invariant v defined above, any pair of number fields (K, K') arising from the triple has the property that:

$$\mathrm{Gal}_l(M_K : K) \simeq \mathrm{Gal}_l(M_{K'} : K').$$

It turns out that this statement can be generalised to the Galois group of the maximal abelian extension K^{ab} of K. Let $\mathcal{G}_K^{ab}$ denote the abelianized absolute Galois group of a number field K: $\mathcal{G}_K^{ab} = \mathrm{Gal}(K^{ab} : K)$. It is an abelian pro-finite group and denoting by $\mathcal{G}_{K,l}^{ab}$ its l-part for a prime number l co-prime to v, $l \neq 2$, one has, as before:

$$\mathcal{G}_{K,l}^{ab} \simeq \mathcal{G}_{K',l}^{ab}$$

—see [27].

Note that the group $\mathcal{G}_K^{ab}$ is a pro-finite group and hence has a so-called Krull topology under which it becomes a topological group. The above isomorphism then can be considered not only as and isomorphism of abstract groups, but also as an isomorphism of pro-finite groups. We will discuss this in details later, see section 1.6.2.

1.5 Artin L-functions

In this section we define and state basic properties of the so-called Artin L-functions. This is a generalisation of the notion of the Dedekind zeta-function which plays a central role in number theory. The setting is the following: to a Galois extension of number fields $L : K$ with Galois

group $G = \mathrm{Gal}(L : K)$ and a complex representation ρ of G one attaches the Artin L-function $L_K(\rho, s)$ which is a meromorphic function of complex variable s. In order to define it we first need to introduce the notion of the Frobenius Substitution. For reference see [36], chapter 10.

1.5.1 The Frobenius Substitution

Let $L : K$ be a normal extension of number fields of degree n with the Galois group $G = \mathrm{Gal}(L : K)$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_L$ lying above it. Consider the decomposition group $D_\mathfrak{q}$ of the ideal $\mathfrak{q}$:

$$D_\mathfrak{q} = \{\sigma \in G | \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

Denoting the residue fields $\mathcal{O}_K/\mathfrak{p}$ by $k_\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{q}$ by $k_\mathfrak{q}$, there exists a homomorphism from $D_\mathfrak{q}$ to the Galois group of $\mathrm{Gal}(k_\mathfrak{q} : k_\mathfrak{p})$. The kernel $I_\mathfrak{q}$ of this homomorphism is called the *inertia group* of $\mathfrak{q}$. We have the following exact sequence:

$$1 \to I_\mathfrak{q} \to D_\mathfrak{q} \to \mathrm{Gal}(k_\mathfrak{q} : k_\mathfrak{p}) \to 1.$$

Since $k_\mathfrak{q} : k_\mathfrak{p}$ is an extension of finite fields, the Galois group $\mathrm{Gal}(k_\mathfrak{q} : k_\mathfrak{p})$ is cyclic and generated by the Frobenius automorphism $\phi_\mathfrak{p} : x \to x^{\mathcal{N}(\mathfrak{p})}$. Obviously $D_\mathfrak{q}/I_\mathfrak{q} \simeq \mathrm{Gal}(k_\mathfrak{q} : k_\mathfrak{p})$ and since $I_\mathfrak{q}$ is trivial if and only the prime ideal $\mathfrak{p}$ is unramified we have $D_\mathfrak{q} \simeq \mathrm{Gal}(k_\mathfrak{q} : k_\mathfrak{p})$ for all unramified $\mathfrak{p}$. For any ideal $\mathfrak{q}$ we define a Frobenius element at $\mathfrak{q}$ as any element of the pre-image of $\phi_\mathfrak{p}$ in $D_\mathfrak{q}/I_\mathfrak{q}$ and we will denote any such element by $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$. In the case where $\mathfrak{p}$ is unramified $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is an actual element of $G = \mathrm{Gal}(L : K)$, but in general case this element is defined only up to inertia $I_\mathfrak{q}$. If one picks another prime ideal $\mathfrak{q}'$ lying over $\mathfrak{p}$ then $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is a conjugate of $\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}}$:

$$\forall g \in G : \mathrm{Frob}_{g(\mathfrak{q})/\mathfrak{p}} = g\,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,g^{-1}.$$

Finally, we define $\mathrm{Frob}_\mathfrak{p}$ as the conjugacy class of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ for some $\mathfrak{q}$. If G is abelian and $\mathfrak{p}$ is unramified then $\mathrm{Frob}_\mathfrak{p}$ is an element of G and is called the Artin symbol at $\mathfrak{p}$.

1.5.2 Definition of Artin L-functions

In the setting of the previous paragraph let $\rho : G \to \mathrm{Gl}_m(\mathbb{C})$ be a complex representation of G of dimension m. To this data we attach a function of a complex variable s which we denote by $L_K(\rho, s)$. This function will be defined as a product over all places $\mathfrak{p}$ of K of local L-functions.

Suppose first that $\mathfrak{p}$ is unramified. Then we pick any representative g of $\mathrm{Frob}_\mathfrak{p}$. Then $\rho(g)$ is an automorphism of the vector space $V = \mathbb{C}^n$ and we denote its characteristic polynomial by $P_\mathfrak{p}(t)$:

$$P_\mathfrak{p}(t) = \det(E - t\rho(g)),$$

where E denotes the identity matrix. Of course $\rho(g)$ depends on the choice of g, but $P_\mathfrak{p}(t)$ does not. We define *the Euler factor* $L_{K,\mathfrak{p}}(\rho, s)$ at $\mathfrak{p}$ as $P_\mathfrak{p}(\mathcal{N}(\mathfrak{p})^{-s})^{-1}$.

Remark 1.32. *By rewriting* $\det(E - t\rho(g)) = (1 - \lambda_1 t)\dots(1 - \lambda_n t)$, *where* $\lambda_i \in \mathbb{C}^\times$ *we see* $L_{K,\mathfrak{p}}(\rho, s)$ *as a finite product of geometric series* $\frac{1}{\det(E - t\rho(g))} = \prod_{i=1}^n \frac{1}{1-\lambda_i t}$ *which converges for* $t \in \mathbb{C}$ *with* $|t|$ *small enough. By plugging* $t = \mathcal{N}(\mathfrak{p})^{-s}$ *we see that* $L_{K,\mathfrak{p}}(\rho, s)$ *converges for* $\Re(s)$ *big enough.*

If $\mathfrak{p}$ is a ramified prime ideal then we consider the subspace W which is the inertia invariant $W = (V)^{I_\mathfrak{q}}$ part of V. This is not a sub-representation of G but it is a sub-representation ψ of $D_\mathfrak{q}$, moreover the inertia subgroup $I_\mathfrak{q}$ acts trivially and therefore ψ defines a well-defined homomorphism from $D_\mathfrak{q}/I_\mathfrak{q}$ to $\mathrm{Aut}(W)$ and by picking any representative g of $\mathrm{Frob}_\mathfrak{p}$ we could consider the characteristic polynomial $P_\mathfrak{p}(t) = \det(E - t\psi(g))$. As before the characteristic polynomial does not depend on the choice of the representative g and therefore we also define $L_{K,\mathfrak{p}}(\rho, s)$ for ramified primes as $P_\mathfrak{p}(\mathcal{N}(\mathfrak{p})^{-s})^{-1}$.

Finally, we define:

$$L_K(\rho, s) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} L_{K,\mathfrak{p}}(\rho, s).$$

The above argument about the convergence of the local L-factors can be extended to a proof of the fact that the whole Artin L-series $L_K(\rho, s)$ absolutely converges for $\Re(s)$ big enough[1]. It is possible to prove that $L_K(\rho, s)$ satisfies a functional equation which allows us to define it as meromorphic function over $\mathbb{C}$.

Example 1.33. *Consider the example of $K = \mathbb{Q}(i)$. This is a normal extension of $\mathbb{Q}$ with a cyclic Galois group C_2 of order two generated by the complex conjugation τ. Consider the non-trivial character χ of C_2. If for an odd prime number p the ideal (p) splits as $\mathfrak{p}_1\mathfrak{p}_2$ then the decomposition group of each $\mathfrak{p}_i$, $i \in \{1, 2\}$ is trivial and τ switches the ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$. This means that the Euler factor $L_{K,p}(\chi, s)$ at p is $\frac{1}{1-p^{-s}}$. The ideal (p) for $p = 3 \mod 4$ stays inert in $\mathbb{Z}[i]$, the residue field k_p is a quadratic extension of $\mathbb{F}_p$ and $\tau(x) = x^p$ for $x \in k_p$, i.e., τ is the Frobenius at p and since the character χ is non-trivial we have $\chi(\tau) = -1$ and therefore $L_{K,p}(\chi, s) = \frac{1}{1+p^{-s}}$. For the ramified prime (2) we have $I_2 = C_2$ and $V^{I_2} = \{0\}$, therefore the corresponding Euler factor is trivial. Summing up we have:*

$$L_K(\chi, s) = \prod_{p=1 \mod 4} \frac{1}{1-p^{-s}} \prod_{p=3 \mod 4} \frac{1}{1+p^{-s}} = \prod_{p \neq 2} \frac{1}{1-(-1)^{\frac{p-1}{2}}p^{-s}} = \frac{\zeta_K(s)}{\zeta_\mathbb{Q}(s)}.$$

1.5.3 Properties of Artin L-functions

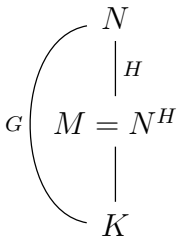
Now we state the basic properties of L-functions needed for further investigation. Let N be a finite Galois extension of a number field K. As usual we denote by G the Galois group $\mathrm{Gal}(N : K)$.

1. *Additivity.* This property states that the L-function of a direct sum of two representations is equal to the product of L-functions of these representations. More concretely, let ρ_1, ρ_2 denote two complex representations of a finite group G. Then

$$L_K(\rho_1 \oplus \rho_2, s) = L_K(\rho_1, s)L_K(\rho_2, s).$$

2. *Induction.* Let H be a not necessarily normal subgroup of G and let $M = N^H$ be the corresponding intermediate field.

[1] the region of the convergence depends on K and ρ of course.



Given a complex representation ρ of H one considers the induced representation $\mathrm{Ind}_H^G(\rho)$ of G. The induction property then says:

$$L_M(\rho, s) = L_K(\mathrm{Ind}_H^G(\rho), s).$$

3. *Inflation.* Suppose in the previous setting that the group H is normal and denote the quotient $G/H = \mathrm{Gal}(M : K)$ by Q. Let ψ be a complex representation of Q. Then it induces a representation Ψ of G via the quotient homomorphism $G \to Q$. The inflation property states:

$$L_K(\Psi, s) = L_K(\psi, s).$$

4. *Multiplicative independence over* $\mathbb{Q}$. Suppose $K = \mathbb{Q}$. Let ρ_1, ρ_2 be two complex representations of $\mathrm{Gal}(N : \mathbb{Q})$. Then:

$$L_{\mathbb{Q}}(\rho_1, s) = L_{\mathbb{Q}}(\rho_2, s) \Leftrightarrow \rho_1 \simeq \rho_2.$$

Note that this claim is not valid if one replaces $\mathbb{Q}$ by another number field, see discussion in the section 2.2.

1.5.4 Examples

Quadratic Extensions

Let K be a quadratic extension of $\mathbb{Q}$. This is a Galois extension with a Galois group G of order two. By the induction property:

$$\zeta_K(s) = L_K(1, s) = L_{\mathbb{Q}}(\mathrm{Ind}_{\{1\}}^G 1, s).$$

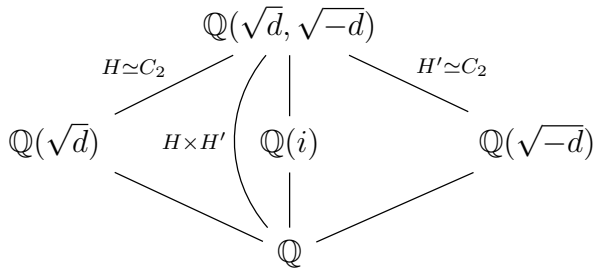
By representation theory one has $\mathrm{Ind}_{\{1\}}^G = 1 \oplus \chi$, where 1, χ denote trivial and non-trivial representations of G respectively. Therefore by the additivity property:

$$\zeta_K(s) = L_{\mathbb{Q}}(1, s) L_{\mathbb{Q}}(\chi, s) = \zeta_{\mathbb{Q}}(s) L_{\mathbb{Q}}(\chi, s),$$

which explains the decomposition in example 1.33.

Biquadratic Extension

Let $d > 0$ be a square-free integer. Consider the field $K = \mathbb{Q}(\sqrt{d}, \sqrt{-d})$. We have the following Galois correspondence diagram:



We have $G = \mathrm{Gal}(K : \mathbb{Q}) = H \times H' \simeq C_2 \times C_2$. This group has four different irreducible characters 1, χ, χ', $\chi\chi'$. It is easy to see that:

$$\mathrm{Ind}_{\{1\}}^{G} 1 \simeq 1 \oplus \chi \oplus \chi' \oplus \chi\chi'.$$

By adding two trivial characters to both sides and taking L-functions we get:

$$\zeta_K(s)\zeta_{\mathbb{Q}}^2(s) = \zeta_{\mathbb{Q}}^3(s) L_{\mathbb{Q}}(\chi, s) L_{\mathbb{Q}}(\chi', s) L_{\mathbb{Q}}(\chi\chi', s) = \zeta_{\mathbb{Q}(\sqrt{d})}(s)\zeta_{\mathbb{Q}(\sqrt{-d})}(s)\zeta_{\mathbb{Q}(i)}(s).$$

Finally by applying the class number formula and using the fact that $\mathrm{Reg}(\mathbb{Q}(i)) = \mathrm{Reg}(\mathbb{Q}(\sqrt{-d})) = h_{\mathbb{Q}(i)} = 1$ one obtains the following formula due to Dirichlet:

$$\frac{h_K \,\mathrm{Reg}(K)}{w_K} = \frac{h_{\mathbb{Q}(\sqrt{d})} h_{\mathbb{Q}(\sqrt{-d})} \,\mathrm{Reg}(\mathbb{Q}(\sqrt{d}))}{4 w_{\mathbb{Q}(\sqrt{d})} w_{\mathbb{Q}(\sqrt{-d})}}.$$

After simplifying the above formula one can show that:

$$\frac{h_K}{h_{\mathbb{Q}(\sqrt{d})} h_{\mathbb{Q}(\sqrt{-d})}} \in \{\frac{1}{2}, 1\}.$$

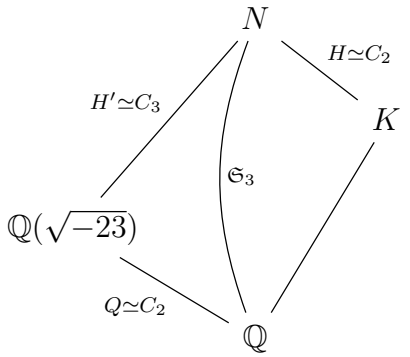
Such kind of relations were generalized by Brauer and now called Brauer relations, see [23].

Extensions with Galois Group $\mathfrak{S}_3$

In general one has $\mathrm{Ind}_{\{1\}}^{G}(1) \simeq \oplus \rho_i^{\dim(\rho_i)}$, where ρ_i runs over all irreducible complex representations of the finite group G. In particular, for every Galois extension N over K we have:

$$\zeta_N(s) = \prod_{\rho_i} L_K(\rho_i, s)^{\dim \rho_i}.$$

Let us consider the example of the normal closure N of the field K given by adjoining a root of the polynomial $x^3 - x - 1$ from section 1.1. Since the discriminant of f is (-23) the Galois group $\mathrm{Gal}(N : \mathbb{Q}) = \mathfrak{S}_3$ is the symmetric group of order six. Let us draw the Galois correspondence diagram:



The group $\mathfrak{S}_3$ has three irreducible complex representations: the trivial representation 1, the one-dimensional sign representation χ and the two-dimensional representation ρ. First of all this means:

$$\zeta_N(s) = \zeta_{\mathbb{Q}}(s)L_{\mathbb{Q}}(\chi, s)L_{\mathbb{Q}}(\rho, s)^2.$$

Now we have the restriction homomorphism $\mathfrak{S}_3 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{-23}) : \mathbb{Q}) \simeq C_2$. By the inflation property therefore we have:

$$\zeta_{\mathbb{Q}(\sqrt{-23})}(s) = \zeta_{\mathbb{Q}}(s)L_{\mathbb{Q}}(\chi, s)$$

and

$$\zeta_N(s) = \zeta_{\mathbb{Q}(\sqrt{-23})}L_{\mathbb{Q}}(\rho, s)^2.$$

On the other hand if we denote the two non-trivial characters of $H' = \mathrm{Gal}(N : \mathbb{Q}(\sqrt{-23})) \simeq C_3$ by ψ and $\overline{\psi}$ we get the decomposition:

$$\zeta_N(s) = \zeta_{\mathbb{Q}(\sqrt{-23})}(s)L_{\mathbb{Q}(\sqrt{-23})}(\psi, s)L_{\mathbb{Q}(\sqrt{-23})}(\overline{\psi}, s),$$

and therefore:

$$L_{\mathbb{Q}(\sqrt{-23})}(\psi, s)L_{\mathbb{Q}(\sqrt{-23})}(\overline{\psi}, s) = L_{\mathbb{Q}}(\rho, s)^2 \tag{1.4}$$

Now let us consider the zeta-function $\zeta_K(s)$. By the induction property we have:

$$\zeta_K(s) = L_{\mathbb{Q}}(\mathrm{Ind}_H^G 1, s),$$

where we keep the notation from the above diagram $H = \mathrm{Gal}(N : K)$. Note that $\mathrm{Ind}_H^G 1$ is a three dimensional representation which contains the trivial representation. By comparing the traces of these representations one has $\mathrm{Ind}_H^G 1 \simeq 1 \oplus \rho$. This gives us another relation:

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s)L_{\mathbb{Q}}(\rho, s).$$

Relation 1.4 allows us to find an explicit formula for coefficients of $L_{\mathbb{Q}}(\rho, s)$ via the class field theory. After devoting a bit more efforts one shows that $L_{\mathbb{Q}}(\rho, s)$ is actually the Mellin transform of a modular form of weight one and level 23 with respect to the Legendre character $\left(\frac{\cdot}{23}\right)$. By the explicit computations this modular form is $\eta(\tau)\eta(23\tau)$ where $\eta(\tau) = q^{\frac{1}{24}}\prod_n(1-q^n)$, see [46].

1.6 On Absolute Galois Groups

1.6.1 Around the Neukirch-Uchida Theorem

The above subject concerning arithmetically equivalent number fields has also influenced the study of other invariants attached to a number field K. One remarkable example is the absolute Galois group $\mathcal{G}_K$ of K. Recall that to each field one associates its absolute Galois group $\mathcal{G}_K = \mathrm{Gal}(K^{sep} : K)$, where K^{sep} is the separable closure of K. The absolute Galois group $\mathcal{G}_K$ is not only a group, but also a *pro-finite group*, i.e., $\mathcal{G}_K$ is isomorphic to the inverse limit of an inverse system of discrete finite groups. In particular, $\mathcal{G}_K$ has the so-called *Krull topology* and is a topological group. Under this topology $\mathcal{G}_K$ is a compact, Hausdorff and totally disconnected topological group. The last three properties actually could be taken as a definition of a pro-finite group.

Lemma 1.34. *A topological group G is pro-finite if one of the following equivalent conditions holds:*

1. *G is a compact, Hausdorff and totally disconnected topological group;*
2. *G is isomorphic to a closed subgroup of a product of finite discrete groups*
3. *G is isomorphic to the inverse limit of an inverse system of discrete finite groups.*

Proof. A good reference for the proof and also for general theory of pro-finite groups is [41]. □

For some fields K the group $\mathcal{G}_K$ is easy to describe:

1. If $K = \mathbb{R}$ is a field of real numbers, then $\mathcal{G}_K \simeq \mathbb{Z}/2\mathbb{Z}$;
2. If $K = \mathbb{F}_q$, $q = p^n$ is a finite field, then $\mathcal{G}_K \simeq \widehat{\mathbb{Z}}$.

Here $\widehat{\mathbb{Z}}$ denotes the additive group of pro-finite integers:

$$\widehat{\mathbb{Z}} = \{(a_n) \in \prod_{n=1}^{\infty} (\mathbb{Z}/n\mathbb{Z}) | \forall n, m : n|m \Rightarrow a_m = a_n \mod n\}.$$

The last example illustrates that there are infinitely many non-isomorphic fields sharing isomorphic groups $\mathcal{G}_K$. On the other hand, if we add some additional restrictions on $\mathcal{G}_K$ then it is possible to recover many properties of K. The most classical example is the following result:

Theorem 1.35 (Artin-Schreier)**.** *Suppose $\mathcal{G}_K$ is finite. Then*

1. *$\mathcal{G}_K \simeq \mathbb{Z}/2\mathbb{Z}$;*
2. *K has characteristic zero;*
3. *K is a real closed field, i.e., $K^{sep} = K(i)$, where $i^2 = -1$.*

This Theorem served as motivation for Jurgen Neukirch (24 July 1937 – 5 February 1997) who asked himself the following question: given a number field K what kind of information about K one can recover from $\mathcal{G}_K$ considered as topological group? The following Theorem bearing his name gives a remarkable answer to the Neukirch's problem.

Theorem 1.36 (Neukirch-Uchida)**.** *Suppose K, K' are two number fields such that $\mathcal{G}_K \simeq \mathcal{G}_{K'}$ as topological groups. Then $K \simeq K'$.*

Neukirch gave a proof for the case of normal extensions of $\mathbb{Q}$ in 1969, see [35]. An essential step in his proof is to recover from $\mathcal{G}_K$ the degree of almost all places of K and as suggested by Theorem 1.23 the Dedekind zeta-function $\zeta_K(s)$ of K. Then Uchida extended his results in 1976 to arbitrary number fields, see [56]. The above Theorem is the starting point for the field of *Anabelian Geometry*, a branch of number theory whose main goal is to recover properties of an object X from its fundamental group $\pi(X)$. As we will see soon it turns out that this group must be sufficiently non-abelian in order to recover the isomorphism type; that is why this theory is called anabelian.

1.6.2 On Abelianized Absolute Galois Group

The absolute Galois group $\mathcal{G}_K$ for a number field K is a quite difficult object to study. For instance the Neukirch-Uchida Theorem does not tell us much about the structure of $\mathcal{G}_K$. Another interesting object related to the group $\mathcal{G}_K$ is the so-called abelianized absolute Galois group $\mathcal{G}_K^{ab} = \mathrm{Gal}(K^{ab} : K) = \mathcal{G}_K / \overline{[\mathcal{G}_K, \mathcal{G}_K]}$, where K^{ab} denotes the maximal abelian extension of K and $\overline{[\mathcal{G}_K, \mathcal{G}_K]}$ is the topological closure of the commutator subgroup of $\mathcal{G}_K$. The abelianized absolute Galois group is more suitable for study since global class field theory provides us with a description of $\mathcal{G}_K^{ab}$ in terms of other invariants of the field K, for instance the idele class group. For example, if K is the field of rational numbers $\mathbb{Q}$ then the famous Kronecker-Weber Theorem tells us that any finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension $\mathbb{Q}(\zeta_n)$, where ζ_n denotes the primitive n-th root of unity, and hence $\mathcal{G}_{\mathbb{Q}}^{ab} \simeq \widehat{\mathbb{Z}}^{\times}$ and by rewriting the last group in slightly different terms one has an isomorphism of pro-finite groups:

$$\mathcal{G}_{\mathbb{Q}}^{ab} \simeq \widehat{\mathbb{Z}} \times \prod_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

For number fields different from $\mathbb{Q}$ the description of $\mathcal{G}_K^{ab}$ given via class field theory is not that explicit, but still allows us to study this group. This matter concerning the description of the abelianization $\mathcal{G}_K^{ab}$ of $\mathcal{G}_K$ has attracted much attention since the work [38] where in particular it was shown that there exists an example of imaginary quadratic fields with different class groups and with isomorphic $\mathcal{G}_K^{ab}$. A dramatic improvement was achieved in [1], where the authors produced a lot of new examples of non-isomorphic imaginary quadratic fields which share the same isomorphism type of $\mathcal{G}_K^{ab}$. Moreover, based on their computations they made a conjecture that there are infinitely many imaginary quadratic fields with:

$$\mathcal{G}_K^{ab} \simeq \widehat{\mathbb{Z}}^2 \times \prod_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

They also conjectured that there are infinitely many isomorphism types of pro-finite groups which occur as $\mathcal{G}_K^{ab}$ for some imaginary quadratic field K. We will prove this conjecture in the last chapter of the thesis.

1.7 Results of the Thesis

Now we are able to formulate the main results of the present thesis. But first we will start from one general remark. In the 20th century number theory enlarged its field of interests from number fields to the so-called global function fields. A global function field K is the field of functions of a curve X defined over a finite field $\mathbb{F}_q$. In what follows by a curve we always mean smooth, projective, geometrically connected variety of dimension one. It turns out that global function fields behave in a very similar way to number fields: for every statement in the number field case it is often possible to discover and prove its analogue on the function field side and vice versa. Often this analogue is not unique, but this makes the theory even more attractive. This interaction also provides us with a bridge from number theory to algebraic geometry since the list of main objects of study of algebraic geometry of course includes algebraic curves. For a more algebraic point of view on function fields one could consult [42] and [50]. For a more geometric point of view we recommend [54]. This thesis is devoted to the understanding of possible function field analogues of the topics discussed in the introductory chapter and improvements of the corresponding results in the number field case. The dissertation has five more chapters: three of them are devoted to results on the function field side and two chapters are concerned with results about number fields. Now we briefly explain the motivation and the main results of each chapter.

1.7.1 Chapter Two

In chapter two we keep studying the interaction between group theory and number theory with focus on applications of the subject to the theory of arithmetically equivalent number fields. In particular, we provide a few more explicit instances of pairs of arithmetically equivalent number fields, discuss the notion of arithmetical equivalence for arbitrary extensions of number fields and also formulate and prove Theorem 2.4 of Professor Bart de Smit. In short, the last Theorem states that two isomorphism classes of number fields can be distinguished by the set of Artin L-functions of abelian Galois representations attached to absolute Galois groups of these fields. Finally, we extend Theorem 2.4 and produce an alternative proof of the Uchida's part of the Neukirch-Uchida Theorem. The main results are Theorem 2.8 and Corollary 2.9. This chapter is related to the pre-print [49].

1.7.2 Chapter Three

We started our investigation from the following informal question: what is an analogue of the arithmetical equivalence in the function field side. For a given curve X defined over a finite field $\mathbb{F}_q$, a natural idea is to consider an $\mathbb{F}_q$-rational generically étale morphism from X to $\mathbb{P}^1$. In other words, we are considering finite separable geometric extensions of the field $\mathbb{F}_q(t)$. This allows us to speak about notions of splitting, arithmetical and Gassmann equivalences when the field $\mathbb{Q}$ is replaced by the rational function field $\mathbb{F}_q(t)$. Surprisingly these notions are still equivalent, but one needs to be more careful with equality of zeta-functions. In the function field case there are at least two possible definitions of zeta-function attached to a global function field K. The first approach is more classical Dedekind zeta-function of a complex variable s. Another aproach is more modern and uses the theory of so-called Goss zeta-functions whose

definition is slightly far from the scope of this thesis, but an interested reader could consult [20]. The last approach was extensively studied in [8]. In our research we prefer to stand on the approach which uses more classical Dedekind-zeta functions: we extend results from Nagata [32] on arithmetically equivalent function fields which allow us to prove an analogue of Theorem 2.5 discussed in section 2.3 of the current chapter for extensions of $\mathbb{F}_q(t)$. Also we provide:

1. Examples of arithmetically equivalent, but not isomorphic function fields;
2. An algorithm to construct many new pairs of arithmetically equivalent function fields by using torsion points of elliptic curves defined over $\mathbb{F}_q(t)$;
3. A discussion on some properties of arithmetically equivalent function fields.

This chapter is based on the pre-print [48].

1.7.3 Chapter Four

In the third chapter of the thesis we develop a different approach to the generalisations of Theorem 2.4 to the function field side. Given a curve X over a finite field $\mathbb{F}_q$ we consider the set of zeta-functions of abelian coverings of X of degree prime to the characteristic p of the constant field. The motivation for this is the following. First, the map from the curve X to $\mathbb{P}^1$ in the previous chapter plays a crucial role in the whole story, but is absolutely non-canonical. In order to make it more canonical, one could ask what kind of information about X it is possible to obtain from zeta-functions of coverings of X. In general this set is quite difficult to study, but if one restricts attention to abelian Galois coverings then it is possible to construct and study such sets by using class field theory for function fields. Note that from the Dedekind zeta-function of a curve C one could recover its genus $g(C)$. Therefore it is convenient to consider the list $\lambda_X(g)$ of zeta-functions of abelian coverings of X of a given genus g. Since there are only finitely many curves of a given genus defined over a given finite field this list is finite. In our research we obtain a complete description for such a list when $X = E$ is an elliptic curve and the genus of the cover is two[2]. The main result of this chapter states that if $j(E) \neq 0$, 1728 then this list depends only on the number of $\mathbb{F}_q$-rational 2-torsion points of E. We also provide an explicit description of such a list and discuss the cases with $j(E) = 0$, 1728. This chapter relies on pre-print [47].

1.7.4 Chapter Five

In this chapter we change our focus towards the problem about the structure of the abelianization of absolute Galois groups of global function fields. In 1977 Uchida [57] also published an article concerning a function field analogue of the Neukirch-Uchida Theorem discussed above. This Theorem states that the geometric isomorphism class of the curve X is determined by the isomorphism class of the absolute Galois group $\mathcal{G}_K = \mathrm{Gal}(K^{sep} : K)$ considered also as topological group. As in the number field case the following problems are natural to ask: what kind of information one could recover from the isomorphism class of the abelianization $\mathcal{G}_K^{ab}$ of

[2] under the assumption that the characteristic of the constant field is different from two and three.

$\mathcal{G}_K$? More concretely, does the maximal abelian quotient of the absolute Galois group determine the global function field K up to isomorphism? If not, which function fields share the same isomorphism class of $\mathcal{G}_K^{ab}$ for some fixed isomorphism class of $\mathcal{G}_K^{ab}$? In this chapter we provide a complete answer. Given a global function field K we associate to it three invariants: characteristic p of the constant field $\mathbb{F}_q$ of K, the non-p part d_K of $\log_p(q)$ and the non-p part of the class group of K, see the introduction of the chapter four for exact definitions. Then our main result in this section is the following:

Theorem 1.37. *Given two global function fields K and K', the pro-finite groups $\mathcal{G}_K^{ab}$ and $\mathcal{G}_{K'}^{ab}$ are isomorphic if and only if the three invariants introduced above coincide for K and K'.*

This chapter also includes the following results and corollaries:

1. Given the isomorphism type of $\mathcal{G}_K^{ab}$ we explain how to recover these three invariants in a group-theoretical way;
2. Given these three invariants of a global function field K we reconstruct the isomorphism type of $\mathcal{G}_K^{ab}$;
3. There are infinitely many pairwise non isomorphic global function fields with isomorphic $\mathcal{G}_K^{ab}$;
4. There are infinitely many isomorphism types of pro-finite groups which occur as $\mathcal{G}_K^{ab}$ for some function field K.

This chapter comes from the pre-print [11].

1.7.5 Chapter Six

In the final chapter we use our result from previous chapter to improve results of [1] on isomorphism types of abelianized absolute Galois groups of imaginary quadratic fields. In particular we prove that there are infinitely many isomorphism types of pro-finite groups which occur as $\mathcal{G}_K^{ab}$ and also we construct many new examples of imaginary quadratic fields sharing the same isomorphism type of $\mathcal{G}_K^{ab}$. This chapter is related to the pre-print [12].

Chapter 2

Some Remarks With Regard to the Arithmetical Equivalence and Fields Sharing Same L-functions

2.1 Introduction

Having stated basic features of Artin L-functions we will show how to use them to elaborate studies of arithmetically equivalent number fields. There are three related topics we are going to consider in this chapter:

1. The first topic concerns the discussion about the property 4 of Artin L-functions which we called *multiplicative independence over* $\mathbb{Q}$ and analogues of Theorem 1.23 where the field $\mathbb{Q}$ is replaced by an arbitrary number field. Among others this problem was extensively studied by Nagata whose result we will describe in Theorem 2.1 and generalise later to the function field case, see Theorems 3.1 and 3.2 in the next chapter of the thesis.

2. The second part is related to the reconstruction of the isomorphism class of a given number field K by Artin L-functions of different representations attached to Galois extensions of K. The main result of that topic is Theorem 2.4 of Bart de Smit which states that for every number field K there exists an L-function which occurs only for that field. This result will also be generalised later in Theorem 3.3 to the function field side.

3. In the final section of this chapter we consider some extension of Theorem 2.4 as well as its applications towards a proof of the Uchida's part of the Neukirch-Uchida Theorem. The main results are Theorem 2.8 and Corollary 2.9.

2.2 Non-arithmetically equivalent extensions of Number Fields

2.2.1 Nagata's approach

As before let K and K' be two number fields. Let N denote their common Galois closure over $\mathbb{Q}$ and let $G = \mathrm{Gal}(N : \mathbb{Q})$, $H = \mathrm{Gal}(N : K)$, $H' = \mathrm{Gal}(N : K')$. Recall that in notations of Theorem 1.23 by the induction property we have:

$$\zeta_K(s) = L_{\mathbb{Q}}(\mathrm{Ind}_H^G(1_H), s),$$

and therefore by the multiplicative independence of Artin L-functions over $\mathbb{Q}$ we obtain:

$$\zeta_K(s) = \zeta_{K'}(s) \text{ if and only if } \mathrm{Ind}_H^G(1_H) \simeq \mathrm{Ind}_{H'}^G(1_{H'}).$$

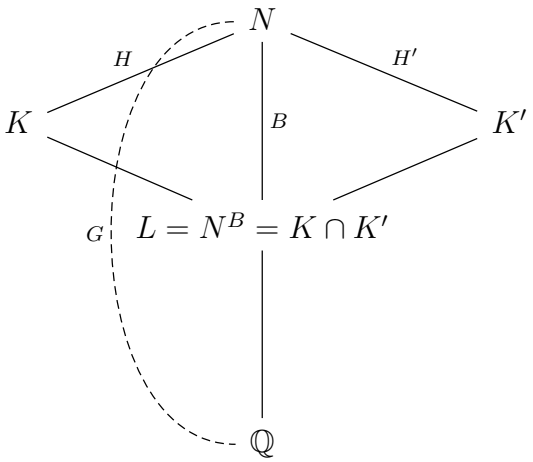
Phrasing this in a different way we regard the trivial representation 1 of the group G and restrict it to subgroups H and H'. Considering two L-functions $L_K(1|_H, s)$ and $L_{K'}(1|_{H'}, s)$ we have: K and K' are arithmetically equivalent if and only if these two L-functions match. There are at least two important questions a reader could ask here. The first one is: what if we pick another irreducible representation ρ of G and consider its restrictions to H and H' and compare the corresponding L-functions? And the second question is: what if we replace the base field $\mathbb{Q}$ with another number field such that multiplicative independence does not hold? how can we detect arithmetical equivalence over that field?

Surprisingly, by using elementary properties of representations of finite groups and properties of Artin L-functions we have discussed above, it is possible to show that the answer to both problems stated above is given by the following result due to K. Nagata, who published [32] in 1986:

Theorem 2.1 (Nagata)**.** *Let K and K' be two finite extensions of a fixed number field L. Let N denote their common Galois closure over L and let $G = \mathrm{Gal}(N : L)$, $H = \mathrm{Gal}(N : K)$, $H' = \mathrm{Gal}(N : K')$. Then K and K' are arithmetically equivalent over L if and only if for every irreducible representation ρ of G we have: $L_K(\rho|_H, s) = L_{K'}(\rho|_{H'}, s)$.*

Proof. See Theorem 3.1 from the next chapter. □

Let us consider a particular instance which explains this lemma. Namely, we focus our attention on Example 1.15 from the introduction. There we picked a Gassmann triple (G, H, H') with G isomorphic to $\mathrm{Gl}_2(\mathbb{F}_p)$. It is easy to see that actually H and H' are subgroups of the proper Borel subgroup $B = \left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \in G \right\}$ of G and hence one can consider a triple of finite groups (B, H, H') and ask whether this triple is Gassmann or not. By the evaluation of permutation characters one has $\mathrm{Ind}_H^B(1_H) \not\simeq \mathrm{Ind}_{H'}^B(1_{H'})$, which means that (B, H, H') is not a Gassmann triple. Keeping notations of Theorem 1.23 we obtain equality of zeta-functions $\zeta_K(s) = \zeta_{K'}(s)$ and the following Galois correspondence diagram:



(2.1)

In order to see Lemma 2.1 in action we pick $p = 3$, in that case G has order $(p^2-1)(p^2-p) = 48$, B has order $(p-1)^2p = 12$ and index 4 in G and both $(H,\, H')$ have index $p-1 = 2$ in B. It follows that H and H' are normal subgroups and that there is a non-trivial abelian character χ of B which factors as a non-trivial character through the quotient B/H', i.e. a character with $\ker(\chi) = H$. Then $\chi_{|H} = 1_{|_H}$ and therefore $L_K(\chi_{|H}) = \zeta_K(s)$, meanwhile $L_{K'}(\chi_{|_{H'}})$ is an L-function of a non-trivial abelian character of H' and therefore it has no poles as $s \to 1$, which implies that $L_K(\chi_{|H}) \neq L_{K'}(\chi_{|_{H'}})$.

Magma scripts

As before we add a Magma script to verify the examples we discussed above. We split the script into two parts. The first part is a group-theoretical verification:

```
p := 3; k := GF(p);
G := GL(2,k);
TheBorelGroup := Subgroups(G: OrderEqual := 12)[1]‘subgroup;
TheBorelSubgroups := Subgroups(TheBorelGroup: IndexEqual := 2);
for H in TheBorelSubgroups do
  "Permutation Character:", PermutationCharacter(TheBorelGroup, H‘subgroup);
end for;
```

This script produces the following output, which shows that indeed the corresponding permutation representations are not isomorphic:

```
Permutation Character: ( 2, 0, 2, 0, 2, 0 )
Permutation Character: ( 2, 0, 0, 2, 2, 0 )
Permutation Character: ( 2, 2, 0, 0, 2, 2 )
```

In the second part we construct explicitly number fields K, K', L which fit to the diagram (2.1). We are doing this by using torsion points on elliptic curves, similar to the method introduced in [9]. Recall the following main steps of the algorithm:

1. Pick a general elliptic curve E over $\mathbb{Q}$. We denote by $g(x, y)$ the polynomial y^2-x^3-ax-b which defines E;

2. Find a polynomial $f(x)$ with roots corresponding to the x-coordinates of the 3-torsion points $E[3]$ of E, i.e. a 3-division polynomial of E;
3. Evaluate resultant $z(x)$ of f and g with respect to x;
4. Finally, compute the Galois closure N of the number field defined by $z(x)$.

According to Serre's open image theorem for a general elliptic curve E we have:

$$\mathrm{Gal}(N, \mathbb{Q}) \simeq \mathrm{Gl}_2(\mathbb{F}_p).$$

Here is an implementation of this algorithm:

```
// Steps 1, 2 and 3
a := 1; b := 1;
E := EllipticCurve([a, b]);
K := Rationals();
R<x,y> := PolynomialRing(K,2);
g<x,y> := y^2-x^3-a*x-b;
f := DivisionPolynomial(E, 3);
ResultantOfFandG := Resultant(Evaluate(f, x), g, x);

// Mapping the resultant of f and g to the polynomial ring of one variable
S<z> := PolynomialRing(Rationals());
HomRtoS := hom<R -> S | 0, z>;
h := HomRtoS(ResultantOfFandG);

// The final step: producing explicit equations
FF := NumberField(h);
G, r, N := GaloisGroup(FF) ;
TheBorelGroup := Subgroups(G: IndexEqual := 4)[1]`subgroup;
TheBorelSubgroups := Subgroups(G: IndexEqual := 8);
B<x> := GaloisSubgroup(N, TheBorelGroup);
B;
for H in TheBorelSubgroups do
  GaloisSubgroup(N, H`subgroup);
end for;
```

The output of this script is:

```
x^4 - 11648*x^3 + 43792584*x^2 + 350900032*x - 160837688676272
x^8 + 351459648*x^6 + 25734142535892480*x^4 + 4959894048812650728161 28*x^2 +
    662246092057630641285070 1205504
((x1 - x5) * ((x2 + (x3 + x4)) - (x6 + (x7 + x8))))
x^8 + 5832*x^6 + 10983114*x^4 - 10052399428083
x1
x^8 + 17496*x^6 - 62710038*x^4 + 6198727824*x^2 - 10052399428083
(x2 + (x3 + x4))
```

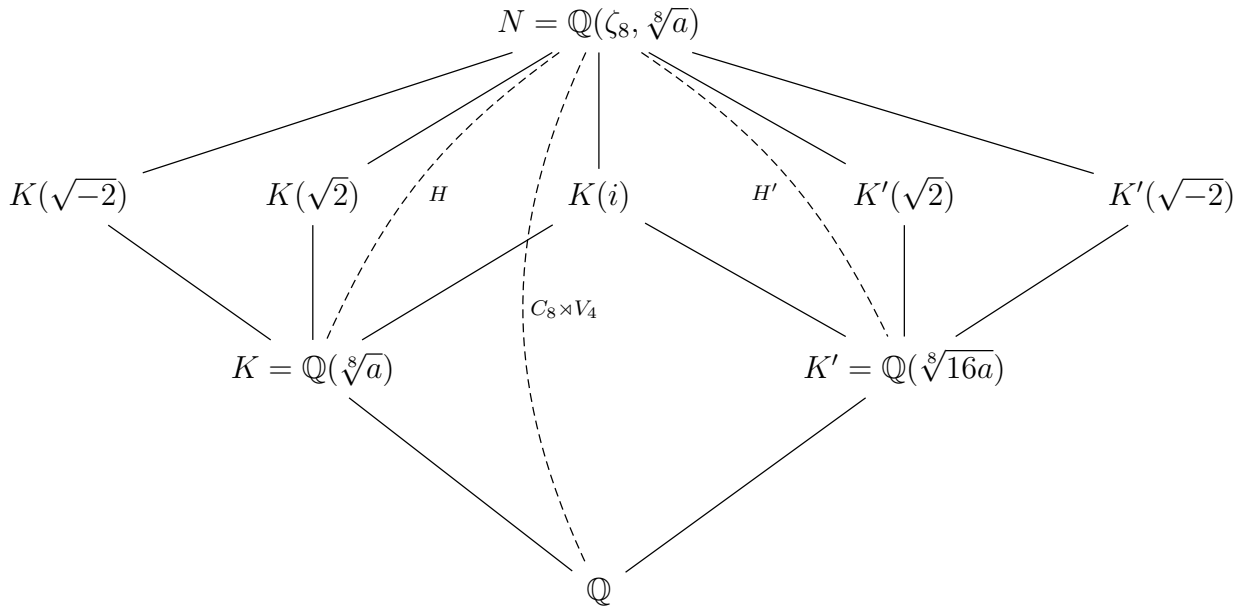
This shows that the number field $L = N^B$ can be defined for instance by the polynomial:

$$x^4 - 11648x^3 + 43792584x^2 + 350900032x - 160837688676272.$$

2.2.2 Yet another example

Slightly generalising Nagata's approach mentioned earlier we could ask: *does there exist a representation χ of H such that for every representation χ' of H' we have $L_K(\chi, s) \neq L_{K'}(\chi', s)$?* Of course if χ is the restriction of a representation ρ of G then the above discussion shows it is not possible to find such a χ, but what if we pick χ which is not the restriction of any representation ρ of G or there are examples where it is not possible to pick such a character? It turns out that if we look thoroughly at fields from example 1.28 then we find out that the answer to the later question is negative: there is an example of a pair (K, K') of non-isomorphic number fields with the following remarkable property. Denoting by N the common normal closure of K and K' there exists a bijection ϕ between the set X of characters of $\mathrm{Gal}(N : K)$ and the set X' of characters of $\mathrm{Gal}(N : K')$ such that for every $\chi \in X$ we have $L_K(\chi, s) = L_{K'}(\phi(\chi), s)$.

Let us consider the example 1.28 more carefully. The normal closure N of $K = \mathbb{Q}(\sqrt[8]{a})$ is $K(\zeta_8)$, where ζ_8 denotes a primitive eighth root of unity. Note that $K(i) = K'(i)$, where $K' = \mathbb{Q}(\sqrt[8]{16a})$. We have $H \simeq H' \simeq V_4$ and the following Galois correspondence diagram:



Lemma 2.2. *There exists a bijection ϕ between characters of H to those of H' such that for every character χ of H holds $L_K(\chi, s) = L_{K'}(\phi(\chi), s)$.*

Proof. This claim is easy to establish from the following observation. First we observe that $\zeta_{K(\sqrt{2})}(s) = \zeta_{K'(\sqrt{2})}(s)$ and $\zeta_{K(\sqrt{-2})}(s) = \zeta_{K'(\sqrt{-2})}(s)$. Indeed, $\zeta_K(s) = \zeta_{K'}(s)$ and $\sqrt{2}$ belongs neither to K nor K', which implies that $K(\sqrt{2})$, $K'(\sqrt{2})$ are arithmetically equivalent and also $K(\sqrt{-2})$, $K'(\sqrt{-2})$. The same argument shows $K(\sqrt{-2})$, $K'(\sqrt{-2})$ are arithmetically equivalent. The group H has three non-trivial characters χ_1, χ_2 and $\chi_1\chi_2$ and up to numeration we have:

$$L_K(\chi_1, s) = \frac{\zeta_{K(\sqrt{2})}(s)}{\zeta_K(s)}, \quad L_K(\chi_2, s) = \frac{\zeta_{K(\sqrt{-2})}(s)}{\zeta_K(s)}, \quad L_K(\chi_1\chi_2, s) = \frac{\zeta_{K(i)}(s)}{\zeta_K(s)}.$$

Replacing K by K' and χ_i by χ_i' we establish the desired bijection. □

Remark 2.3. *Using the above argument for a given pair of arithmetically equivalent number fields K, K' one can construct more examples of pairs of quadratic characters $\chi : \mathcal{G}_K \to \mathbb{C}$, $\chi' : \mathcal{G}_{K'} \to \mathbb{C}$ such that $L_K(\chi, s) = L_{K'}(\chi', s)$. Namely, for a rational prime number p such that $\sqrt{p} \notin K$, K' the number fields $M = K(\sqrt{p})$, $M' = K'(\sqrt{p})$ are also arithmetically equivalent and therefore: $L_K(\chi, s) = \frac{\zeta_M(s)}{\zeta_K(s)} = \frac{\zeta_{M'}(s)}{\zeta_{K'}(s)} = L_{K'}(\chi', s)$, where χ(resp. χ') is the unique non-trivial character of* $\mathrm{Gal}(M : K)$ *(resp.* $\mathrm{Gal}(M' : K')$*).*

2.3 Identifying Number Fields with Artin L-functions

Now it is reasonable to ask the following: could we somehow detect the isomorphism class of a number field K by using Artin L-functions of Galois representations associated to the Galois groups of normal extensions of K? The answer is yes and it is given by Theorem 2.4:

Theorem 2.4. *For each number field K there exists an abelian extension N_K of degree three and a character χ of* $\mathrm{Gal}(N_K : K)$ *such that $L_K(\chi, s)$ occurs only for the isomorphism class of the field K, i.e. if for any other number field K' and any abelian extension $N_{K'}$ of K' there exists a character χ' of* $\mathrm{Gal}(N_{K'} : K')$ *such that $L_K(\chi, s) = L_{K'}(\chi', s)$ then $K \simeq K'$.*

We begin with providing a sketch for the proof of a slightly different version of Theorem 2.4. After that we explain how the statement of Theorem 2.4 follows from what we have discussed.

2.3.1 The First Version of Theorem

We first discuss a proof of another version of Theorem 2.4:

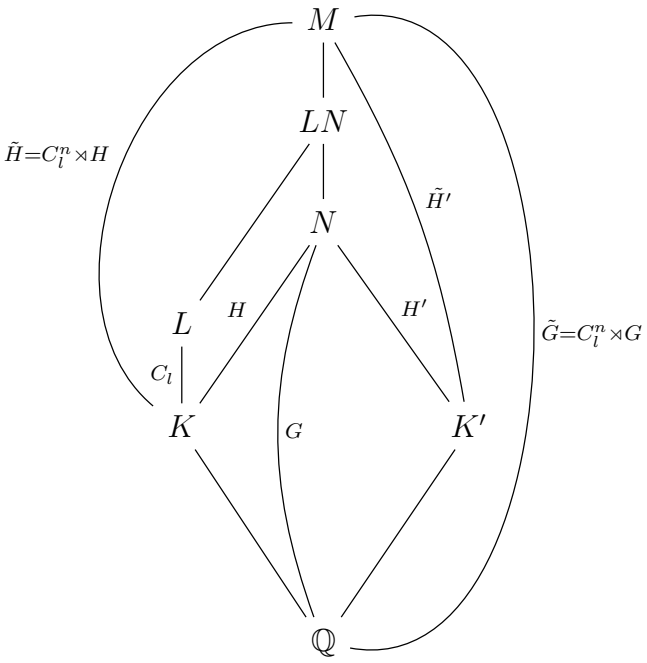
Theorem 2.5. *For every pair of non-isomorphic number fields K, K' with $\zeta_K(s) = \zeta_{K'}(s)$ we may attach a Galois extension M over $\mathbb{Q}$ with the Galois group $\tilde{G}$ which contains both K and K' with $K = M^{\tilde{H}}$, $K' = M^{\tilde{H}'}$ for some subgroups $\tilde{H}$, $\tilde{H}'$ of G and an abelian character χ of $\tilde{H}$ such that for any abelian character χ' of $\tilde{H}'$ we have $L_K(\chi, s) \neq L_{K'}(\chi', s)$. In other words $L_K(\chi, s)$ as an analytic function occurs only for K, but not for K'.*

This goal is achieved in two steps. First we need the following group-theoretical result. Let G be a finite group, H a subgroup of index n, and $C_l = \mu_l \subset \mathbb{C}^\times$ be a cyclic group of order l, where l *is an odd prime*. Consider a G-set G/H of left cosets. We fix some representatives $X_1, \dots X_n$ of G/H such that X_1 is a coset corresponding to the group H. Let us regard semi-direct products $\tilde{G} = C_l^n \rtimes G$ and $\tilde{H} = C_l^n \rtimes H$, where G acts on the components of C_l^n by permuting them as the cosets $\{X_1, \dots, X_n\}$. Let χ be the homomorphism from $\tilde{H}$ to the group C_l defined on the element $\tilde{h} = (\zeta_1, \dots, \zeta_n, h) \in \tilde{H} = C_l^n \rtimes H$ as $\chi(\tilde{h}) = \zeta_1$ i.e. χ is the *projection to the first coordinate*. This is indeed a homomorphism because every $h \in H$ fixes the first coset of G/H. In this setting the following holds:

Theorem 2.6 (Bart de Smit)**.** *For any subgroup $\tilde{H}' \subset \tilde{G}$ and any character $\chi' : \tilde{H}' \to \mathbb{C}^*$ if $\mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi') \simeq \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$ then $\tilde{H}'$ and $\tilde{H}$ are conjugate in $\tilde{G}$.*

Proof. See section 3.4 from the next chapter. □

Next suppose K is a number field such that $\zeta_K(s)$ does not determine K i.e. there exists a number field K' such that $\zeta_K(s) = \zeta_{K'}(s)$, but $K \not\simeq K'$. Then as before this means the normal closure N of K contains K' and there exists a non-trivial Gassmann triple (G, H, H') with $G = \mathrm{Gal}(N/\mathbb{Q})$, $H = \mathrm{Gal}(N/K)$, $H' = \mathrm{Gal}(N/L)$. In this setting we construct a Galois extension M of $\mathbb{Q}$ containing K and K' such that the Galois group $\mathrm{Gal}(M : \mathbb{Q})$ is $\tilde{G}$ and $K = M^{\tilde{H}}$, $K' = M^{\tilde{H}'}$ for $\tilde{G}$, $\tilde{H}$, $\tilde{H}'$ as in Theorem 2.6. This is possible due to Proposition 9.1 from [13]. See the diagram below:



Now consider the abelian character χ of $\tilde{H}$ as in the statement of Theorem 2.6. Suppose χ' is any abelian character of $\tilde{H}' = \mathrm{Gal}(M : K')$. We have:

$$L_K(\chi, s) = L_{K'}(\chi', s) \Rightarrow K \simeq K'.$$

Indeed, by the induction property we have:

$$L_K(\chi, s) = L_{\mathbb{Q}}(\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi), s).$$

Therefore:

$$L_K(\chi, s) = L_K(\chi', s) \Leftrightarrow L_{\mathbb{Q}}(\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi), s) = L_{\mathbb{Q}}(\mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi'), s) \Leftrightarrow \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi) \simeq \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi'),$$

and by Theorem 2.6 we have that $\tilde{H}$ and $\tilde{H}'$ are conjugate and hence K is isomorphic to K'.

2.3.2 Deducing Theorem 2.4 from Theorem 2.5

Now our goal is to deduce Theorem 2.4 from Theorem 2.5. First we note that denoting by ψ the restriction of χ to the Galois group $\mathrm{Gal}(L:K) = C_l$ we obtain a non-trivial one-dimensional character of C_l. By the inflation property we have $L_K(\chi, s) = L_K(\psi, s)$, where the latter L-function is an abelian L-function of the abelian extension L over K.

In the same setting as before suppose that there exist an abelian extension $N_{K'}$ of K' and a character ψ' of $\mathrm{Gal}(N_{K'} : K')$ such that $L_K(\psi, s) = L_{K'}(\psi', s)$. We would like to show that there exists an abelian character χ' of $\tilde{H}' = \mathrm{Gal}(M : K')$ such that $L_{K'}(\chi', s) = L_K(\psi', s)$ and therefore we can apply Theorem 2.5. In other words we would like to show that the character ψ' can be treated as an abelian character χ' of $\tilde{H}'$ in the setting of Theorem 2.5.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and denote the absolute Galois group of fields K, K', $\mathbb{Q}$ by $\mathcal{G}_K$, $\mathcal{G}_{K'}$ and $\mathcal{G}_{\mathbb{Q}}$ respectively. We consider ψ as a character of $\mathcal{G}_K$ via the projection $\mathcal{G}_K \to \tilde{H}$. In a similar way ψ' is a character of $\mathcal{G}_{K'}$. By the induction property we have:

$$L_K(\psi, s) = L_{\mathbb{Q}}(\mathrm{Ind}_{\mathcal{G}_K}^{\mathcal{G}_{\mathbb{Q}}} \psi, s),$$

and

$$L_{K'}(\psi', s) = L_{\mathbb{Q}}(\mathrm{Ind}_{\mathcal{G}_{K'}}^{\mathcal{G}_{\mathbb{Q}}} \psi', s).$$

Since by our assumptions $L_K(\psi, s) = L_{K'}(\psi', s)$ we have:

$$\mathrm{Ind}_{\mathcal{G}_K}^{\mathcal{G}_{\mathbb{Q}}} \psi \simeq \mathrm{Ind}_{\mathcal{G}_{K'}}^{\mathcal{G}_{\mathbb{Q}}} \psi'.$$

But then kernels of these representations of $\mathcal{G}$ must coincide. Since M is the fixed field of the action of $\ker(\mathrm{Ind}_{\mathcal{G}_K}^{\mathcal{G}_{\mathbb{Q}}} \psi)$ on $\overline{\mathbb{Q}}$ we have that M is also the fixed field of the action of $\ker(\mathrm{Ind}_{\mathcal{G}_{K'}}^{\mathcal{G}_{\mathbb{Q}}} \psi')$ on $\overline{\mathbb{Q}}$. This means that the extension $N_{K'}$ can be embedded into the field M and the character ψ' is an abelian character of $\tilde{H}'$.

2.4 Neukirch-Uchida Theorem

Recall from the first chapter that the famous Neukirch-Uchida theorem states that:

Theorem 2.7. *For given number fields K, K' the existence of a topological isomorphism of profinite groups $\mathcal{G}_K \simeq \mathcal{G}_{K'}$ implies the existence of an isomorphism of fields $K \simeq K'$ themselves.*

The story behind this result is the following. In 1969 Neukirch [34] gave a proof for the case of normal extensions of $\mathbb{Q}$. He proved this by recovering Dedekind zeta-function $\zeta_K(s)$ of K from $\mathcal{G}_K$ in group-theoretical terms and then applying Theorem 1.23 to show that in this case $\zeta_K(s)$ determines the isomorphism class of K. A few years later in 1976 Uchida [56] extended Neukirch's results to the case of arbitrary number fields. Uchida's approach was then also used by himself and others to generalise the Theorem to the case of all global fields. For a modern exposition, see Chapter XII in [37]. Without any doubt Uchida's proof is beautiful and important, but it contains some difficult technical details which make this proof a bit less clear especially for those who are relatively new to the topic. The goal of the present section is to provide an alternative, in some sense more elementary approach to the proof of Uchida's

part. The new proof also has another advantage, since it stays closer to Neukirch's original idea. This new approach is based on the following idea.

Given a number field K we associate to it a set Λ_K of Dedekind zeta-functions of finite abelian extensions of K:

$$\Lambda_K = \{\zeta_L(s) \mid L \text{ is a finite abelian extension of } K\}.$$

Our main goal is to prove the following Theorem:

Theorem 2.8. *For every number field K the set Λ_K determines the isomorphism class of K. This means that if for any other number field K' the two sets Λ_K and $\Lambda_{K'}$ coincide, then $K \simeq K'$.*

The following observation shows that Theorem 2.8 allows us to achieve our goal and produce an alternative way to Uchida's part:

Corollary 2.9. *In the above setting suppose that $\mathcal{G}_K \simeq \mathcal{G}_{K'}$. Then $\Lambda_K = \Lambda_{K'}$ and therefore $K \simeq K'$.*

Proof. Indeed, given an isomorphism class of $\mathcal{G}_K$ we consider all closed subgroups of finite index $H \subset \mathcal{G}_K$ such that the quotient $\mathcal{G}_K/H$ is a finite abelian group. By pro-finite Galois theory we have one-to-one correspondence between such H and finite abelian extensions L of K within a fixed algebraic closure $\overline{K}$ given by $H \to (\overline{K})^H$. Now by using Neukirch's Theorem (see chapter 4 in [34]) we reconstruct $\zeta_L(s)$ in a group theoretical manner from H and therefore reconstruct Λ_K from $\mathcal{G}_K$. □

From now on we concentrate our attention on the proof of 2.8.

On the Proof of Theorem 2.8

To deduce Theorem 2.8 we extend Theorem 2.4 by replacing the L-function of the abelian character χ by the Dedekind ζ-function of the abelian extension N_K of K:

Theorem 2.10. *For each number field K there exists an abelian extension N_K of degree three such that the pair $\zeta_{N_K}(s)$, $\zeta_K(s)$ occurs only for the isomorphism class of the field K, i.e. if for any other number field K' and any abelian extension $N_{K'}$ of K' we have $\zeta_K(s) = \zeta_{K'}(s)$ and $\zeta_{N_K}(s) = \zeta_{N'_{K'}}(s)$ then $K \simeq K'$.*

Remark 2.11. *Note that the degree of a number field K is determined by $\zeta_K(s)$. Therefore, $\zeta_K(s)$ can be recovered from $\Lambda(K)$ as unique element whose corresponding field has minimal degree.*

The above remark shows that Theorem 2.8 and Theorem 2.10 are equivalent and we can focus on proving the last statement.

2.4.1 The proof

First we fix $l = 3$ and prove the following auxiliary statement:

Lemma 2.12. *In the setting of Theorem 2.6 the induced representation* $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$ *is an irreducible representation of* $\tilde{G}$.

Proof. In order to verify irreducibility of $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$ we regard the standard scalar product and show that $(\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi), \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi))_{\tilde{G}} = 1$. Applying Frobenius reciprocity:

$$(\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi), \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi))_{\tilde{G}} = (\chi, \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)|_{\tilde{H}})_{\tilde{H}} = \frac{1}{|\tilde{H}|}\sum_{\tilde{h}\in\tilde{H}} \bar{\chi}(\tilde{h}) \cdot \mathrm{Tr}(\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)|_{\tilde{H}}(\tilde{h})). \tag{2.2}$$

Let $\tilde{h} = (\zeta_1, \dots, \zeta_n, h) \in \tilde{H}$. Then by definition of χ we have $\bar{\chi}(\tilde{h}) = \bar{\zeta_1}$. Now consider the matrix $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)|_{\tilde{H}}(\tilde{h})$. We fix the following representatives for cosets of $\tilde{G}/\tilde{H}$ as $\tilde{X}_i = (1, \dots, 1, X_i) \in \tilde{G}$, where X_i are the representatives of cosets of G/H we picked before. By definition of the induced representation and because h fixes first conjugacy class of G/H we have that in the top left corner of that matrix ζ_1 is located. Now we fix an integer $1 < i \leq n$ and consider the diagonal element $a_i(\tilde{h})$ in the (i,i)-th position. Consider the permutation of cosets $\tilde{X}_1, \dots \tilde{X}_n$ by $\tilde{h}$ and denote by j an index such that $\tilde{h}\tilde{X}_i = \tilde{X}_j$. If $i \neq j$ then $a_i(\tilde{h}) = 0$ and therefore such i adds no contribution to the expression (2.2). Otherwise, by definition of the induced representation $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)|_{\tilde{H}}$ we have $a_i(\tilde{h}) = \chi(\tilde{X}_i^{-1}\tilde{h}\tilde{X}_i) = \zeta_{k_i}$ for some index $k_i \in \{2, \dots, n\}$. In other words, k_i is an index such that $X_i^{-1}X_{k_i} \in H$. For fixed $\tilde{h}$ and i there are elements $\tilde{h}_1$, $\tilde{h}_2$ such that $(\tilde{h}, \tilde{h}_1, \tilde{h}_2)$ pairwise coincide in all coordinates except the k_i-th one. Because $1 + \zeta_{k_i} + \bar{\zeta}_{k_i} = 0$ we have that sum of $a_i(\tilde{h})$ for those $\tilde{h}$, $\tilde{h}_1$, $\tilde{h}_2$ is zero and because they coincide on first coordinate we have $\chi(\tilde{h}) = \chi(\tilde{h}_j)$ for j in $\{1, 2\}$. Therefore for fixed $i > 1$ we have:

$$\sum_{\tilde{h}\in\tilde{H}} \bar{\chi}(\tilde{h}) a_i(\tilde{h}) = 0.$$

Now we consider the expression (2.2):

$$\begin{aligned}
\frac{1}{|\tilde{H}|}\sum_{\tilde{h}\in\tilde{H}} \bar{\chi}(\tilde{h}) \cdot \mathrm{Tr}(\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)|_{\tilde{H}}(\tilde{h})) &= \frac{1}{|\tilde{H}|}\sum_{\tilde{h}\in\tilde{H}} \bar{\chi}(\tilde{h}) \cdot (\chi(\tilde{h}) + \sum_{i>1}^{i\leq n} a_i(\tilde{h})) = \\
&= \frac{1}{|\tilde{H}|}\sum_{\tilde{h}\in\tilde{H}} \bar{\chi}(\tilde{h})\chi(\tilde{h}) + \frac{1}{|\tilde{H}|}\sum_{\tilde{h}\in\tilde{H}} (\bar{\chi}(\tilde{h}) \cdot (\sum_{i>1}^{i\leq n} a_i(\tilde{h}))) = \\
&= \frac{1}{|\tilde{H}|}\sum_{\tilde{h}\in\tilde{H}} 1 + \frac{1}{|\tilde{H}|}\sum_{i>1}(\sum_{\tilde{h}\in\tilde{H}} \bar{\chi}(\tilde{h}) a_i(\tilde{h})) = 1 + 0.
\end{aligned}$$

□

By using this lemma we can prove the main group theoretical result of this note:

Theorem 2.13. *In the above setting let* $U_{\tilde{H},\chi} = \ker(\chi) = \{h \in \tilde{H} | \chi(h) = 1\}$ *and let* $U_{\tilde{H}',\chi'} = \ker(\chi')$. *Suppose that* $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(1) \simeq \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(1)$ *and* $\mathrm{Ind}_{U_{\tilde{H},\chi}}^{\tilde{G}}(1) \simeq \mathrm{Ind}_{U_{\tilde{H}',\chi'}}^{\tilde{G}}(1)$. *Then either* $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi) \simeq \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi')$ *or* $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi) \simeq \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\bar{\chi}')$.

Proof. Since $l = 3$ we have that C_l has only three characters $1, \chi, \bar{\chi}$ and therefore:

$$\mathrm{Ind}_{U_{\tilde{H},\chi}}^{\tilde{G}}(1) \simeq \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi) \oplus \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\bar{\chi}) \oplus \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(1).$$

Hence, from the assumption of the Theorem it follows that:

$$\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi) \oplus \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\bar{\chi}) \simeq \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi') \oplus \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\bar{\chi}').$$

In Lemma 2.12 we showed that $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$, $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\bar{\chi})$ are *irreducible representations* of $\tilde{G}$. But if a direct sum of two irreducible representations of a finite group is isomorphic to a direct sum of two other *non-zero representations* then those representations are pairwise isomorphic up to a permutation. It follows that either $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi) \simeq \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi')$ or $\mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi) \simeq \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\bar{\chi}')$. □

Finally, we can provide:

Proof of Theorem 2.10. Suppose K is a number field such that $\zeta_K(s)$ does not determine K i.e. there exists a number field K' such that $\zeta_K(s) = \zeta_{K'}(s)$, but $K \ncong K'$. Then as before we construct a Galois extension M of $\mathbb{Q}$ as in Theorem 2.4, see figure 2.3.1. Let L' be *any abelian extension* of K' such that $\zeta_{L'} = \zeta_L$. Then L and L' share the same normal closure over $\mathbb{Q}$ and therefore L' is a subfield of M. According to remark 2.11 we also have that the degree of L' over K' is three. Observe that in notations of Theorem 2.13 from the previous section one has: $\mathrm{Gal}(M : L) = \ker(\chi) = U_{\tilde{H},\chi}$ for a non-trivial character χ of $\mathrm{Gal}(L : K)$ and $\mathrm{Gal}(M : L') = \ker(\chi')$ for a non-trivial character χ' of $\mathrm{Gal}(L' : K')$. By the induction property of Artin L-functions we have: $\zeta_L(s) = L_{\mathbb{Q}}(\mathrm{Ind}_{U_{\tilde{H},\chi}}^{\tilde{G}}(1), s)$.

Finally, because of multiplicative independence of L-functions over $\mathbb{Q}$ we have:

$$L_{\mathbb{Q}}(\mathrm{Ind}_{U_{\tilde{H},\chi}}^{\tilde{G}}(1), s) = L_{\mathbb{Q}}(\mathrm{Ind}_{U_{\tilde{H}',\chi'}}^{\tilde{G}}(1), s) \Leftrightarrow \mathrm{Ind}_{U_{\tilde{H},\chi}}^{\tilde{G}}(1) \simeq \mathrm{Ind}_{U_{\tilde{H}',\chi'}}^{\tilde{G}}(1).$$

This means that from the assumptions of Theorem 2.10 we deduced conditions of Theorem 2.13. Therefore because of Theorem 2.6 we have that $\tilde{H}$ and $\tilde{H}'$ are conjugate and hence K is isomorphic to K'. □

Part II

Function Fields and Their L-functions

Chapter 3

Arithmetical Equivalence for Global Function Fields

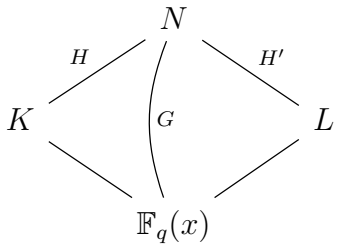
3.1 Introduction

3.1.1 Preliminaries

Let $q = p^m$, p be a prime number and $k = \mathbb{F}_q$. Let us consider two curves X and Y over k. As usual by a curve we mean a smooth, projective, geometrically connected variety of dimension one over k. If we fix a k-rational generically etale morphisms of X and Y to $\mathbb{P}^1$, then we obtain two finite separable geometric extensions of $\mathbb{F}_q(x)$ and we will denote them by K and K' respectively. By analogy with the number field case discussed in the previous chapter, we have notions of arithmetical equivalence, splitting equivalence, Gassmann equivalence and Dedekind zeta-function. For the sake of coherence let us briefly explain some notions, for details see [42], chapters V and IX.

First we recall that the polynomial ring $A = \mathbb{F}_q[x]$ is an analogue of $\mathbb{Z}$ with prime numbers replaced by monic irreducible polynomials. Prime ideals in $\mathbb{F}_q[x]$ are in one-to-one correspondence with monic irreducible polynomials in $\mathbb{F}_q[x]$. The ring $\mathbb{F}_q[x]$ is also a principal ideal domain. Any finite separable extension K of $\mathbb{F}_q(x)$ is given as quotient $\mathbb{F}_q[x,y]/(g(x,y))$ where $g(x,y) \in \mathbb{F}_q[x,y]$ is a monic, separable, irreducible polynomial in y with with coefficients in $\mathbb{F}_q[x]$. We suppose that this extension is geometric which means that the exact constant field of K is also $\mathbb{F}_q$. This restriction is not very important, but makes some theorems easier to state. Given a finite separable geometric extension K of $\mathbb{F}_q(x)$ we consider the integral closure $\mathcal{O}_K$ of $\mathbb{F}_q[x]$ in K. As in the number field case, in general this is not a principal ideal domain, but is a Dedekind domain, therefore in the function field case, the analogue of the Kummer-Dedekind theorem 1.2 from the previous chapter holds, as before see [33], chapter IV for the general statement about factorization of primes in Dedekind domains. It means the factorization of all except finitely many prime ideals (f) in $\mathcal{O}_K$ is given via factorization of the image of $g(x,y)$ into irreducible polynomials in the polynomial ring $(\mathbb{F}_q[x]/(f(x)))[y]$ associated to the residue field of (f). We say two such extensions K, K' *split equivalently* if for all except finitely many prime ideals (f) there is a bijection from prime ideals in $\mathcal{O}_K$ lying above (f) to those ideals of $\mathcal{O}_{K'}$. They are *arithmetically equivalent* if this bijection is degree preserving for almost all

primes. Finally since both extensions K, K' are separable they have common Galois closure which we denote by N. Note that the full constant field of N could be different from $\mathbb{F}_q$. Let $G = \mathrm{Gal}(N/\mathbb{F}_q(x))$, $H = \mathrm{Gal}(N/K)$, $H' = \mathrm{Gal}(N/L)$. See the diagram below.



As before we will say that (G, H, H') form a Gassmann triple if $\mathrm{Ind}_H^G(1_H) \simeq \mathrm{Ind}_{H'}^G(1_{H'})$, where 1_H(and $1_{H'}$) means trivial representation of H(of H' respectively). In this case we will also say that K, K' are Gassmann equivalent. Finally to each such extension one associates its Dedekind zeta-function. Following notations from [42], chapter V we define it as:

$$\zeta_K(s) = \sum_{\mathfrak{a} \geq 0} \mathcal{N}(\mathfrak{a})^{-s},$$

where $\mathfrak{a}$ runs over effective divisors of the corresponding curve X. In particular we include in the definition of $\zeta_K(s)$ infinite places of X and therefore $\zeta_K(s)$ does not depend on the map from X to $\mathbb{P}^1$.

It is not difficult to see that in this settings notions of Gassmann equivalence, splitting equivalence and arithmetical equivalence coincide. But in contrast to the number field case, Theorem 1.23 from the previous chapter is false in its full generality for the function field case. Namely, the implication from 1 to 2 is problematic. The problem is that the Dedekind zeta-function does not determine the splitting type, since in general there exist places in K with the same norm above different places of $\mathbb{F}_q(x)$. One suitable approach here is to change the definition of the zeta-function associated to K. It turns out, that if one replace usual zeta-function by the so-called *lifted Goss zeta-function*, then an analogue of Theorem 1.23 theorem becomes true. We refer an interested reader to [8]. The main purpose of this chapter is to recall and then extend another approach to study arithmetically equivalent global function fields.

3.1.2 Results of the Chapter

Let K/F be a Galois extension of global fields with the Galois group $G = \mathrm{Gal}(K/F)$. Then for any finite dimensional complex representation ρ of G one attaches the Artin L-function $L_F(\rho, s)$. The definition is essentially the same as in the number field case with one exception that we also need to include infinite primes of K. This is a meromorphic function of complex variable s. It also satisfies induction, inflation and additivity properties. Moreover by Theorem of A.Weil if K/F is geometric, ρ is irreducible and non-trivial then $L_K(\rho, s)$ is a polynomial in q^{-s}, see Theorem 9.16B, from [42]. For the sake of brevity we will denote it by $L_F(\rho)$, omitting the variable s.

As we already mentioned, K.Nagata in 1986 published [32] from which a careful reader can extract the following result:

Theorem 3.1. *Let K, K' denote two finite separable geometric extensions of $\mathbb{F}_q(x)$. Let N denote the common Galois closure and $G = \mathrm{Gal}(N/\mathbb{F}_q(x))$, $H = \mathrm{Gal}(N/K)$, $H' = \mathrm{Gal}(N/K')$. Let $\rho_1, \ldots, \rho_n$ denote all irreducible complex representations of G. Let $\psi = \mathrm{Ind}_H^G(1_H)$ and $\psi' = \mathrm{Ind}_{H'}^G(1_{H'})$. The following are equivalent:*

1. *For all i such that $1 \leq i \leq n$, we have $L_K(\rho_i|_H) = L_{K'}(\rho_i|_{H'})$;*
2. *$L_K(\psi|_H) = L_{K'}(\psi|_{H'})$ and $L_K(\psi'|_H) = L_{K'}(\psi'|_{H'})$;*
3. *K and K' are arithmetically equivalently;*
4. *K and K' split equivalently;*
5. *(G, H, H') forms a Gassmann triple.*

In this chapter we improve his argument and prove the above Theorem as a particular case of the following more general result[1]:

Theorem 3.2. *In the above settings let α denotes a complex representation of H and α' denotes a complex representation of H'. Let $\psi = \mathrm{Ind}_H^G(\alpha)$ and $\psi' = \mathrm{Ind}_{H'}^G(\alpha')$. For any representation ρ of G let $\bar{\rho}$ denote the dual representation of ρ.The following are equivalent:*

1. *For all i such that $1 \leq i \leq n$ we have equality of Artin L-functions: $L_K(\alpha \otimes \rho_i|_H) = L_{K'}(\alpha' \otimes \rho_i|_{H'})$*
2. *$L_K(\bar{\alpha} \otimes (\psi|_H)) = L_{K'}(\bar{\alpha'} \otimes (\psi|_{H'}))$, and*
   $L_K(\bar{\alpha} \otimes (\psi'|_H)) = L_{K'}(\bar{\alpha'} \otimes (\psi'|_{H'}))$;
3. *Induced representations ψ and ψ' are isomorphic.*

This Theorem is not just a formal generalisation of Nagata's results but also allows us to use group theory to construct for any given pair of non-isomorphic global function fields a *finite list of L-functions which distinguishes them.* As in the previous section this goal is achieved in two steps. First we need the group-theoretical result discussed in the previous chapter, namely Theorem 2.6. Next, in the settings of Theorem [3.1] we construct a Galois extension M of $\mathbb{F}_q(t)$ containing K and K' such that the Galois group $\mathrm{Gal}(M : \mathbb{F}_q(t))$ is $\tilde{G}$ and $K = M^{\tilde{H}}$, $K' = M^{\tilde{H}'}$ for $\tilde{G}$, $\tilde{H}$, $\tilde{H}'$ as in Theorem [2.6]. Altogether, this gives us:

Theorem 3.3. *For a given pair K and K' of finite separable geometric extensions of $F = \mathbb{F}_q(t)$ there exists a Galois extension M of $\mathbb{F}_q(t)$ with Galois group $\tilde{G}$, such that $K = M^{\tilde{H}}$ and $K' = M^{\tilde{H}'}$ for some subgroups $\tilde{H}$, $\tilde{H}'$ of $\tilde{G}$ with the following properties. There exists an abelian character α of $\tilde{H}$ such that for any abelian character α' of $\tilde{H}'$ the following are equivalent :*

1. *For any irreducible representation ρ of $\tilde{G}$ we have equality of Artin L-functions:*

$$L_K(\alpha \otimes \rho|_{\tilde{H}}) = L_{K'}(\alpha' \otimes \rho|_{\tilde{H}'});$$

[1] In order to get Nagata's result plug in the settings trivial representations $\alpha = 1_H$ and $\beta = 1_{H'}$

2. $L_K(\bar{\alpha} \otimes (\psi|_{\tilde{H}})) = L_{K'}(\bar{\alpha'} \otimes (\psi|_{\tilde{H'}}))$, *and*
   $L_K(\bar{\alpha} \otimes (\psi'|_{\tilde{H}})) = L_{K'}(\bar{\alpha'} \otimes (\psi'|_{\tilde{H'}}))$,
   where $\psi = \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\alpha)$ *and* $\psi' = \mathrm{Ind}_{\tilde{H'}}^{\tilde{G}}(\alpha')$;

3. *Induced representations* ψ *and* ψ' *are isomorphic.*

Moreover, if those conditions hold then K *and* K' *isomorphic as extensions of* $\mathbb{F}_q(t)$.

The chapter has the following structure: in the next section we give a proof of Theorem 3.2. After that we study arithmetical equivalence for global function fields: we provide few explicit examples of non-isomorphic, but arithmetically equivalent global function fields, discuss an algorithm to construct two-parametric family of such pairs for many base fields of different characteristic and briefly review properties of such fields. In the next section we give a proof of Theorem 2.6 and in the last section we give a proof of Theorem 3.3.

3.2 On the L-functions criteria

In this section we are going to prove our main Theorem 3.2, but before that, let us first consider one particular example of Theorem 3.1. This example illustrates the following: we construct two degree two extensions K, K' of $\mathbb{F}_7(x)$ such that $\zeta_K(s) = \zeta_{K'}(s)$, but K and K' are not arithmetically equivalent. Denoting by N the common normal closure of K and K' and keeping notations from the settings of 3.1 we will construct a character χ of $\mathrm{Gal}(N : \mathbb{F}_7(x))$ such that

$$L_K(\chi|_H, s) \neq L_{K'}(\chi|_{H'}, s).$$

Example 3.4. *Consider two elliptic curves* E *and* E' *over* $\mathbb{F}_7$, *affine part of which defined by equations* $y^2 = x^3 + 1$ *and* $y^2 = x^3 + 3x + 1$ *respectively. Let us denote by* K *and* K' *the corresponding function fields. One checks that*

$$\zeta_K(T) = \frac{7T^2 + 4T + 1}{(1 - T)(1 - 7T)} = \zeta_{K'}(T),$$

where $T = 7^{-s}$. *Hence by the theorem of A.Weil,* E *and* E' *are* $\mathbb{F}_7$*-isogenous, but* $j(E) = 0$ *and* $j(E') = 2$ *so they are not isomorphic even over the algebraic closure* $\overline{\mathbb{F}_7}$ *and hence* $K \ncong K'$.

In the above example we have two quadratic extensions $\mathbb{F}_7(\sqrt{f_i(x)})/\mathbb{F}_7(x)$, where $f_1(x) = x^3 + 1$ and $f_2(x) = x^3 + 3x + 1$. Obviously those are abelian Galois extensions with Galois group C_2. It means that despite the fact that K and K' share the same ζ-function they do not share splitting type(otherwise they must be isomorphic). According to Theorem 3.1 this means that there exists an L-function which distinguishes them. More concretely, let us consider the common Galois closure N. We denote by G, H, H' Galois groups of $\mathrm{Gal}(N/\mathbb{F}_7(x)), \mathrm{Gal}(N/K), \mathrm{Gal}(N/K')$, respectively. We have $G = C_2 \oplus C_2$ and hence there exists a one-dimensional character χ of G such that $\chi|_H = 1_H$ and $\chi|_{H'} \neq 1_{H'}$. Now $L_K(\chi|_H) = \zeta_K$ and therefore this function has a pole at $s = 1$. But, $L_{K'}(\chi|_{H'})$ is an Artin L-function of a non-trivial abelian character, hence it has no poles, see [42],chapter IX. Therefore we see that

$$L_K(\chi|_H) \neq L_{K'}(\chi|_{H'}).$$

This idea gives rise to Theorems 3.1 and 3.2.

Proof of Theorem 3.2. First we show implication **from (1) to (3)**. For any fixed representation ρ of G we consider $L_K(\alpha \otimes \rho|_H)$. This is a meromorphic L-function with no poles outside $s = 0$ and $s = 1$, see [42]. By properties of Artin L-functions this function has a pole at $s = 1$ of order $(\alpha \otimes \rho|_H, 1)_H$, possibly zero. Because of properties of complex representations: $(\alpha \otimes \rho|_H, 1)_H = (\rho|_H, \bar{\alpha})_H$, where $\bar{\alpha}$ means the dual of the representation α. By Frobenius reciprocity we have

$$(\rho|_H, \bar{\alpha})_H = (\rho, \mathrm{Ind}_H^G(\bar{\alpha}))_G.$$

In means that equality $L_K(\alpha \otimes \rho_i|_H) = L_{K'}(\alpha' \otimes \rho_i|_{H'})$ implies

$$(\rho_i, \mathrm{Ind}_H^G(\bar{\alpha}))_G = (\rho_i, \mathrm{Ind}_{H'}^G(\bar{\alpha}'))_G.$$

Since ρ_i runs over all irreducible representations of G it means that

$$\mathrm{Ind}_H^G(\bar{\alpha}) \simeq \mathrm{Ind}_{H'}^G(\bar{\alpha}')$$

and therefore $\mathrm{Ind}_H^G(\alpha) \simeq \mathrm{Ind}_{H'}^G(\alpha')$.

From (3) to (1). By Frobenius reciprocity for each i, $j \in \{1 \dots n\}$ we have:

$$(\mathrm{Ind}_H^G(\alpha \otimes \rho_i|_H), \rho_j)_G \simeq (\alpha \otimes \rho_i|_H, \rho_j|_H)_H \simeq (\alpha, (\bar{\rho}_i \otimes \rho_j)|_H)_H \simeq (\mathrm{Ind}_H^G(\alpha), \bar{\rho}_i \otimes \rho_j)_G,$$

By our assumptions $\mathrm{Ind}_H^G(\alpha) \simeq \mathrm{Ind}_{H'}^G(\alpha')$, we therefore have:

$$(\mathrm{Ind}_H^G(\alpha), \bar{\rho}_i \otimes \rho_j)_G \simeq (\mathrm{Ind}_{H'}^G(\alpha'), \bar{\rho}_i \otimes \rho_j)_G,$$

and hence for each irreducible representation ρ_i, we have:

$$\mathrm{Ind}_H^G(\alpha \otimes \rho_i|_H) \simeq \mathrm{Ind}_{H'}^G(\alpha' \otimes \rho_i|_{H'}).$$

Finally, by the Artin induction property it follows that:

$$L_K(\alpha \otimes \rho_i|_H) = L_{\mathbb{F}_q(x)}(\mathrm{Ind}_H^G(\alpha \otimes \rho_i|_H)),$$

and therefore we are done.

From (2) to (3). As before from equality of L-functions we obtained equality of orders of poles at $s = 1$ and therefore following equalities:

$$(\bar{\alpha} \otimes (\psi|_H), 1_H)_H = (\bar{\alpha'} \otimes (\psi|_{H'}), 1_{H'})_{H'}$$

and

$$(\bar{\alpha} \otimes (\psi'|_H), 1_H)_H = (\bar{\alpha'} \otimes (\psi'|_{H'}), 1_{H'})_{H'}.$$

By Frobenius reciprocity we have:

$$(\bar{\alpha} \otimes (\psi|_H), 1_H)_H = (\alpha, \psi|_H)_H = (\psi, \psi)_G$$

and

$$(\bar{\alpha'} \otimes (\psi|_{H'}), 1_{H'})_{H'} = (\alpha', \psi|_{H'})_{H'} = (\psi', \psi)_G$$

Therefore assumptions of (2) implies $(\psi,\psi)_G = (\psi,\psi')_G = (\psi',\psi')_G$. Let us consider the scalar of product of the virtual representation $\psi - \psi'$ with itself: $(\psi-\psi',\psi-\psi')_G = (\psi,\psi)_G - 2(\psi,\psi')_G + (\psi',\psi')_G = 0$. Which implies that ψ and ψ' are isomorphic.

From (3) to (2)

Note that $L_K(\bar{\alpha}\otimes(\psi|_H)) = L_{\mathbb{F}_q(x)}(\mathrm{Ind}_H^G(\bar{\alpha}\otimes(\psi|_H)))$. Therefore in order to get equality of L-functions it is enough to show:

$$\mathrm{Ind}_H^G(\bar{\alpha}\otimes(\psi|_H)) \simeq \mathrm{Ind}_{H'}^G(\bar{\alpha'}\otimes(\psi|_{H'})).$$

Let ρ_i run over irreducible representations of G. By Frobenius reciprocity we have:

$$(\mathrm{Ind}_H^G(\bar{\alpha}\otimes(\psi|_H)),\rho_i)_G = (\bar{\alpha}\otimes\psi|_H,\rho_i|_H)_H = (\bar{\alpha},\rho_i|_H\otimes\bar{\psi}|_H)_H = (\bar{\psi},\rho_i\otimes\bar{\psi})_G.$$

Since $\psi=\psi'$ we have:

$$(\bar{\psi},\rho_i\otimes\bar{\psi})_G = (\bar{\psi'},\rho_i\otimes\bar{\psi})_G = (\bar{\alpha'},\rho_i|_{H'}\otimes\bar{\psi}|_{H'})_{H'} = (\bar{\alpha'}\otimes\psi|_{H'},\rho_i|_{H'})_{H'} = (\mathrm{Ind}_{H'}^G(\bar{\alpha'}\otimes(\psi|_{H'})),\rho_i)_G$$

Which means that two representations are isomorphic:

$$\mathrm{Ind}_H^G(\bar{\alpha}\otimes(\psi|_H)) \simeq \mathrm{Ind}_{H'}^G(\bar{\alpha'}\otimes(\psi|_{H'})).$$

By replacing ψ by ψ' we obtained the second equality of L-functions. □

Note that if α is the trivial representation, then $L_K(\alpha\otimes\rho_H) = L_K(\rho_H)$. Therefore equality of L-functions for each irreducible ρ: $L_K(\rho|_H) = L_{K'}(\rho|_{H'})$ implies arithmetical equivalence and vice versa.

This remark generalises the fact that equality of zeta-functions in the number field case is the same as arithmetical equivalence. At first sight this generalisation to the function field side seems to be not very natural, since it depends on the k-rational map of the curve X to $\mathbb{P}^1$ and not given in the intrinsic terms of X, but as we will see in the next section, this map is very important for the notion of arithmetical equivalence: it is possible to map curves X and Y to $\mathbb{P}^1$ in two different ways, such that their function fields are arithmetically equivalent under the first pair of maps, but not arithmetically equivalent under the second pair of maps.

3.3 On Gassmann Equivalence

3.3.1 Examples

In order to find examples of arithmetically equivalent function fields we must find a non-trivial example of a Gassmann triple (G,H,H') and solve the inverse Galois problem for G. As we already mentioned in 1.4.2 Gassmann triples corresponding to field extensions of degree up to 15 were classified in [5]. It follows that fields with Galois group $G \simeq \mathrm{PGL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ give rise to at least two non-trivial Gassmann triples: one in degree seven and one in degree fourteen. Also, fields with Galois group $G \simeq \mathrm{PSL}_2(\mathbb{F}_{11})$ give rise to at least one pair of arithmetically equivalent fields of degree eleven.

Using Magma we compute the Galois group of the splitting field of a given polynomial $f \in \mathbb{F}_q(x)[y]$ chosen in some particular way and find all intermediate subfields. By doing that for many different f we find explicit equations of arithmetically equivalent function fields and compare their properties.

Some Constructions

Here are some examples.

Example 3.5. *Let $p = 7$, $q = p^2$ and let α be a generator of $\mathbb{F}_q^*$. Consider the function field extension of $\mathbb{F}_q(x)$ given by $f(y) = y^{p+1} + y - x^{p+1}$. Its splitting field N has degree 168 and Galois group $\mathrm{Gal}(N : \mathbb{F}_q(x)) \simeq \mathrm{PGL}_3(\mathbb{F}_2)$. Inside this field we have at least two pairs of arithmetically equivalent global function fields:*

1. *$K_1 : y^7 + 6x^8y^3 + \alpha^{28}x^{12}y + 4$ and $K_1' : y^7 + 5x^8y^3 + \alpha^4x^{12}y + 6$;*
2. *$K_2 : y^{14} + 3x^8y^6 + \alpha^4x^{12}y^2 + 5$ and $K_2' : y^{14} + 3x^8y^6 + \alpha^{28}x^{12}y^2 + 5$;*

Note that since these fields arise from non-trivial triple (G, H, H') it means that they are not isomorphic as extensions of $\mathbb{F}_q(x)$, but it may happen that K and K' isomorphic as abstract fields. Indeed, one could check that in this case we have $K_1 \simeq K_1'$ and $K_2 \simeq K_2'$ as fields.

An interesting question is: is it possible to find arithmetically equivalent function fields K and K' that are not isomorphic as abstract fields? It was mentioned in [6] that a result by J.P. Serre states that the function field of the normal closure of the field given by $y^{p+1} - xy + 1$ over $\mathbb{F}_p$ has Galois group $\mathrm{PSL}_2(\mathbb{F}_p)$. By working out this example for $p = 7$ and $p = 11$ one finds a positive answer to the above question:

Example 3.6. *Consider the curve defined by the affine equation $y^8 - xy + 1$ over $\mathbb{F}_7$. The corresponding function field N of the normal closure has degree 168 and the Galois group is $G \simeq \mathrm{PGL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. Inside this field we have at least two pairs of arithmetically equivalent global function fields:*

1. *$K_1 : y^7 + 2y^3 + 2y + 6x^2$ and $K_1' : y^7 + y^3 + 5y + 4x^2$;*
2. *$K_2 : y^{14} + 4y^6 + 5y^2 + 5x^2$ and $K_2' : y^{14} + 4y^6 + 2y^2 + 5x^2$;*

Being arithmetically equivalent they share the same zeta-function and therefore their Weil-polynomials $f_K(T)$ are the same. Since $\#\,\mathrm{Pic}^0(C)[\mathbb{F}_q] = h = f_K(1)$ is the class number, we have that in contrast to the number fields they share the same class numbers, see [10]. But they have different class groups[2], hence they are not isomorphic. Indeed according to Magma we have:

$$\mathrm{Cl}(K_1) \simeq \mathrm{Cl}(K_2) \simeq \mathbb{Z}/8\mathbb{Z}$$

but

$$\mathrm{Cl}(K_1') \simeq \mathrm{Cl}(K_2') \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

The fact that $\mathrm{Cl}(K_1) \simeq \mathrm{Cl}(K_2)$ and $\mathrm{Cl}(K_1') \simeq \mathrm{Cl}(K_2')$ is not coincidence: $K_1 \simeq K_2$ and $K_1' \simeq K_2'$ as abstract fields. Another important remark here is that the genus of K_1 and K_1' is one. They have a rational point over $\mathbb{F}_7$ and therefore correspond to two elliptic curves E and E' defined over $\mathbb{F}_7$. By considering Weierstrass models of E and E' one gets degree two extensions of $\mathbb{F}_7(x)$, such that they are not arithmetically equivalent. More concretely, the curve defined by $y^7 + 2y^3 + 2y + 6x^2 = 0$ is isomorphic to the elliptic curve E_1 defined by $y^2 - x^3 - x = 0$ and the

[2]By a class group we mean the group of $\mathbb{F}_q$-rational points on the Jacobian variety $\mathrm{Jac}(X)$ associated to X.

curve given by the equation $y^7+y^3+5y+4x^2=0$ is isomorphic to the elliptic curve E_2 defined by $y^2-x^3-3x=0$. This illustrates that the notion of arithmetical equivalence completely depends on the map from X to $\mathbb{P}^1$.

Example 3.7. *Consider the curve defined by the affine equation* $y^{12}-xy+1=0$ *over* $\mathbb{F}_{11}$. *The corresponding function field* N *of the normal closure has degree 660 and the Galois group is* $G\simeq \mathrm{PSL}_2(\mathbb{F}_{11})$. *Inside this field we have at least one pair of arithmetically equivalent global function fields:* $K_1: y^{11}+2y^5+8y^2+10x^2=0$ *and* $K_1': y^{11}+2y^5+3y^2+10x^2=0$.

One checks that K_1 and K_1' are not isomorphic as global fields, also have genus one and that $\mathrm{Cl}(K_1)\simeq \mathrm{Cl}(K_1')\simeq \mathbb{Z}/12\mathbb{Z}$.

Magma scripts

Let us first check example 3.5

```
// Initializing the function field F
p := 7; q := p^2;
K<alpha> := GF(q);
R<x> := FunctionField(K);
P<y> := PolynomialRing(R);
f := y^(p+1) + y - x^(p+1);
FF<alpha> := FunctionField(f);

// Verifying that the Galois of the normal closure of F is isomorphic to PGL_3(F_2)
G0 := PGL(3,2);
G, r, N := GaloisGroup(FF);
"Degree of the normal closure N of K is", #G;
"Is G isomorphic to PGL_3(F_2): ", IsIsomorphic(G,G0);

h := Subgroups(G: IndexEqual := 7);
H_1 := h[1]`subgroup;
H_2 := h[2]`subgroup;
"Is H_1 conjugate to H_2 inside G: ", IsConjugate(G, H_1, H_2);

"The group H_1 corresponds to the field extensions: ", GaloisSubgroup(N, H_1);
"The group H_2 corresponds to the field extensions: ", GaloisSubgroup(N, H_2);
```

This script produces the following output which completely aligned with the expectations:

```
Degree of the normal closure N of K is 168
Is G isomorphic to PGL_3(F_2):  true Homomorphism of GrpPerm: G, Degree 8, Order
2^3 * 3 * 7 into GrpPerm: G0, Degree 7, Order 2^3 * 3 * 7 induced by
    (1, 6)(2, 4)(3, 7)(5, 8) |--> (2, 6)(4, 5)
    (1, 4, 8, 2)(3, 6, 5, 7) |--> (1, 6)(2, 4, 3, 7)
Is H_1 conjugate to H_2 inside G:  false
The group H_1 corresponds to the field extensions:  y^7 + 6*x^8*y^3 +
```

```
    alpha^28*x^12*y + 4
((((x1 + x4) + x6) + x8)^2 + (((x2 + x3) + x5) + x7)^2)
The group H_2 corresponds to the field extensions:  y^7 + 5*x^8*y^3 +
    alpha^4*x^12*y + 6
((((x1 + x5)^2 + (x6 + x2)^2) + (x8 + x3)^2) + (x4 + x7)^2)
```

Let us also check that for instance fields K_1, K_1' from 3.6 indeed split equivalently. To do so we pick a few random prime ideals $\mathcal{P}$ in $\mathbb{F}_q[x]$ and compare factors of reductions of $y^7 + 2y^3 + 2y + 6x^2$ and $y^7 + y^3 + 5y + 4x^2$ modulo $\mathcal{P}$:

```
p := 7;
Fq := GF(p);
k<x> := RationalFunctionField(Fq);

for i in [1..10] do
  P := RandomIrreduciblePolynomial(Fq, i);
  R<x> := ExtensionField<k, x | P>;
  RR<y> := PolynomialRing(R);
  f := y^7 + 2*y^3 + 2*y + 6*x^2;
  g := y^7 + y^3 + 5*y + 4*x^2;
  "Factorization of f mod", P, Factorization(f);
  "Factorization of g mod", P, Factorization(g);
end for;
```

The above code confirms that indeed at least for some randomly chosen primes $\mathcal{P}$ there exists a degree preserving bijection between ideals of $\mathcal{O}_{K_1}$ lying above $\mathcal{P}$ to those ideals of $\mathcal{O}_{K_1'}$:

```
...
Factorization of f mod x^2 + 5*x + 3
[
    <y + 6*x + 5, 1>,
    <y^3 + (3*x + 6)*y^2 + 4*x*y + 4, 1>,
    <y^3 + (5*x + 3)*y^2 + 3*x*y + 4, 1>
]
Factorization of g mod x^2 + 5*x + 3
[
    <y + 3*x + 6, 1>,
    <y^3 + (5*x + 3)*y^2 + (x + 5)*y + x + 6, 1>,
    <y^3 + (6*x + 5)*y^2 + (6*x + 2)*y + x + 6, 1>
]
Factorization of f mod x^3 + 4*x^2 + 4*x + 6
[
    <y^7 + 2*y^3 + 2*y + 6*x^2, 1>
]
Factorization of g mod x^3 + 4*x^2 + 4*x + 6
[
```

```
    <y^7 + y^3 + 5*y + 4*x^2, 1>
]
...
```

Construction by Torsion Points on Elliptic Curves

All the above examples work only for some particular characteristic p of the base field. Moreover, for any example of non-isomorphic Gassmann equivalent pair (K, K') given above fields K and K' actually become isomorphic after a constant field extension. It means that corresponding curves X and Y are twists of each other. In this section we discuss an algorithm to construct examples of families of pairs of arithmetically equivalent global function fields of arbitrary characteristic p of the ground field, provided p is greater than three. By using this approach we found geometrically non-isomorphic arithmetically equivalent global fields.

Let l denote a prime number. As it follows from [5] that extensions with Galois group $G \simeq \mathrm{Gl}_2(\mathbb{F}_l)$ play an important role in the construction of arithmetically equivalent fields. If E is an ordinary elliptic curve defined over $\mathbb{Q}$, then the group $E[l]$ of l-torsion points of E allows us to construct arithmetically equivalent number fields, as in [9]. But in contrast to the number field case, in the function field settings torsion points on elliptic curves over $\mathbb{F}_q(t)$ do not always allow to construct extensions with Galois group isomorphic to $\mathrm{Gl}_2(\mathbb{F}_l)$. The crucial difference appears because of constant field extensions.

More concretely, consider the function field F of the projective line defined over $\mathbb{F}_q$: $F \simeq \mathbb{F}_q(t)$, where $q = p^m$, p is prime. Suppose for simplicity that $p > 3$ and pick parameters a, $b \in \mathbb{F}_q[t]$. Consider an elliptic curve E over F defined by the equation $y^2 = x^3 + ax + b$. For any prime number $l \neq p$ let us consider $\phi_{l,E}(u)$ the l-division polynomial of E. This is a polynomial with coefficients in F and with roots corresponding to x-coordinates of l-torsion points of the elliptic curve E, for example:

$$\phi_{3,E}(u) = 3u^4 + au^2 + 12bu - a^2.$$

Finally, let $R(t, y) = \mathrm{Res}_x(\phi_{l,E}(x), y^2 - (x^3 + ax + b))$ be the resultant with respect to x. This is a polynomial in t and y, whose roots correspond to the coordinates of l-torsion points of E. Generically this is separable polynomial and it generates the finite field extension $K(y)$ of $\mathbb{F}_q(t)$: $K(y) = \frac{\mathbb{F}_q(t)[y]}{(R(t,y))}$. We will denote the Galois group of the normal closure of K over F by G. Let H be the subgroup of $\mathbb{F}_l^\times$ generated by q. The analogue of the so-called *Serre's open image Theorem* for function fields proved by Igusa in 1959 states that for big enough l depending on q we have the following exact sequence, see [3]:

$$1 \to \mathrm{SL}_2(\mathbb{F}_l) \to G \to H \to 1.$$

Moreover, in this sequence $\mathrm{SL}_2(\mathbb{F}_l)$ corresponds to the geometric extension of F and H corresponds to the constant field extension. If $q = 1 \mod l$ then H is trivial and we obtain a geometric extension with $G \simeq \mathrm{SL}_2(\mathbb{F}_l)$. By taking a quotient of G by ± 1, we will get $\mathrm{PSL}_2(\mathbb{F}_l)$. The action of ± 1 is given by gluing points with the same x-coordinate. Therefore, the splitting field of $\phi_{l,E}(x)$ is the geometric extension of $\mathbb{F}_q(t)$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_l)$. Now if $l = 7$ or $l = 11$ we obtain a family of arithmetically equivalent pairs.

Example 3.8. *In the above settings let $p = 29$ and $l = 7$, $a = t$, $b = t + 1$. Then: $\phi_{7,E}(x)$ is a polynomial of degree 24. The splitting field of $\phi_{7,E}(x)$ is a finite geometric extension $K/\mathbb{F}_{29}(t)$ with the Galois group isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. Inside this normal closure following two arithmetically equivalent fields are not isomorphic:*

$$K[x]/(x^7 + 20tx^6 + 14t^2x^5 + (6t^3 + 11t^2 + 22t + 11)x^4 + (5t^4 + 23t^3 + 17t^2 + 23t)x^3 +$$
$$+(20t^5 + 13t^4 + 26t^3 + 13t^2)x^2 + (5t^6 + 20t^5 + 5t^3 + 21t^2 + 14t + 18)x +$$
$$+23t^7 + 26t^6 + 19t^5 + 10t^4 + 5t^3 + 13t^2 + 25t)$$

and

$$K[x]/(x^7 + 16tx^6 + 2t^2x^5 + (18t^3 + 10t^2 + 20t + 10)x^4 + (27t^4 + 3t^3 + 6t^2 + 3t)x^3 +$$
$$+(27t^5 + 17t^4 + 5t^3 + 17t^2)x^2 + (t^6 + 7t^5 + 16t^4 + 15t^3 + 12t^2 + 8t + 2)x +$$
$$+28t^7 + t^6 + 2t^5 + t^4).$$

According to Magma function fields given above have genus 1 and a $\mathbb{F}_{29}$-rational point, therefore they are isomorphic to the function fields of two elliptic curves. Those elliptic curves have different j-invariant, namely 16 and 15 respectively. Therefore, they are geometrically non-isomorphic.

3.3.2 Properties of Arithmetically Equivalent Fields

In this section we will briefly discuss common properties of arithmetically equivalent global fields that will shed some light on the previous examples. Recall the statement 1.18 from the introduction:

Lemma 3.9. *Let G be a finite group and $H \subset G$ a subgroup of index n. Suppose one of the following conditions holds:*

1. *$n \leq 6$;*
2. *H is cyclic;*
3. *$G = \mathbb{S}_n$ the full symmetric group of order n;*
4. *$n = p$ is prime and $G = \mathbb{A}_p$ is the alternating group of order p.*

then any Gassmann triple (G, H, H') is trivial.

Taking into account our main Theorem this statement has the following application to the function field side:

Corollary 3.10. *Let K be a finite separable geometric extension of $\mathbb{F}_q(t)$ of degree n and let N be its Galois closure with Galois group G. Let H be a subgroup of G such that $K = N^H$. Suppose one of the conditions from the previous lemma holds. Let $H' \subset G$ be a subgroup and let $K' = N^{H'}$. Fields K and K' are isomorphic if and only if for each irreducible representation ρ of G we have $L_K(\rho|_H) = L_{K'}(\rho|_{H'})$.*

Adele Rings

Let K be a global field and let A_K denote the Adele ring of K. By definition this is the restricted product of all local completions K_v with respect to $\mathcal{O}_v$, where v denotes a place of K. It has a topology coming from restricted product and therefore it is a topological abelian group.

The first remarkable fact is that in the number field case we have the following implications: $A_K \simeq A_L \Rightarrow \zeta_K = \zeta_L \iff K$ and L arithmetically equivalent. And moreover there exists an example of arithmetically equivalent number fields with non-isomorphic Adele rings, see [44].

On the other hand in the function field side we have the following: $A_K \simeq A_L \iff \zeta_K = \zeta_L \Leftarrow K$ and L arithmetically equivalent. For the proof of equivalence see [55]. Roughly speaking the reason here is that in the function fields case the isomorphism type of the local completion $\mathcal{O}_v$ depends only on the degree of v. For number fields this is not the case.

Ideal Class Group

Arithmetically equivalent function fields share the same zeta-function and therefore they also share the same class-number. Indeed the by the analogue of the class-number formula the order of the class group is given as $L(0)$ where $\zeta_K(s) = \frac{L(s)}{(1-q^{-s})(1-q^{1-s})}$. But their class-groups may be different, as in example [3.6]. Nevertheless exactly as in the number field case we have a Perlis invariant v associated to each Gassmann-triple (G, H, H') . In the function field case also for any prime number $l \neq p$ co-prime to v one has:

$$\mathrm{Cl}_l(K) \simeq \mathrm{Cl}_l(K').$$

In order to see this one could replace word-by-word the construction from the number field case, but probably a slightly more interesting approach is the following taken from [22]. Recall that the class-group is by definition the group of $\mathbb{F}_q$-rational points on the Jacobian $\mathrm{Jac}(X)$ associated to X. Now, to each relation between induced representations of trivial characters one associates isogeny relations between Jacobians of corresponding curves. In the case of Gassmann equivalence one has $\mathrm{Ind}_H^G 1 \simeq \mathrm{Ind}_{H'}^G 1$ which leads to isogenies between Jacobians of corresponding curves X, X'. Degrees of these isogenies are given in terms of the triple (G, H, H') and closely related to the invariant v. This shows that if l is co-prime to v then there exists an isogeny from $\mathrm{Jac}(X)$ to $\mathrm{Jac}(X')$ of degree co-prime to l which leads to the isomorphism of l-parts of class groups.

3.4 On Monomial Representations

The main purpose of this section is to prove Theorem 2.6. Before doing that let us recall some basic facts from the theory of induced representations. Let G be a finite group and H a subgroup. Let χ be a one-dimensional representation of H. Consider the induced representation ψ of G: $\psi = \mathrm{Ind}_H^G \chi$. By definition ψ acts on the vector space V which could be associated with the direct sum of lines $\oplus \mathbb{C}_{g_i}$ where each $\mathbb{C}_{g_i}$ corresponds to the i-th left coset G/H. Such a pair $(\psi, \oplus \mathbb{C}_{g_i})$ is called a *monomial representation*. Let H' be another subgroup of G and $\psi' = \mathrm{Ind}_{H'}^G \chi'$ for one-dimensional χ' of H'. We will say that we have morphism of pairs

$(\psi, \oplus\mathbb{C}_{g_i})$, $(\psi', \oplus\mathbb{C}_{g'_j})$ if we have a morphism of representations f: $\psi \to \psi'$ such that for each line $\mathbb{C}_{g_i}$ we have $f(\mathbb{C}_{g_i}) \subset \mathbb{C}_{g'_j}$ for some j.

Lemma 3.11. *Suppose we have an isomorphism of monomial representations* $(\psi, \oplus\mathbb{C}_{g_i}) \simeq (\psi', \oplus\mathbb{C}_{g'_j})$. *Then H is a conjugate of H' in G.*

Proof. For the reference see [16]. □

Example 3.12. *Let G be the group of multiplicative quaternions with generators a and b. Consider the subgroups $H_a = \{1, a, -1, -a\}$ and $H_b = \{1, b, -1, -b\}$. Let χ_a be an isomorphism $H_a \simeq \mu_4^*$ sending element a to i. Let χ_b be the same character for H_b. Then one has* $\mathrm{Ind}_{H_a}^G \chi_a \simeq \mathrm{Ind}_{H_b}^G \chi_b$ *as representations, but not as monomial representations.*

Let us recall settings for Theorem 2.6. Let G be a finite group and H a subgroup of index n and $C_l = \mu_l$ be a cyclic group of order l, where l is an odd prime. Let us consider semi-direct products $\tilde{G} = C_l^n \rtimes G$ and $\tilde{H} = C_l^n \rtimes H$, where G acts on C_l^n by permuting its component as cosets G/H. Let $g_1, \ldots, g_n$ be representatives of left cosets $G = \cup_i g_i H$. Without loss of generality we assume that $g_1 = e$ is the identity element. Note that g_i for $i \neq 1$ cannot fix the first coset. We define χ to be the homomorphism from $\tilde{H} \to \mu_l$, sending an element $(c_1, \ldots, c_n, g)$ to c_1. This is indeed a homomorphism, since H fixes the first coset. Then the following is true:

Theorem 3.13 (Bart de Smit)**.** *For any subgroup $\tilde{H}' \subset \tilde{G}$ and any abelian character $\chi' : \tilde{H}' \to \mathbb{C}^*$ if $\mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi') \simeq \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$ then $\tilde{H}'$ and $\tilde{H}$ are conjugate in $\tilde{G}$.*

Proof. **Step 1.** Consider cosets $\tilde{G}/\tilde{H}$. We claim that each such coset for $i > 1$ can be represented as $\gamma_i = (1, 1, \ldots, 1, g_i)$, where $g_i \in G/H$. This is true since elements of the form $(\zeta_1, \zeta_2, \ldots, \zeta_n, 1)$ are in $\tilde{H}$, where $(\zeta_1, \zeta_2, \ldots, \zeta_n) \in C_l^n$.

Step 2. Let us consider element $\alpha = (\zeta, 1, \ldots, 1, \ldots, 1) \in \tilde{H}$ where $\zeta \in \mu_l$, $\zeta \neq 1$ is in the first position. Such element fixes each coset $\gamma_i \tilde{H}$. Therefore if $\psi = \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$ then $\psi(\alpha)$ is a diagonal matrix with l-th roots of unity on the diagonal. Moreover, it is the matrix with the first element is ζ on the diagonal and each other diagonal element equals to one. Indeed, by definition of induced representation on the i-th position we have $\chi(\gamma_i^{-1}\alpha\gamma_i)$ and it is easy to see that $\gamma_i^{-1}\alpha\gamma_i$ has 1 on the first position, provided $i \neq 1$.

Step 3. We claim that $\psi'(\alpha_i)$ is also a diagonal matrix, where $\psi' = \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi')$. We know that this is a matrix with exactly one non-zero element in each row and column. Suppose it is not a diagonal, therefore it changes at least two elements and hence trace of this matrix is $\sum_{k=1}^{n-2} \zeta_i$, where ζ_i are roots of unity. Since $\psi \simeq \psi'$ we have $n - 1 + \zeta = \sum_{k=1}^{n-2} \zeta_i$, which can't be true since the absolute value of the left hand side is strictly bigger than $n - 2$. Here we use the fact that $l > 2$ and therefore $\zeta \neq \pm 1$.

Step 4. Let A be an isomorphism of representations ψ and ψ'. We will show that it is *an isomorphism of monomial representations* $(\psi, \oplus\mathbb{C}_i) \simeq (\psi', \oplus\mathbb{C}_j)$. Indeed, it suffices to show that in the given basis A is written as permutation matrix. Suppose it is not and therefore we have at least two non-zero elements in one columm. Also it has another non-zero element in some of those two rows, otherwise $\det(A)$ must be zero which is not since A is an isomorphism. We have $A\psi(\alpha) = \psi'(\alpha)A$ which is easy to calculate since $\psi(\alpha)$ and $\psi'(\alpha)$ are diagonal. By comparing elements from left and right hand sides one has $\zeta = 1$ which leads to the contradiction. □

3.5 The Proof of Theorem 3.3

In this section we will prove Theorem [3.3]. We will denote by F the rational function field with the base field $\mathbb{F}_q$: $F = \mathbb{F}_q(t)$, where $q = p^m$, p is prime. It is enough to show that for any separable geometric extension K of F of degree n, with extension N of K, N normal over F and Galois Groups $G = \mathrm{Gal}(N/F)$ and $H = \mathrm{Gal}(N/K)$ there exist an odd prime l and Galois extension M over F with $\mathrm{Gal}(M/F) \simeq C_l^n \rtimes G$ and $\mathrm{Gal}(M/K) = C_l^n \rtimes H$, where G acts on components of C_l^n by permuting them as cosets G/H. We will prove this statement in a few steps.

The Chebotarev density Theorem for function fields see [42] theorem[9.13B], insures us that for any sufficiently large number T we could find a prime $\mathfrak{p}$ of F which has degree T and splits completely in N. Note that if prime splits completely in N then it also splits completely in K. Now, we pick an odd prime number l co-prime to the characteristic p, to $q-1$, to the order of G and to the class number h_K of K. Then we pick a large enough number T divisible by $(l-1)$. Finally we pick a prime $\mathfrak{p}$ of F of degree T which splits completely in N. Let $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ denote primes of K lying above it. We have:

Lemma 3.14. *In the above settings there exists cyclic ramified extension L_l of K of degree l ramifing only at $\mathfrak{b}_1$.*

Proof. Consider the modulus $\mathfrak{m} = \mathfrak{b}_1$ and associated ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$. We will show this group has a subgroup of order l. Let $\mathcal{O}_K$ denotes the ring of integers of K with respect to the field extension K/F. Class field theory shows that we have the following exact sequence of abelian groups:

$$0 \to \mathbb{F}_q^* \to (\mathcal{O}_K/\mathfrak{m})^* \to \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Cl}(K) \to 0,$$

We claim that $\mathrm{Cl}_{\mathfrak{m}}(K)$ contains a subgroup of order l and since l is prime to the order of $\mathrm{Cl}(K)$ the fixed field corresponding to this subgroup is ramified at $\mathfrak{b}_1$.

Indeed the order of $(\mathcal{O}_K/\mathfrak{m})^*$ is $N(\mathfrak{b}_1) - 1 = q^T - 1$, where $N(\mathfrak{a})$ denotes the norm of an ideal $\mathfrak{a}$. Since T is divisible by $(l-1)$ this quantity is divisible by l. It follows that the order of $\mathrm{Cl}_m(K)$ is divisible by l and therefore we have a cyclic extension of K of degree l which ramifies only at $\mathfrak{b}_1$. □

The next step is to take the common normal closure M of N and L_l.

Lemma 3.15. *The Galois group $\mathrm{Gal}(M/F)$ of the common normal closure M of N and L_l over F is $C_l^n \rtimes G$.*

Proof. By construction N is normal over F and $K = N^H$. Consider the set $\mathrm{Hom}(K, N)$ of all embeddings of K into N. This has an action of G on it isomorphic to the action of G on G/H. For each element $\sigma_i \in \mathrm{Hom}(K, N)$ consider the field K^{σ_i} and corresponding cyclic extension $L^{\sigma_i} = L \otimes_{K^{\sigma_i}} N$. We claim that the composites NL^{σ_i} are linearly disjoint over N when σ_i runs over the set $\mathrm{Hom}(K, N)$. Indeed, consider the set of primes of N which lie over $\mathfrak{p}$ and ramify in the composite NL^{σ_i} over N. Since $H^{\sigma_i} = \mathrm{Gal}(M/K^{\sigma_i})$ fixes K^{σ_i} this set is invariant under the action of H^{σ_i} and not invariant under the action of g for each $g \in G$, $g \notin H^{\sigma_i}$. Hence all NL^{σ_i} ramifies in different primes of N lying above $\mathfrak{p}$. Therefore we have n disjoint C_l-extensions

NL^{σ_i}/N in M and G permutes them as cosets G/H. It follows that we have the following exact sequence:

$$1 \to C_l^n \to \mathrm{Gal}(M/F) \to G \to 1$$

Since the order of G is co-prime to l, by the Schur–Zassenhaus theorem see [43], we have a section from $\gamma : G \to \mathrm{Gal}(M/F)$ which means that this sequence splits and $\mathrm{Gal}(M/F) \simeq C_l^n \rtimes G$ as desired.

□

Chapter 4

L-functions of Genus two Abelian Coverings of Elliptic Curves over Finite Fields

4.1 Introduction

As we already mentioned the approach to arithmetical equivalence from the previous chapter has some disadvantages. For example it uses the map from the curve X to $\mathbb{P}^1$. In this chapter we introduce a different, in some sense more geometrical approach. Our main idea is to associate to a curve X the list of zeta-functions of abelian coverings of X. We expect to obtain some information about X from such a list.

4.1.1 Settings

Let $k = \mathbb{F}_q$ be a finite field with $q = p^n$, where p is prime, we will assume that $p > 3$ in all results. Let C be a curve over k and let d be a natural number prime to p. As usual by a curve we always mean smooth projective geometrically connected variety of dimension 1 over k. To such a curve one associates the set $\mathbb{X}_C(d, g)$ of all isomorphism classes of smooth projective abelian Galois covers of degree d and genus g:

Definition 4.1. *$\mathbb{X}_C(d, g)$ is the set of isomorphism classes of curves X defined over k, such that $g(X) = g$ and there exists an abelian(possibly ramified) Galois-covering $\phi : X \to C$, defined over k, and of degree d.*

On the function field level, any element X in $\mathbb{X}_C(d, g)$ corresponds to an abelian extension $k(X)$ of degree d of the field of functions $k(C)$ of C. Let us denote the Galois group $\mathrm{Gal}(k(X)/\ k(C))$ by G. According to the formalism of Artin's L-functions we have a decomposition law: the ratio of zeta-functions of X and C is equal to the product of all L-functions over all non-trivial characters of G.

Because of the interaction of algebraic geometry and the class field theory, we have a lot of explicit information about $\mathbb{X}_C(d, g)$. For instance, unramified geometrically connected abelian coverings of C are parametrized by subgroups of $\mathrm{Pic}^0(C)$, i.e. the group of $\mathbb{F}_q$-rational points on

the Jacobian variety $\mathrm{Jac}(C)$ and ramified coverings with ramification divisor dividing a divisor m are parametrized by subgroups of the ray-class group associated to m. We will discuss this in details in 4.2.2.

Let us consider the set of all zeta-functions $\zeta_X(T)$ of curves X in $\mathbb{X}_C(d,g)$. For any fixed C, d and g this is a finite set of functions. By a famous theorem of A. Weil, they are rational functions of the form

$$\zeta_X(T) = \frac{f_X(T)}{(1-T)(1-qT)},$$

where $f_X(T) \in \mathbb{Z}[T]$ is the Weil-polynomial of the covering curve X. Such a polynomial keeps a lot of information about X, for example we refer reader to the following classical theorem due to Honda and Tate, see [21]:

Theorem 4.2. *Let* $\mathrm{Jac}(X)$ *denote the Jacobian variety of the curve* X *over* $\mathbb{F}_q$*. Let* X' *denote another curve over* $\mathbb{F}_q$*. Then the following are equivalent:*

1. $\mathrm{Jac}(X)$ *and* $\mathrm{Jac}(X')$ *are* $\mathbb{F}_q$*-isogenous;*
2. *The Weil polynomials of* X *and* X' *are equal:* $f_X(T) = f_{X'}(T)$*.*

In this settings, suppose X is a $\mathbb{F}_q$-covering of C, then we have associated map between Jacobians: $\mathrm{Jac}(C) \to \mathrm{Jac}(X)$ and therefore $\frac{\zeta_X(T)}{\zeta_C(T)} = \frac{f_X(T)}{f_C(T)}$ is a polynomial with integer coefficients. In this chapter we consider the set $\Lambda_C(d,g)$ of all polynomials $\frac{f_X(T)}{f_C(T)}$ for $X \in \mathbb{X}_C(d,g)$.

Definition 4.3. *We define* $\Lambda_C(d,g) = \{\frac{f_X(T)}{f_C(T)} \in \mathbb{Z}[T] | X \in \mathbb{X}_C(d,g)\}$.

It is a remarkable fact that in the case $d = 2$ any element in $\Lambda_C(2,g)$ is the unique Artin L-function which corresponds to the unique non-trivial representation of the Galois group of fields extension $\mathbb{F}_q(X)$ over $\mathbb{F}_q(C)$. This explains the relation with our original motivation given in the previous chapter.

In this chapter we study $\Lambda_C(d,g)$, where $C = E$ is an elliptic curve and $g = 2$. In other words, we study zeta-functions of genus two abelian coverings of elliptic curves.

4.1.2 Results

Let E be an elliptic curve defined over $\mathbb{F}_q$ with $q = p^n$, p is prime and $p > 3$. In our research we obtain complete information about the set $\Lambda_E(d,2)$. It turned out that there are two different possibilities: $d = 2$ and $d > 2$. First we state the following corollary of Galois theory combining with the Riemann-Hurwitz theorem:

Theorem 4.4. *For* $d > 2$ *we have* $\Lambda_E(d,2) = \emptyset$*.*

Proof. See section 4.3. □

Our main result is the theorem for the case $d = 2$. For the sake of shortness here we formulate our result for the case $q = p$. Before we formulate it we need to introduce some notations. Let us denote $a_p = p + 1 - \#E(\mathbb{F}_p)$. For a given elliptic curve E as above we also define the following sets of polynomials:

1. $A_E = \{(pT^2 - a'_pT + 1)$, for a'_p with $|a'_p| \leq 2\sqrt{p}$, $a'_p = a_p \bmod (2)\}$;
2. $B_E = \{(pT^2 - a'_pT + 1)$, for a'_p with $|a'_p| \leq 2\sqrt{p}$, $a'_p = a_p \bmod (4)\}$.

In the above notations we will prove the following:

Theorem 4.5. *Assume that $j(E) \neq 0, 1728$. The following holds:*

1. if $E(\mathbb{F}_p)[2] \not\simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) = A_E$;
2. if $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) = B_E$;

This theorem says that there are only three distinct possibilities for $\Lambda_E(2,2)$. Moreover, which case occurs is completely determined by the structure of $\mathbb{F}_p$-rational 2-torsion points on E. The same results hold for curves with $j(E) = 0$ or $j(E) = 1728$ but with possibly a few exceptions in this list:

Theorem 4.6. *Assume that $j(E) = 0$ or 1728. The following holds:*

1. if $E(\mathbb{F}_p)[2] \not\simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) \subset A_E$; moreover, the number of elements in the difference does not exceed six: $|A_E/\Lambda_E(2,2)| \leq 6$;
2. if $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2) \subset B_E$; moreover, the number of elements in the difference does not exceed six: $|B_E/\Lambda_E(2,2)| \leq 6$;

During the proof we will provide explicit geometric criteria how to find all possible exceptions. Also we will explain how to extend those results to the case $q = p^n$, with $n > 1$. Roughly speaking for a general field, we also have three different cases depending on the group structure on $E(\mathbb{F}_q)[2]$, but now we have a little bit more restrictions on possible values of a'_q: for details see section 4.2.6. The proof is based on some classical results concerning geometry of bi-elliptic curves. More concretely, the main ingredient in our proof is the following result:

Theorem 4.7. *We have a surjective map from the set of pairs (E', α) to the set $\Lambda_E(2,2)$, where E' is an elliptic curve over $\mathbb{F}_q$ and $\alpha : E[2] \simeq E'[2]$ is an isomorphism between Galois module structure on two-torsion points of E and E', such that α is not the restriction of a geometric isomorphism between E and E'.*

The chapter has the following structure: in the next section we show and explain some experimental data for elliptic curves over $\mathbb{F}_5$. Next we will show how to prove our theorem for $d = 2$. Then we will explain cases $d > 2$.

4.2 Explanations, calculations and examples

In this section we are going to study the set $\Lambda_E(2,2)$ for an elliptic curve E defined over $\mathbb{F}_q$. Note that any degree 2 covering is actually a Galois covering. Hence, we could use a well-known geometric theory. A good reference here is [17].

4.2.1 Preliminares

Let E be an elliptic curve over $\mathbb{F}_q$, with characteristic $p > 3$. Let C be a curve of genus $g(C) = 2$ together with the covering map $\phi : C \to E$ of degree 2. Such a curve is called a biellptic curve.

Example 4.8. *If E is given by the affine equation $y^2 = x^3 + ax + b$, then one could take C with affine part defined by $v^2 = u^6 + au^2 + b$ and map $\phi : (x, y) \to (u^2, v)$.*

Since we have a morphism ϕ we have associated map of Jacobian varieties: $\mathrm{Jac}(E) \to \mathrm{Jac}(C)$. Moreover, because $\dim(\mathrm{Jac}(C)) = 2$ we have:

Theorem 4.9. *The curve C is bielliptic covering of E if and only if the Jacobian variety $\mathrm{Jac}(C)$ of the curve C is (2,2)-isogenous to a product of two elliptic curves $E \times E'$.*

In the assumptions of the theorem it is not difficult to provide explicit construction of E'. Namely, since C is a hyper-elliptic we have a unique involution $\tau \in \mathrm{Aut}(C)$, such that $C/\langle\tau\rangle \simeq \mathbb{P}^1$. Since it is unique it lies in the center of $\mathrm{Aut}(C)$. Let us denote by σ the element of $\mathrm{Aut}(C)$ such that $C/\langle\sigma\rangle \simeq E$. By our assumption it also has order two. Consider the curve $E' = C/\langle\sigma\tau\rangle$. Now we have $(\sigma\tau)^2 = \sigma\tau\sigma\tau = \sigma^2\tau^2 = 1$, so we have a degree two map $\phi' : C \to E'$. Note that $E' \not\simeq \mathbb{P}^1$, since otherwise we have $\sigma = \mathrm{id}$. Then, by Riemann-Hurwitz E' is an elliptic curve. Note, that we have the following commutative diagram:

$$\begin{array}{ccc} C & \longrightarrow & E' \simeq C/\langle\sigma\tau\rangle \\ \downarrow & & \downarrow \\ E \simeq C/\langle\sigma\rangle & \longrightarrow & \mathbb{P}^1 \end{array}$$

Finally, we claim that $E \times E'$ is (2,2)-isogenous to the Jacobian surface of C. For the proof and complete discussion see [24] or [15].

Now, according to Tate's theorem mentioned in the previous section we have the following relation between Weil polynomials:

$$f_C(T) = f_E(T) f_{E'}(T) = (qT^2 - a_q T + 1)(qT^2 - a'_q T + 1),$$

where $a_q = q + 1 - \#E(\mathbb{F}_q)$ and $a'_q = q + 1 - \#E'(\mathbb{F}_q)$. So, to describe $\Lambda_E(2, 2)$ it is enough to find all possible values of a'_q.

In other words we just proved the following result:

Theorem 4.10. *There exists a surjective map from the set $\Lambda_E(2, 2)$ to the set of numbers a'_q with property that there exists an elliptic curve E' with $a'_q = q + 1 - \#E'(\mathbb{F}_q)$ and with property that abelian surface $E \times E'$ is (2,2)-isogenous to the Jacobian surface of smooth projective curve C defined over $\mathbb{F}_q$.*

4.2.2 An example over $\mathbb{F}_5$

Let us take $q = p = 5$. Our task, for any given curve E find all possible values of a'_5 as in the above discussion. In order to do that first of all we have to pick a ramification divisor M

Table 4.1: Data for all elliptic curves over $\mathbb{F}_5$

Curve E	j-invariant	a_5	Values of a'_5	IsSupersingular	$\#\operatorname{Aut}_k(E)$
$y^2 = x^3 + 1$	0	0	$0; \pm 2; \pm 4$	true	2
$y^2 = x^3 + 2$	0	0	$0; \pm 2; \pm 4$	true	2
$y^2 = x^3 + x$	3	2	± 2	false	4
$y^2 = x^3 + x + 2$	1	2	$0; \pm 2; \pm 4$	false	2
$y^2 = x^3 + x + 1$	2	-3	$\pm 1; \pm 3$	false	2
$y^2 = x^3 + 2x$	3	4	$0; \pm 2$	false	4
$y^2 = x^3 + 2x + 1$	4	-1	$\pm 1; \pm 3$	false	2
$y^2 = x^3 + 3x$	3	-4	$0; \pm 2$	false	4
$y^2 = x^3 + 3x + 2$	4	1	$\pm 1; \pm 3$	false	2
$y^2 = x^3 + 4x$	3	-2	± 2	false	4
$y^2 = x^3 + 4x + 1$	1	-2	$0; \pm 2; \pm 4$	false	2
$y^2 = x^3 + 4x + 2$	2	3	$\pm 1; \pm 3$	false	2

on E of genus two quadratic cover of E. By Riemann-Hurwitz theorem M is of degree two. Then by taking the maximal abelian extension which corresponds to this divisor we obtain a parametrization for all genus two coverings with given ramification data. More concretely from the class field theory we have the following isomorphism:

$$\phi\colon \operatorname{Pic}^0_M(E) \to \operatorname{Gal}(F_M/F)$$

Here, $F = \mathbb{F}_p(E)$ is the function field of E, F_M is the *Ray class field* corresponding to the pair (F, M) and $Pic^0_M(E)$ is the ray class group associated to M. Hence in order to list all bi-elliptic coverings of E it is enough to list all possible M and for each such M calculate all possible abelian sub-extensions of genus two. By doing that, for any E we provide list of all possible a'_5 and compare it with other invariants of E. We implement our calculations by using Magma computer algebra system. Note that $1728 = 3 \mod (5)$ and hence in case $p = 5$ we use both values for $j(E)$. Also note that in the table we list isomorphism classes of curves over $k = \mathbb{F}_5$, not over $\overline{\mathbb{F}_5}$.

4.2.3 Observations

From the data provided by the above table one could note that there exist to different patterns: a_p is odd or even. This is not very difficult to explain:

Lemma 4.11. *For any fixed E over $\mathbb{F}_q$, if $(qT^2 + a'_qT + 1) \in \Lambda_E(2, 2)$ then $a_q = a'_q \bmod (2)$.*

Proof. Consider the covering $\phi : C \to E$ of degree two. From Riemann-Hurwitz theorem we have that ramification divisor of ϕ has to be degree two, so it is either a sum of two points of degree one, or a one point of degree two. Here we use the fact that $p > 2$ and we don't have so-called wild-ramification. Since ϕ is of degree two, we get the number of $\mathbb{F}_q$-points on C is even. From the decomposition of the Weil polynomial we have $q + 1 - \#C(\mathbb{F}_q) = q(a_q + a'_q)$. Now, just take last equality modulo two and use the fact that q is odd. □

A second remarkable thing is a some sort of symmetry: if a'_p occurs then also $(-a'_p)$ is in the list. We will explain this phenomena later, but now we note that this is related to quadratic twists of E. For proof, see corollary 4.17.

Finally, the last and the main observation is that for *general curve* these are the only restrictions. More contritely, one could note that if $j(E) \neq 0, 1728$ and $E(\mathbb{F}_p)[2]$ is not isomorphic to the full group $C_2 \oplus C_2$ then any $a'_p = a_p \bmod (2)$ occurs. But if $E(\mathbb{F}_p)[2] \simeq C_2 \oplus C_2$ then $\Lambda_E(2,2)$ consists of all $a'_p = a_p \bmod (4)$, still provided we are in the case $j(E) \neq 0, 1728$.

Also, the same result holds for E with $j(E) = 0, 1728$, but with possible up to 4 and 6 exceptions respectively, depending on which twists of E defined over $\mathbb{F}_p$. Later we will give explicit geometric criteria which answers if there are any exceptions in the list.

Example 4.12. *1. Consider the curve E defined by $y^2 = x^3 + x$. In this case $a_5 = 2$, $j(E) = 1728$ and it is easy to see that it has four rational two-torsion points: $(0,0)$, $(2,0)$, $(3,0)$ and ∞. According to our prediction the only values which may occurs are $\{\pm 2\}$. Which is indeed the case.*

2. Consider the curve E defined by $y^2 = x^3 + 1$. Here we have $a_5 = 0$, $j(E) = 0$ and $E(\mathbb{F}_5)[2] \simeq C_2$, generated by $(4,0)$. Then we predict that the following values occurs $\{0, \pm 2, \pm 4\}$. This coincides with our data.

3. Consider the curve E defined by $y^2 = x^3 + 3x$. Here we have $a_5 = -4$, $j(E) = 1728$ and $E(\mathbb{F}_5)[2] \simeq C_2$, generated by $(0,0)$. But the values ± 4 do not occur in our list. It happens because $j(E) = 1728$ and so in this case we have two exceptions.

4.2.4 The basic construction

A crucial fact in our investigation is the following construction due to Kani, see [25] and [21].

Let n be a prime number with $(n,p) = 1$. Given two elliptic curves E and E' over $\mathbb{F}_q$ with isomorphism α as Galois modules $E[n] \simeq E'[n]$, which is anti-isometry with respect to the Weil-paring. Let Γ_α be the graph of α in $E \times E'$. Consider surface $A_\alpha \simeq E \times E'/\Gamma_\alpha$. It is (n,n)-isogenous to $E \times E'$. Moreover, it turns out that it has *principal polarization* θ which comes from polarization on $E \times E'$:

$$\begin{array}{ccc} E \times E' & \xrightarrow{[n]} & \hat{E} \times \hat{E}' \\ \downarrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \hat{\phi}} \\ A_\alpha & \xrightarrow{\theta} & \hat{A}_\alpha \end{array}$$

According to the theorem of A.Weil [58]: the pair (A_α, θ) is a polarized Jacobain surface of some, possible not smooth curve C of (arithmetic) genus two.

Theorem 4.13. *The curve C constructed above is smooth if and only if the isomorphism α of Galois modules is not the restriction of a geometric isogeny ϕ of degree $d = i(n-i)$ between $E(\bar{k}) \to E'(\bar{k})$, with $0 < i < n$. Moreover, any smooth C such that $\mathrm{Jac}(C)$ is (n,n)-isogenous to $E \times E'$ appears in this way.*

In our case $n = 2$ and hence $i = 1$, but geometric isogeny of degree one is necessary geometric isomorphism, therefore we have:

Corollary 4.14. *There exists a surjective map $\Lambda_E(2,2)$ to the set of all a'_q such that there exists an elliptic curve E' over $\mathbb{F}_q$ with $a'_q = q + 1 - \#E'(\mathbb{F}_q)$ and an isomorphism α of Galois modules $E[2]$ and $E'[2]$ such that α is not the restriction of a geometric isomorphism between E and E'.*

By working with the Galois module structure on $E[2]$ we provide a proof of our main theorem.

4.2.5 On Galois Module Structure on $E[2]$

According to the previous section, we must understand which isomorphisms between Galois modules are not restrictions of geometric isomorphisms between curves. In order to do that in this section we briefly recall possible Galois module structures on $E[2]$ and its relations with $\mathrm{Aut}_{\bar{k}}(E)$.

Galois group $G_k \simeq \mathrm{Gal}(\bar{k}/k)$ is generated by the Frobenius element π. Hence we could restrict our attention to the action of π on $E[2]$. Recall that as abelian group $E[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. There are three possibilities for the Galois module structure on $E[2]$: either π is acting trivially or the action is by a 2-cycle or a 3-cycle. In the first case $E[2]$ has four rational points, in the second case only two and in the later case only one rational point, namely the zero point.

For a given pair of elliptic curves E, E' over $k = \mathbb{F}_q$ let us consider the set $\mathrm{Isom}_{\bar{k}}(E, E')$. If it is empty, then $j(E) \neq j(E')$ and any isomorphism between $E[2]$ and $E'[2]$ is not the restriction of a geometric isomorphism. Otherwise, suppose now that $\mathrm{Isom}_{\bar{k}}(E, E')$ is not empty. Then we have $j(E) = j(E')$ and $|\mathrm{Isom}_{\bar{k}}(E, E')| = |\mathrm{Aut}_{\bar{k}}(E)| = |\mathrm{Aut}_{\bar{k}}(E')|$. Now let $\mathrm{Isom}_{AG}(E[2], E'[2])$ be the set of isomorphisms between $E[2]$ and $E'[2]$ considered as abelian groups and $\mathrm{Isom}_G(E[2], E'[2])$ be the set of isomorphisms as Galois-modules. We have the following:

$$\mathrm{Isom}_{\bar{k}}(E, E') \to \mathrm{Isom}_{AG}(E[2], E'[2]) \supset \mathrm{Isom}_G(E[2], E'[2]),$$

where the map is just the restriction of automorphism to the two-torsion points.

Now we are going to investigate which elements of $\mathrm{Isom}_G(E[2], E'[2])$ do not come from restriction of elements of $\mathrm{Isom}_{\bar{k}}(E, E')$.

Recall that if $p > 3$ then we have exactly the following possibilities:

1. $j(E) \neq 0, 1728$ and $\mathrm{Aut}_{\bar{k}}(E) = \mathbb{Z}/2\mathbb{Z}$;
2. $j(E) = 0$ and E is given by $y^2 = x^3 + b$ and $\mathrm{Aut}_{\bar{k}}(E) = \mu_6$;
3. $j(E) = 1728$ and E is given by $y^2 = x^3 + ax$ and $\mathrm{Aut}_{\bar{k}}(E) = \mu_4$.

Therefore, $\#\mathrm{Isom}_{\bar{k}}(E, E')$ is either 0, 2, 4 or 6. Suppose $\#\mathrm{Isom}_{\bar{k}}(E, E')$ is not zero and hence we also have a bijective map from $\mathrm{Isom}_G(E[2], E'[2])$ to $\mathrm{Aut}_G(E[2]) = \mathrm{Isom}_G(E[2], E[2])$. Note that there are exactly three types of $\mathrm{Aut}_G(E[2])$:

1. If $E(\mathbb{F}_q)[2] = C_2 \oplus C_2$, then $\mathrm{Aut}_G(E[2]) \simeq \mathrm{Gl}_2(\mathbb{F}_2)$;

2. If $E(\mathbb{F}_q)[2] = C_2$, then $\mathrm{Aut}_G(E[2]) \simeq C_2$;

3. If $E(\mathbb{F}_q)[2] = \{0\}$, then $\mathrm{Aut}_G(E[2]) \simeq C_3$.

Theorem 4.15. *Given two geometrically isomorphic elliptic curves E and E' defined over $\mathbb{F}_q$, we have that every element of $\mathrm{Isom}_G(E[2], E'[2])$ is the restriction of a geometric isomorphism if and only if one of the following pair of conditions holds:*

1. *$j(E) = j(E') = 0$ and $E(\mathbb{F}_q)[2] = \{0\}$ and E is a quadratic twist of E';*

2. *$j(E) = j(E') = 1728$ and $E(\mathbb{F}_q)[2] \simeq C_2$ and E is a quadratic twist of E'.*

Proof. Suppose $j(E) = j(E') \neq 0, 1728$. Let us fix any $\bar{k}$-isomorphism $\phi : E \to E'$. Then $\mathrm{Isom}_{\bar{k}}(E, E') = \{\pm\phi\}$. But then, every element in $\mathrm{Isom}_{\bar{k}}(E, E')$ acts trivially on two-torsion points and hence there exists at most one element in $\mathrm{Isom}_G(E[2], E'[2])$ which is the restriction of geometric isomorphism. On the other hand, we always have more than one isomorphism of Galois module structure between $E[2]$ and $E'[2]$.

Suppose $j(E) = j(E') = 0$. In this case E can be given by $y^2 = x^3 + b$ and E' is given by $y^2 = x^3 + b'$. Let us fix $t \in \bar{k}$ such that $t^6 = \frac{b'}{b}$. Consider a map $\phi : E \to E'$ such that $\phi(x, y) = (t^2x, t^3y)$. Let us fix an element $\rho \in \bar{k}$, $\rho \neq 1$, such that $\rho^3 = 1$. And let us denote by $[\rho]$ the following element of $\mathrm{Aut}(E)$, namely $[\rho](x, y) = (\rho x, y)$. Then $\mathrm{Isom}_{\bar{k}}(E, E') = \{\pm\phi, \pm\phi[\rho], \pm\phi[\rho]^2\}$. By restricting these maps to the maps from $E[2] \to E'[2]$ we obtain three different maps, say $\{1, \tau, \tau^2\}$, since as before $\pm$ acts identically on two-torsion points. Now, two torsion points of E' are $\{\infty, (c, 0), (\rho c, 0), (\rho^2 c, 0)\}$, where c is any root of the equation $x^3 + b' = 0$. Therefore, if $E(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$ or $E(\mathbb{F}_q)[2] \simeq C_2$, then we have an element in $\mathrm{Isom}_G(E[2], E'[2])$ which is not the restriction of a geometric isomorphism. Finally, suppose that $E(\mathbb{F}_q)[2] = \{0\}$. In this case it is easy to see that each element of $\mathrm{Isom}_G(E[2], E'[2])$ is the restriction of an element of $\mathrm{Isom}_{\bar{k}}(E, E')$ if and only if $(t^2)^p = t^2$ which is equivalent to the fact that $\frac{b}{b'}$ is a cube in $\mathbb{F}_p$. Or in other words that E is a quadratic twist of E'.

Finally, suppose we are in the case $j(E) = j(E') = 1728$. Then E can be given by $y^2 = x^3 + bx$ and E' is given by $y^2 = x^3 + b'x$. Two-torsion points of E are $\{\infty, (0, 0), (\sqrt{-b}, 0), (-\sqrt{-b}, 0)\}$. Note then the point $(0, 0)$ is always a rational point on $E($ and $E')$, hence $E(\mathbb{F}_q)[2]$ is either C_2 or $C_2 \oplus C_2$. Let us fix an element $i \in \bar{k}$ such that $i^2 = -1$. We will denote by $[i]$ the following automorphism of E: $[i](x, y) = (-x; iy)$. Let us also fix an element $t \in \overline{\mathbb{F}_p}$ such that $t^4 = \frac{b'}{b}$ and the following geometric isomorphism ϕ from $E \to E'$ which sends (x, y) to (t^2x, t^3y). Then $\mathrm{Isom}_{\bar{k}}(E, E') = \{\pm\phi, \pm[i]\phi]\}$. Restriction to two-torsion points gives us two different elements. If $E(\mathbb{F}_q)[2] \simeq C_2$, then any element of $\mathrm{Isom}_G(E[2], E'[2])$ is the restriction of an element of $\mathrm{Isom}_{\bar{k}}$ if and only if $t^2 \in \mathbb{F}_p$ or, in other words, $\frac{b'}{b}$ is a square in $\mathbb{F}_p$. The last statement is equivalent to the fact that E is a quadratic twist of E'. In contrast, if $E(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$, then we could always pick an isomorphism of the Galois module structure on two-torsion points which is not the restriction of a geometric isomorphism. □

4.2.6 The Proof for the case $d = 2$

In this section we give a proof of our main theorem. First, we prove a few auxiliary lemmas.

Lemma 4.16. *Every quadratic twists E' of an elliptic curve E share isomorphic Galois module structure of two-torsion points and has opposite trace of Frobenius.*

Proof. For the first statement note that Galois structure of the two-torsion points completely determined by the roots of polynomial $f(x)$, where the elliptic curve E is given by the equation $y^2 = f(x)$. Now, one could check that quadratic twist of E is given by $y^2 = d * f(x)$, where $d \in \mathbb{F}_q^*/\mathbb{F}_q^{*2}$. Hence $E'[2]$ is isomorphic to the $E[2]$ as Galois module. For the second statement of the proposition note that $\#E(\mathbb{F}_q) + \#E'(\mathbb{F}_q) = 2q + 2$ and hence $a_q = -a'_q$. □

By using this lemma we obtain the following:

Corollary 4.17. *Suppose $pT^2 - a'_pT + 1$ is in $\Lambda_E(2, 2)$. Then also $pT^2 + a'_pT + 1$ is.*

Proof. If $-a'_p$ occurs in the list, then there exists an elliptic curve $E_1^{'}$ with isomorphism between $E_1^{'}[2]$ and $E[2]$, which is not the restriction of a geometric isomorphism between $E_1^{'}$ and E. Then we could take $E_2^{'}$ which is the quadratic twist of $E_1^{'}$. It has the same Galois-module structure and negative sign of Frobenius. Obviously, we have isomorphism between $E_2^{'}[2]$ and $E[2]$, which is not the restriction of a geometric isomorphism between $E_2^{'}$ and E. □

The following result is useful for our purposes.

Lemma 4.18. *a_q is odd if and only if π acts as C_3 on $E[2]$.*

Proof. Frobenius element π acts on $E[2]$ as three-cycle if and only if it has exactly one fixed point, namely the zero-point. It happens if and only if $E(\mathbb{F}_q)$ is not divisible by two. But $a_q = q + 1 - \#E(\mathbb{F}_q)$, which shows that a_q is even if and only if π acts as C_3. □

Definition 4.19. *Fix a finite field $\mathbb{F}_q$. Let N be an integer number in the Hasse interval: $N \in [-2\sqrt{q}; 2\sqrt{q}]$. We will call it admissible if there exists an elliptic curve E over $\mathbb{F}_q$ with $q + 1 - \#E(\mathbb{F}_q) = N$.*

The following lemma is the classical statement due to Waterhouse, for reference see [45].

Theorem 4.20. *The number N is admissible if and only if one of the following conditions holds:*

1. $\gcd(p, N) = 1$;
2. *$q = p^{2n+1}$, $n \in \mathbb{N}$ and one of the following holds:*
   (a) *N=0;*
   (b) *$N = \pm 2^{n+1}$ and $p = 2$;*
   (c) *$N = \pm 3^{n+1}$ and $p = 3$;*
3. *$q = p^{2n}$, $n \in \mathbb{N}$ and one of the following holds:*
   (a) *$N = \pm 2p^n$;*
   (b) *$N = \pm p^n$ and $p \neq 1 \mod (3)$;*

(c) $N = 0$ *and* $p \neq 1 \mod (4)$*;*

Remark 4.21. *Suppose* $q = p$ *and* $p > 3$*. Then we have* $|a'_p| \leq 2\sqrt{p} < p$ *and hence a condition* $\gcd(a'_p; p) = 1$ *is automatically holds. Hence, in this settings any number* N *in the Hasse interval is admissible.*

Combing these results together we already have one cases of our theorem for case $q = p$:

Corollary 4.22. *Let* E *be an elliptic curve over* $\mathbb{F}_p$ *with* $j(E) \neq 0$ *and* $a_p = 1 \mod (2)$*. Then* $\Lambda_E(2, 2)$ *consists of all polynomials of the form* $pT^2 - a'_pT + 1$*, with* $a'_p \in [-2\sqrt{p}; 2\sqrt{p}]$ *such that* $a'_p = 1 \mod (2)$*. If* $j(E) = 0$ *the same result holds, with up to 6 exceptions.*

Proof. Suppose $j(E) \neq 0, 1728$. Given a'_p as above we could construct an elliptic curve E' with $\#E'(\mathbb{F}_q) = q + 1 - a'_p$, by the previous remark. Now, since $a'_p = 1 \mod (2)$, by corollary 4.18 there exists isomorphism as Galois-modules between $E[2]$ and $E'[2]$. We have to check that it possible to pick an isomorphism of Galois-modules which is not the restriction of a geometric isomorphism between E and E'. This is possible, because of discussion in Theorem 4.15.

If $j(E) = 1728$, then we have at least one rational 2-torsion point, namely $(0, 0)$ hence this is not the case.

If $j(E) = 0$ then for any given a'_p we still could pick an elliptic curve E' and find an isomorphism of Galois-module structure. If $j(E') \neq 0$ then any such an isomorphism is not the restriction of a geometric isomorphism. Otherwise if $j(E') = j(E) = 0$ then according to Theorem 4.15 in this case any isomorphism between two-torsion parts comes from the restriction of a geometric isomorphism if and only if E is a quadratic twist of E'. This implies that all the exceptions which could occur, come from twists of E, but there are no more than six twists of elliptic curve defined over k. □

Remark 4.23. Note that even if E' is geometrically isomorphic to E, then it *does not* imply that a'_p does not occur in $\Lambda_E(2, 2)$, because it may happen that in the isogeny class associated to a'_p there is a curve E'' which is not geometrically isomorphic to E, but with isomorphism of Galois modules $E[2]$ and $E''[2]$. According to our data this happens very often.

Remark 4.24. There is an obvious generalization to the case $q = p^n$ with $n > 1$. Namely, we must pick an *admissible* a'_q with $a'_q = 1 \mod (2)$ and take an elliptic curve E'. Then, by the same reason there exists an isomorphism of Galois module structure on two-torsion points not coming from a geometric isomorphism between curves, except cases where $j(E') = j(E) = 0$.

The case that a_q is even is a little bit more delicate. The reason is that we have two possibilities for $E(\mathbb{F}_p)[2]$. It is either C_2 or $C_2 \oplus C_2$.

Namely, suppose we are in the case $a_q = 0 \mod (2)$. Since q is odd, It also means that $\#E(\mathbb{F}_q) = 0 \mod (2)$. There are two different cases:

1. $\#E(\mathbb{F}_q) = 0 \mod (4)$, hence $E(\mathbb{F}_q)[2] \simeq C_2$ or $E(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$;

2. $\#E(\mathbb{F}_q) = 2 \mod (4)$, hence $E(\mathbb{F}_q)[2] \simeq C_2$;

We see a problem here, because *a priori* given an isogeny class of an elliptic curve E with $\#E(\mathbb{F}_q) = 0 \mod (4)$, we can't decide whether there exists curve E' in the same isogeny class with $E'(\mathbb{F}_q)[2] \simeq C_2$ or with $E'(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$. In order to solve this problem, we need two lemmas about two-torsion points on elliptic curves in the isogeny class of given elliptic curve E:

Lemma 4.25. *Suppose E is an elliptic curve over $k = \mathbb{F}_q$ such that $4 \mid \#E(\mathbb{F}_q)$. If $E(\mathbb{F}_q)[2] = C_2$ then there exists an elliptic curve E' defined over k with two properties:*

1. *E' is $\mathbb{F}_q$-isogenous to E;*
2. *$E'(\mathbb{F}_q)[2] = C_2 \oplus C_2$.*

Proof. Since $4|\#E(\mathbb{F}_q)$ and $E(\mathbb{F}_q)[2] = C_2$ we have that $E(\mathbb{F}_q)[4] = C_4$. We denote by P a generator of this group. We have $E[2] = \{0, 2P, M, M + 2P\}$, where M is a non-rational two-torsion point of E. Note that $\pi(M) = M + 2P$. Consider $H = \langle 2P \rangle$ and elliptic curve $E' = E/\langle H \rangle$. Obviously, E' is isogenous to E. We claim that $E'[2] = C_2 \oplus C_2$. Indeed, consider the equation $2R = 2P$, it has exactly four solutions $\{P, 3P, P + M, 3P + M\}$. Let us denote the map $E \to E/\langle H \rangle$ by i. Then $i(P), i(P + M)$ are two different non-trivial two-torsion points on E'. We claim that π acts trivially on both $i(P)$ and $i(P + M)$. Indeed,

$$i(P) = i(\pi(P)) = \pi i(P)$$

and

$$\pi(i(P + M)) = i(P + \pi(M)) = i(P + 2P + M) = i(P + M).$$

But if π acts trivially on two non-zero elements of $E'[2]$ then it acts trivially on all points of $E'[2]$. □

Recall, that for any elliptic curve E over $\mathbb{F}_q$ and prime number $l \neq p$, we associate the Tate module $T_l(E) = \varprojlim_k (E[l^k])$. Now, π acts on points of E and therefore acts on $T_l(E)$.

Lemma 4.26. *Suppose E is an elliptic curve over $k = \mathbb{F}_q$ such that $4 \mid \#E(\mathbb{F}_q)$. If $E(\mathbb{F}_q)[2] = C_2 \oplus C_2$, then the following are equivalent:*

1. *There exists an elliptic curve E' with $E'(\mathbb{F}_q)[2] = C_2$ and k-isogenous to E;*
2. *$\pi \in \mathrm{Aut}(T_2(E))$ is not in $\mathbb{Z}_2^*$;*
3. *$a_q \neq \pm 2\sqrt{q}$.*

Proof. First we will prove equivalence between one and two.

Suppose π acts as an 2-adic integer, then any finite 2-subgroup H of $E(\overline{\mathbb{F}_q})$ is rational. Now for any E' that is k-isogenous to E, there exists finite rational subgroup $H \subset E(\overline{\mathbb{F}_q})$ such that $E' \simeq E/H$. Let H_1 be a maximal group such that $H \subset H_1$ and H is of index two inside H_1. Consider $H_1/H \subset E/H \simeq E'$. Since H_1/H is a 2-subgroup, then π acts trivially on it. On the other hand $E'[2] \simeq H_1/H$, it means that $E'[2]$ is rational.

Suppose π is not in $\mathbb{Z}_2^*$. It means that there exists $P \in T_2(E)$, $P = (P_1, P_2, \dots)$, $P_i \in E[2^i]$ such that $\pi(P) \notin \langle P \rangle$. Since $\pi(P_1) = P_1$, there exists number i such that $\pi(P_i) \in \langle P_i \rangle = H$,

but $\pi(P_{i+1}) \notin \langle P_{i+1} \rangle = H_1$. It means that elliptic curve $E' \simeq E/H$, which is isogenous to E has a non-rational two-torsion point, namely $P_{i+1} \mod H$.

Finally we will show that (2) is equivalent to (3). Suppose π acts as an element of $\mathbb{Z}_2^*$, meaning that in some basis of $T_2(E)$ it acts as a scalar matrix. Its characteristic polynomial is $f(x) = x^2 - a_q x + q$, which is of the form $f(x) = (x \pm \sqrt{q})^2$ when π is a scalar. This shows that $a_q = \pm 2\sqrt{q}$. Suppose $a_q = \pm 2\sqrt{q}$, then we know that the characteristic polynomial of π is $f(x) = (x \pm \sqrt{q})^2$. Now we claim that the minimal polynomial of π is $x \pm \sqrt{q}$. Indeed, we have the following sequence:

$$E(\overline{\mathbb{F}_q}) \xrightarrow{\pi \pm \sqrt{q}} E(\overline{\mathbb{F}_q}) \xrightarrow{\pi \pm \sqrt{q}} E(\overline{\mathbb{F}_q})$$

Where the composition of two maps is zero, since the minimal polynomial divides the characteristic polynomial. But, this is the map between two projective curves over algebraically closed field, which means that it is either zero or surjective map. If $(\pi \pm \sqrt{q})$ is not zero map, then also $(\pi \pm \sqrt{q})^2$. Therefore the minimal polynomial of π is $(x \pm \sqrt{q})$, which means that π is a diagonal matrix.

□

Combining this two results together we have the following theorem:

Theorem 4.27. *Given elliptic curve E over $\mathbb{F}_q$ such that $4 | \#E(\mathbb{F}_q)$ we have:*

1. *if $a_q \neq \pm 2\sqrt{q}$, then in the isogeny class corresponding to E there exist elliptic curves E', E'' with $E'(\mathbb{F}_q)[2] = C_2$ and $E''(\mathbb{F}_q)[2] = C_2 \oplus C_2$;*
2. *if $a_q = \pm 2\sqrt{q}$, then any elliptic curve E' isogenous to E has $E'(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$.*

Corollary 4.28. *Suppose, E is an elliptic curve with $j(E) \neq 1728$ and with $E(\mathbb{F}_q)[2] = C_2$. Then $\Lambda_E(2,2)$ consists of all $qT^2 - a'_q T + 1$ for all admissible a'_q with property $a'_q = 0 \mod (2)$ and $a_q \neq \pm 2\sqrt{q}$. If $j(E) = 1728$ the same result holds with possibly four exceptions.*

Proof. Suppose $j(E) \neq 0, 1728$. As before, for a given admissible number a'_q we could construct an elliptic curve E'. Condition $a'_q = 0 \mod (2)$ implies that either $E'(\mathbb{F}_q)[2] \simeq C_2$ or $E'(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$. If $\#E'(\mathbb{F}_q) = 2 \mod (4)$ we are done because then $E'(\mathbb{F}_q)[2] = C_2$ and theorem 4.15. If $\#E'(\mathbb{F}_q) = 0 \mod (4)$, then we are done because of theorem 4.27.

If $j(E) = 0, 1728$, then we only have problems with $j(E) = j(E')$, but then theorem 4.15 shows that only possible exceptions could appear in the case $j(E) = 1728$. This exceptions one-to-one correspond to twists of E, but there are no more than 4 twists of an elliptic curve E with $j(E) = 1728$. □

Corollary 4.29. *Suppose, E is an elliptic curve with $E(\mathbb{F}_q)[2] = C_2 \oplus C_2$. Then $\Lambda_E(2,2)$ consists of all $qT^2 - a'_q T + 1$ for all admissible a'_q with property $q + 1 - a'_q = 0 \mod (4)$.*

Proof. First note that this condition mentioned above guarantees that for given a'_q there exists an elliptic curve E'' in the corresponding isogeny class and as before by theorem 4.27 in this isogeny class we could construct elliptic curve E' with $E'(\mathbb{F}_q)[2] \simeq C_2 \oplus C_2$. According to theorem 4.15 for any such pair of E and E' we could construct isomorphism between $E[2]$ and $E'[2]$ which is not the restriction of a geometric isomorphism. □

4.3 The case $d > 2$

The main purpose of this section is to show:

Theorem 4.30. *For $d > 2$ with $p \not| d$, we have $\Lambda_E(d, 2) = \emptyset$.*

Proof. We will show, that there is no abelian Galois coverings of an elliptic curve by a genus two smooth projective curve of degree $d > 2$, provided that the characteristic of the base field is prime to d. Without loss of generality we could suppose k is algebraically closed.

Suppose that C is an abelian covering of E of degree $d > 2$. As we already mentioned there exists a unique involution $\tau \in \mathrm{Aut}(C)$ such that $C/\langle\tau\rangle \simeq \mathbb{P}^1$. Moreover, because τ is unique, it lies in the center of $\mathrm{Aut}(C)$ and hence we have the following commutative diagram:

$$\begin{array}{ccc} C & \xrightarrow{2} & \mathbb{P}^1 \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} \\ E & \xrightarrow[2]{} & \mathbb{P}^1 \end{array}$$

Note that *all maps here are abelian Galois coverings*: $C \to E$ is by our assumptions, the shorter morphism $C \to \mathbb{P}^1$ since it has degree 2 and the longer $C \to \mathbb{P}^1$ is abelian covering because of Galois theory.

Let us apply Riemann-Hurwitz theorem to the covering $C \to E$. We have

$$(2g_C - 2) = d(2g_E - 2) + \sum_{p \in C}(e_p - 1),$$

and hence

$$\sum_{p \in C}(e_p - 1) = 2.$$

Since by assumptions this is a Galois-covering, this means that there are only three possibilities for the ramification divisor: either we have ramification in one point of E of type $(e_1, e_2) = (2, 2)$, two different points on E with ramification index $e_i = 2$ or ramification exactly at one point with ramification index $e_1 = 3$. In the first case we have $d = 4$, in the second we have $d = 2$ and finally, in the last case we have $d = 3$. This proves, that $d \leq 4$. Note that if $d = 2$ or $d = 3$ then the Galois-group of a covering $C \to E$ is cyclic. But if $d = 4$ then the Galois group is either C_4 or $C_2 \oplus C_2$.

Now, suppose $d = 3$. Consider the map $C \to \mathbb{P}^1$ which is of degree six. Riemann-Hurwitz for this covering tells us :

$$2 = 6(-2) + \sum_{p \in C}(e_p - 1),$$

which implies $\sum(e_p - 1) = 14$. Now since we have Galois covering of degree six, the only possible ramification types are 6, $(3, 3)$ and $(2, 2, 2)$. Suppose we have m_i points of i-th ramification type. It implies that $5m_1 + 4m_2 + 3m_1 = 14$, but this equation has only three solutions in

non-negative integers: $(2,1,0)$, $(1,0,3)$ and $(0,2,2)$. Riemann-Hurwitz for the covering $C \to E$ gives us:

$$(2) = 0 + \sum_{p \in C}(e_p - 1),$$

which implies that the only possible ramification index is (3) with ramification exactly at one point. This excludes possibilities $(2,1,0)$ and $(0,2,2)$ because they both have at least two points on C with ramification index divisible by 3. Now, consider the covering $\mathbb{P}^1 \to \mathbb{P}^1$ of degree 3. Riemann-Hurwitz for this case:

$$-2 = -6 + \sum_{p \in \mathbb{P}^1}(e_p - 1),$$

or $4 = \sum(e_p - 1)$, which implies that we must have two points with ramification index (3). But then the covering $C \to \mathbb{P}^1$ of degree six must have at least two points with ramification index divisible by three. This provides contradiction to the case $(1,0,3)$ which has only one point with ramification index divisible by three.

The last case is $d = 4$. Suppose that the Galois group is $C_2 \oplus C_2$. It implies that there are two different elements σ, τ of $\mathrm{Aut}(C)$ each of order two such that there exist two curves $X \simeq C/\langle\sigma\rangle$ and $Y \simeq C/\langle\tau\rangle$ and the following commutative diagram:

$$\begin{array}{ccc} C & \xrightarrow{2} & X \\ \downarrow{\scriptstyle 2} & & \downarrow{\scriptstyle 2} \\ Y & \xrightarrow[2]{} & E \end{array}$$

By Riemann-Hurwitz theorem one has $g(X) = g(Y) = 1$ and therefore covering $Y \to E$ is unramified. Hence the covering $C \to X$ is also unramified, which leads to the contradiction.

Finally, suppose that the Galois group is C_4.

As before, there exist two elements $\sigma, \tau \in \mathrm{Aut}(C)$ such that

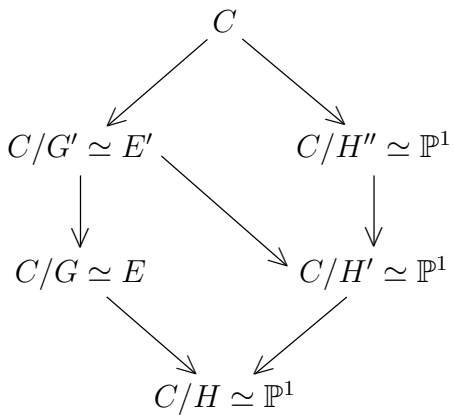
$$C/\langle\sigma\rangle \simeq E$$

and

$$C/\langle\tau\rangle \simeq \mathbb{P}^1,$$

where τ has order two and σ has order $d = 4$. It implies that there exists an elliptic curve $E' = C/\langle\sigma^2\rangle$ such that morphism from C to E factors through E'. We denote $G' = \langle\sigma^2\rangle$, $G = \langle\sigma\rangle$ and $H'' = \langle\tau\rangle$. Also we have two subgroups $H = \langle\sigma, \tau\rangle \simeq C_4 \oplus C_2$, $H' = \langle\sigma^2, \tau\rangle \simeq C_2 \oplus C_2$ of $\mathrm{Aut}(C)$ such that $C/H \simeq \mathbb{P}^1$ and $C/H' \simeq \mathbb{P}^1$.

The following diagram illustrates the whole picture :



Consider the covering $C \to C/H \simeq \mathbb{P}^1$ of degree eight. Riemann-Hurwitz for this morphism tells us:

$$2 = -16 + \sum_{p \in C}(e_p - 1),$$

or equivalently $18 = \sum(e_p - 1)$. Since degree of this covering is eight, possible ramification types are (8), $(4,4)$ or $(2,2,2,2)$. Suppose we have m_i points of i-th ramification type. Then $7m_1+6m_2+4m_3 = 18$, which has exactly the following list of solutions in non-negative integers: $(2,0,1)$, $(0,3,0)$, $(0,1,3)$. Riemann-Hurwitz for $C \to E$ gives us $2 = 0+\sum(e_p-1)$ and therefore we have exactly one ramified point, it has ramification type $(2,2)$. Then solutions $(2,0,1)$ and $(0,3,0)$ are automatically excluded from our consideration. Finally, suppose we are in the case of $(0,1,3)$. We will show that Galois theory implies that there are at least two points with ramification index at least four. Indeed, if p is ramified point for morphism $C/H' \to C/H$, then its inertia group $I_p \subset H \simeq C_4 \oplus C_2$ does not lie in the $H' \simeq C_2 \oplus C_2$. But then, it means it has an element of order at least four. The same time, Riemann-Hurwitz argument shows that there are exactly two points which ramify in the covering $C/H' \to C/H$ and therefore there should be at least two elements of ramification index at least four.

□

Part III

Isomorphism Classes of Maximal Abelian Quotients of Absolute Galois Groups

Chapter 5

On Abelianized Absolute Galois Groups of Global Function Fields

5.1 Introduction

As we mentioned in the first chapter the famous theorem of Uchida [57] states that the isomorphism class of a global function field K is determined by the isomorphism class of the absolute Galois group $\mathcal{G}_K = \mathrm{Gal}(K^{sep} : K)$ considered as topological group. One of the essential steps in the Uchida's proof is to recover from $\mathcal{G}_K$ its abelian part $\mathcal{G}_K^{ab}$ with some additional data, like decomposition and inertia subgroups. The following questions are natural to ask: what kind of information can one recover from the isomorphism class of the pro-finite abelian group $\mathcal{G}_K^{ab}$? More concretely, does the abelian part of the absolute Galois group determine the global function field K up to isomorphism? If not, which function fields share the same isomorphism class of $\mathcal{G}_K^{ab}$?

For a global function field K of characteristic p with exact constant field $\mathbb{F}_q$, $q = p^n$ we define the invariant d_K as the natural number such that $n = p^k d_K$ with $\gcd(d_K, p) = 1$, $k \in \mathbb{Z}_{\geq 0}$. Let $\mathrm{Cl}^0(K)$ denotes the degree zero part of the class-group of K. In other words, $\mathrm{Cl}^0(K)$ is the abelian group of $\mathbb{F}_q$-rational points of the Jacobian variety associated to the curve X. For any abelian group A and a prime number l we denote by A_l its l-part: $A_l = A \otimes \mathbb{Z}_l$, where $\mathbb{Z}_l$ denotes the ring of l-adic integers. We also denote by $A_{\text{non-}l}$ the non-l part of A : $A_{\text{non-}l} = A/A_l$. The main purpose of this chapter is to prove the following result:

Theorem 5.1. *Suppose K and K' are two global function fields. Then $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$ as pro-finite groups if and only if the following three conditions hold:*

1. *K and K' share the same characteristic p;*
2. *Invariants d_K and $d_{K'}$ coincide: $d_K = d_{K'}$;*
3. *The non p-parts of class-groups of K and K' are isomorphic:*

$$\mathrm{Cl}^0_{non\text{-}p}(K) \simeq \mathrm{Cl}^0_{non\text{-}p}(K').$$

In particular, two function fields with the same field of constants $\mathbb{F}_q$ have isomorphic $\mathcal{G}_K^{ab}$ if and only if they have isomorphic $\mathrm{Cl}^0_{non\text{-}p}(K)$.

The proof of Theorem 5.1 includes explicit reconstruction of the invariants p, d_K and $\mathrm{Cl}^0_{\text{non-}p}(K)$ from $\mathcal{G}_K^{ab}$. More concretely, let $s_l(\mathcal{G}_K^{ab})$ be the least integer k such that $\mathcal{G}_K^{ab}$ has direct summand of the form $\mathbb{Z}/l^k\mathbb{Z}$ and let $p^\star$ denotes $(-1)^{\frac{p-1}{2}}p$ if p is odd and p otherwise, then:

Theorem 5.2. *Given the isomorphism class of the topological group $\mathcal{G}_K^{ab}$ we have:*

1. *The characteristic of K is the unique prime p such $\mathcal{G}_K^{ab}$ has no elements of order p;*
2. *The non-p part $\mathrm{Cl}^0_{non\text{-}p}(K)$ of the class-groups of K is isomorphic to the torsion of the quotient $\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]}$, where $\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]}$ denotes the closure of the torsion subgroup of $\mathcal{G}_K^{ab}$:*

$$\mathrm{Cl}^0_{non\text{-}p}(K) \simeq (\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]})[\mathrm{tors}].$$

3. *The natural number d_K is the unique number co-prime to p such that for any prime number $l \neq p$:*

$$\mathrm{ord}_l(d_K) = \begin{cases} 0, & \text{if } l = 2 \text{ and } s_2(\mathcal{G}_K^{ab}) = 1; \\ s_l(\mathcal{G}_K^{ab}) - \mathrm{ord}_l((p^\star)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

Proof. See corollaries 5.12 and 5.13. □

By using these theorems we will establish the following:

Corollary 5.3. *Let K be the rational function field (with genus zero) over a fixed constant field $\mathbb{F}_q$ and let E be an elliptic function field (with genus one) defined over the same constant field, such that*[1] *$\#\,\mathrm{Cl}^0(E) = q$. Then there exists isomorphism of topological groups $\mathcal{G}_K^{ab} \simeq \mathcal{G}_E^{ab}$.*

This corollary provides some answers to the above questions. For example, it follows that for every q there exists a pair of function fields K, K' over $\mathbb{F}_q$ with $g(K) = 0$, $g(K') = 1$ and $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$. In particular, the genus g_K of K and therefore the Dedekind zeta-function $\zeta_K(s)$ of K are not determined by the isomorphism class of $\mathcal{G}_K^{ab}$ even if the constant field $\mathbb{F}_q$ is fixed. The above example also shows that:

Corollary 5.4. *For every p there exist infinitely many pairwise non-isomorphic function fields K of characteristic p with isomorphic $\mathcal{G}_K^{ab}$.*

Proof. Fix a prime number p and let $q = p^{p^k}$, where k is a non-negative integer. Let F_k and E_k denote rational and elliptic function fields from the previous example with exact constant field $\mathbb{F}_q$. Then, according to the our main theorem for any non-negative integers k, l we have: $\mathcal{G}_{K_l}^{ab} \simeq \mathcal{G}_{E_k}^{ab}$. □

Applying some classical results about the two-part of $\mathrm{Cl}^0(K)$ of hyper-elliptic function fields we will also show that:

[1] the existence of such field is guaranteed by the Waterhouse theorem, see section 5.4.

Corollary 5.5. *For any given q with $p > 2$ infinitely many distinct isomorphism types of $\mathcal{G}_K^{ab}$ occur for function fields with exact constant field $\mathbb{F}_q$.*

Proof. See theorem 5.42 from the last section. □

Unfortunately, the answer to the question about distribution of global fields over fixed constant field $\mathbb{F}_q$ sharing the same $\mathcal{G}_K^{ab}$ is not clear at the moment, since we don't know if there are infinitely many such fields with a given non p-part of the class group. In particular, it seems to be reasonable to state the following **conjecture:** *there are infinitely many curves defined over fixed finite field $\mathbb{F}_q$, $q = p^n$ with order of the group of $\mathbb{F}_q$-rational points of the Jacobian varieties associated to them to be a power of p.* If the conjecture is true then what is the proportion of such curves, say as q fixed and g tends to infinity?

The main idea towards our result was inspired by the work [1], where authors produced an elegant description for the isomorphism class of the topological group $\mathcal{G}_K^{ab}$, where K denotes *imaginary quadratic number field*. But note also that there are many completely different technical details, which point in a different direction.

This chapter has the following structure: in the next section we will sketch the proof of Theorem 5.1. Then we prove all the necessarily lemmas in the section 5.3. Finally, we will discuss the question about construction of non-isomorphic function fields with isomorphic and non-isomorphic abelian parts of their absolute Galois groups and prove corollaries 5.3, 5.4 and 5.5.

5.2 Outline of the Proof

Global class field theory provides an internal description of the abelian part of the absolute Galois group of a global or local field K in terms of arithmetic objects associated to K. We will use the *idèle*-theoretical approach: see section 5.3.2 for details and the classical books [36], [59], [2] for complete discussion. For a given global function field K we denote by $\mathcal{I}_K$ the group of idèles of K and by $\mathcal{C}_K$ the *idèle class-group of K*, i.e. the quotient group of $\mathcal{I}_K$ by the multiplicative group $K^\times$. Recall that we have a split exact sequence:

$$0 \to \mathcal{C}_K^0 \to \mathcal{C}_K \xrightarrow{\deg} \mathbb{Z} \to 0,$$

where $\mathcal{C}_K^0$ is the degree zero part of the idèle class group and the map from $\mathcal{C}_K$ to $\mathbb{Z}$ is the degree map.

Theorem 5.6 (The Main Theorem of Class Field Theory for Global Function FIelds)**.** *In the above settings there exists an isomorphism of topological groups: $\mathcal{C}_K^0 \oplus \widehat{\mathbb{Z}} \simeq G_K^{ab}$.*

Proof. See section 5.3.2. □

We will show that $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$ if and only if $\mathcal{C}_K^0 \simeq \mathcal{C}_{K'}^0$. The key ingredient in the our proof is Pontryagin duality for locally compact abelian groups, which allows us to reduce question about pro-finite abelian groups to the question about discrete torsion groups.

Lemma 5.7. *Let A and B be two pro-finite abelian groups. If $A \oplus \widehat{\mathbb{Z}} \simeq B \oplus \widehat{\mathbb{Z}}$ then $A \simeq B$ in the category of pro-finite abelian groups.*

Proof. See section 5.3.1. □

This lemma reduces our question to the description of $\mathcal{C}_K^0$ as a topological group. Let v denote a place of K and K_v, $\mathcal{O}_v$ denotes the corresponding completion and its ring of integers respectively. Then we derive the following exact sequence.

Lemma 5.8. *There exists an exact sequence of topological groups, where the finite groups have the discrete topology:*

$$1 \to \mathbb{F}_q^\times \to \prod_v \mathcal{O}_v^\times \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1.$$

Proof. See section 5.3.3. □

For the next step we recall in lemma 5.17 the isomorphism $\mathcal{O}_v^\times \simeq \mathbb{F}_{q^n}^\times \times \mathbb{Z}_p^\infty$, where n is the degree of a place v and $\mathbb{Z}_p$ denotes the group of p-adic integers. Denoting by $\mathcal{T}_K$ the group $(\prod_v \mathbb{F}_{q^{\deg(v)}}^\times)/\mathbb{F}_q^\times$ we will get the following exact sequence, see section 5.3.3:

$$1 \to \mathcal{T}_K \times \mathbb{Z}_p^\infty \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1 \tag{5.1}$$

There are two crucial observations about this sequence. First we will prove the following structure theorem for the group $\mathcal{T}_K$:

Theorem 5.9. *Given a function field K with exact constant field $\mathbb{F}_q$, where $q = p^n$ there exists an isomorphism $\mathcal{T}_K \simeq \prod_{l,m} (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}}$, where the product is taken over all prime numbers l and all positive integers m and $a_{l,m}$ denotes a finite or countable cardinal number. Moreover, the coefficients $a_{l,m}$ depend only on q and the following holds:*

1. *Each $a_{l,m}$ is either zero or the infinite countable cardinal;*
2. *For $l = p$ we have $a_{p,m} = 0$ for all m;*
3. *For $l \neq p$, $l \neq 2$ there exists a unique non-negative integer $N_q(l)$ such that $a_{l,m}$ is infinite if and only if $m \geq N_q(l)$;*
4. *For $p \neq 2$ and $l = 2$ there exists a unique non-negative integer $N_q(2)$ such that for $q = 1 \mod 4$ we have $a_{2,m}$ is infinite if and only if $m \geq N_q(2)$, and for $q = 3 \mod 4$ we have $a_{2,m}$ is infinite if and only if $m = 1$ or $m \geq N_q(2)$;*
5. *Given two prime powers q_1, q_2 the numbers $N_{q_1}(l)$ and $N_{q_2}(l)$ coincide for all l if and only if $q_1 = p^{n_1}$, $q_2 = p^{n_2}$ with $\frac{n_1}{n_2} = p^m$, for some integer m.*

Proof. See section 5.3.4. For expression of $N_q(l)$ see lemma 5.21 and lemma 5.22. □

Definition 5.10. *The exact sequence of abelian groups $0 \to A \to B \xrightarrow{\psi} C \to 0$ is called* totally non-split *if there is no non-trivial subgroup S of C such that the sequence $0 \to A \to \psi^{-1}(S) \to S \to 0$ splits.*

The second observation about 5.1 is the key point in the our proof.

Theorem 5.11. *All torsion elements of $\mathcal{C}^0_K$ are in $\mathcal{T}_K$. Therefore the exact sequence 5.1 is totally non-split. Moreover, the topological closure of the torsion subgroup of $\mathcal{C}^0_K$ is $\mathcal{T}_K$: $\overline{\mathcal{C}^0_K[\text{tors}]} = \mathcal{T}_K$.*

Proof. See section 5.3.5. □

Because of the description of $\mathcal{T}_K$ this theorem gives us:

Corollary 5.12. *If $\mathcal{G}^{ab}_K \simeq \mathcal{G}^{ab}_{K'}$ as pro-finite groups then $\mathcal{T}_K \simeq \mathcal{T}_{K'}$, in particular the characteristic p and the invariant d_K are determined by the isomorphism class of $\mathcal{G}^{ab}_K$.*

Proof. Since $\mathcal{G}^{ab}_K \simeq \mathcal{C}^0_K \oplus \widehat{\mathbb{Z}}$ and the group $\widehat{\mathbb{Z}}$ is torsion free, we have that $\mathcal{T}_K$ is also the closure of the torsion subgroup of $\mathcal{G}^{ab}_K$. Then theorem 5.9 shows that p is a unique prime such that this group has no elements of order p.

For the natural number d_K consider the torsion group $\mathcal{G}^{ab}_K[\text{tors}]$. By Theorem 5.9 this group has direct summand of the form $\mathbb{Z}/l^k\mathbb{Z}$ for a fixed prime $l \neq p$ if and only if $k \geq N_q(l)$ or $l = 2$, $k = 1$, $p = 3 \mod 4$ and $d_K = 1 \mod 2$. In the proof of Theorem 5.9 we will show that $N_q(l) = \text{ord}_l(d_K) + \text{ord}_l((p^\star)^{l-1} - 1)$, where $p^\star = -p$ if $p = 3 \mod 4$ and $p^\star = p$ otherwise. Which implies the formula:

$$\text{ord}_l(d_K) = \begin{cases} 0, & \text{if } l = 2 \text{ and } s_2 = 1 \\ s_l(\mathcal{G}^{ab}_K) - \text{ord}_l((p^\star)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

□

Since each pro-finite abelian group is isomorphic to the limit of finite abelian groups, by the Chinese remainder theorem it is also isomorphic to the product over prime numbers of its primary components. We will work with these components separately instead of working with the whole group. Keeping the same notation as for finite abelian groups, for any pro-finite abelian group G and a prime number l we denote by G_l the l-part of G: $G \otimes \mathbb{Z}_l$. Now let l be a prime number different from p, we have:

$$1 \to \mathcal{T}_{K,l} \to \mathcal{C}^0_{K,l} \to \text{Cl}^0_l(K) \to 1.$$

Which shows that:

$$\text{Cl}^0_l(K) \simeq \mathcal{C}^0_{K,l} / \overline{\mathcal{C}^0_{K,l}[\text{tors}]}.$$

Corollary 5.13. *If $\mathcal{G}^{ab}_K \simeq \mathcal{G}^{ab}_{K'}$ as pro-finite groups then the non p-parts of the class-groups of K and K' are isomorphic: $\text{Cl}^0_{non\text{-}p}(K) \simeq \text{Cl}^0_{non\text{-}p}(K')$.*

Proof. We know that $\mathcal{G}^{ab}_K \simeq \mathcal{C}^0_K \oplus \widehat{\mathbb{Z}}$ and that $\mathcal{T}_K = \overline{\mathcal{G}^{ab}_K[\text{tors}]}$. Considering the l-part we get:

$$\mathcal{G}^{ab}_{K,l} / \overline{\mathcal{G}^{ab}_{K,l}[\text{tors}]} \simeq (\mathcal{C}^0_{K,l} / \mathcal{T}_{K,l}) \oplus \mathbb{Z}_l.$$

Since $\mathbb{Z}_l$ is torsion free, we have:

$$(\mathcal{G}^{ab}_{K,l} / \overline{\mathcal{G}^{ab}_{K,l}[\text{tors}]})[\text{tors}] \simeq \mathcal{C}^0_{K,l} / \mathcal{T}_{K,l} \simeq \text{Cl}^0_l(K).$$

Finally, note that the p-part of the torsion group of $\mathcal{G}_K^{ab}$ is trivial and hence combining all primes l different from p we get:

$$\mathrm{Cl}^0_{\text{non-}p}(K) \simeq (\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]})[\mathrm{tors}].$$

□

Proof of Theorem 5.1. The above two corollaries imply the only if part of Theorem 5.1. Now, we are going to discuss the question about the other implication. Our goal is to show that for a given isomorphism class of $\mathcal{T}_K$ and non p-part of the class group there is only one possibility for $\mathcal{C}_K^0$ to fit in the exact sequence 5.1.

Consider the p-part of the exact sequence 5.1:

$$1 \to \mathbb{Z}_p^\infty \to \mathcal{C}^0_{K,p} \to \mathrm{Cl}^0_p(K) \to 1.$$

By using the fact that this sequence is totally non-split we will show, see lemma 5.31 that this implies $\mathcal{C}^0_{K,p} \simeq \mathbb{Z}_p^\infty$, in particular the isomorphism type of $\mathcal{G}^{ab}_{K,p}$ *doesn't depend on* $\mathrm{Cl}^0_p(K)$.

We fix a prime number $l \neq p$ and consider the l-part which is of course also totally non-split:

$$1 \to \mathcal{T}_{K,l} \to \mathcal{C}^0_{K,l} \to \mathrm{Cl}^0_l(K) \to 1. \tag{5.2}$$

Obviously, if $\mathrm{Cl}^0_l(K) \simeq 0$ then $\mathcal{C}^0_{K,l} \simeq \mathcal{T}_{K,l}$. Our goal is to show that even if $\mathrm{Cl}^0_l(K)$ is not the trivial group then the isomorphism type of $\mathcal{C}^0_{K,l}$ is uniquely determined by isomorphism types of $\mathcal{T}_{K,l}$, $\mathrm{Cl}^0_l(K)$ and the fact that the exact sequence 5.2 is totally non-split.

In order to achieve our goal we need the following:

Theorem 5.14. *Let $\{C_i\}$ be a countable set of finite cyclic abelian l-groups with orders of C_i are not bounded as i tends to infinity and let A be any finite abelian l-group. Then up to isomorphism there exists a unique torsion abelian l-group B satisfying two following conditions:*

1. *There exists an exact sequence: $1 \to A \to B \to \oplus_{i\geq 1} C_i \to 1$;*
2. *A is the set of all divisible elements of B: $A = \cap_{n\geq 1} nB$.*

Proof. See section 5.3.6 □

Applying Pontryagin duality to the exact sequence 5.2 we get:

$$1 \leftarrow (\mathcal{T}_{K,l})^\vee \leftarrow (\mathcal{C}^0_{K,l})^\vee \leftarrow (\mathrm{Cl}^0_l(K))^\vee \leftarrow 1.$$

We will show in corollary 6.7 that this sequence dual to the sequence 5.2 satisfies conditions of Theorem 5.14 and therefore $(\mathcal{C}^0_{K,l})^\vee$ is uniquely determined. So its dual $\mathcal{C}^0_{K,l}$ is uniquely determined.

□

5.3 Proof of Lemmas

In this section we are going to prove all the results needed for our proof. Let us start from recalling some basic facts about pro-finite abelian groups. Standard references are [26] and [18].

5.3.1 Preliminaries

Let A be an abelian group. If this group is finitely generated then the structure theorem says that A is isomorphic to $\mathbb{Z}^r \oplus A_{\text{tors}}$ where r is a non-negative integer called rank and A_{tors} is a finite abelian group. Given two such groups we have that they are isomorphic if and only if their ranks are equal and torsion parts are isomorphic. The structure of an infinitely generated abelian group is more complicated. An element x of the abelian group A is *divisible* if for any $n \in \mathbb{N}$ there exists $y \in A$ such that $x = ny$. The group A is *divisible* if all its elements are divisible. For example $\mathbb{Q}$ is divisible. Another example is the so-called *Prüfer p-group* which is defined as union of all p^k roots of unity in $\mathbb{C}^\times$ for a fixed prime number p: $Z(p^\infty) = \{\zeta \in \mathbb{C}^\times | \zeta^{p^k} = 1, k \in \mathbb{N}\}$. Note that we have an isomorphism of abstract groups: $Z(p^\infty) \simeq \mathbb{Q}_p/\mathbb{Z}_p$, where $\mathbb{Q}_p$ denotes the abelian group of p-adic numbers and $\mathbb{Z}_p$ is a subgroup of all p-adic integers.

A group is called *reduced* if it has no non-zero divisible elements.

Lemma 5.15. *Each abelian group A contains a unique maximal divisible subgroup D and it is the direct sum of D and some reduced subgroup R: $A \simeq D \oplus R$.*

The structure of the divisible subgroup is clear.

Lemma 5.16. *Every divisible group D is isomorphic to a direct sum of copies of $\mathbb{Q}$ and $Z(p^\infty)$ for different prime numbers p.*

Proof. The proofs can be found in chapter 3 of [18]. □

The structure of the reduced part of A can be more complicated and usually involves the theory of Ulm invariants. In this chapter we will work with the reduced part directly not referring to the Ulm invariants at all.

Pontryagin Duality

We need to recall some properties of Pontryagin duality for locally compact abelian groups. A good reference including some historical discussion is [29]. Let $\mathbb{T}$ be the topological group $\mathbb{R}/\mathbb{Z}$ given with the quotient topology. If A is any locally compact abelian group then one considers Pontryagin dual $A^\vee$ of A which is the group of all *continuous homomorphisms* from A to $\mathbb{T}$:

$$A^\vee = \text{Hom}(A, \mathbb{T}).$$

This group has the so-called compact-open topology and is a topological, locally compact group. Here we list some properties of Pontryagin duality we use during the proof:

1. Pontryagin duality is a contra-variant functor from the category of locally compact abelian groups to itself;
2. If A is a finite abelian group with the discrete topology then $A^\vee \simeq A$ non-canonically;
3. We have the canonical isomorphism: $(A^\vee)^\vee \simeq A$;
4. Pontryagin dual of a pro-finite abelian group A is a discrete torsion group and vice versa;

5. Pontryagin duality sends direct products to direct sums and vice versa;
6. Pontryagin dual of $\mathbb{Z}_p$ is $Z(p^\infty)$ and dual of $\mathbb{Q}/\mathbb{Z}$ equipped with the discrete topology is the group of pro-finite integers $\widehat{\mathbb{Z}}$;
7. Pontryagin dual of a divisible group A is torsion free and vice versa.

Having stated this we are able to prove our lemmas.

Proof of Lemma 5.7. Let A and B be two pro-finite abelian groups such that $A\oplus\widehat{\mathbb{Z}} \simeq B\oplus\widehat{\mathbb{Z}}$. Applying Pontryagin duality to the above isomorphism we obtain:

$$(A)^\vee \oplus \mathbb{Q}/\mathbb{Z} \simeq (B)^\vee \oplus \mathbb{Q}/\mathbb{Z}.$$

By lemma 5.15 each abelian group is isomorphic to the direct sum of its reduced and divisible components. Using the fact that $\mathbb{Q}/\mathbb{Z}$ is divisible we have that reduced part of $(A)^\vee$ and $(B)^\vee$ are isomorphic. Now, according to the Lemma 5.16 the divisible part of $(A)^\vee \oplus \mathbb{Q}/\mathbb{Z}$ is a direct sum of copies of $\mathbb{Q}$ and $Z(p^\infty)$ and since $\mathbb{Q}/\mathbb{Z} \simeq \oplus_p Z(p^\infty)$ divisible parts of $(A)^\vee$ and $(B)^\vee$ are isomorphic. Therefore $(A)^\vee$ and $(B)^\vee$ are isomorphic and hence $A \simeq B$.

□

5.3.2 Class Field Theory

In this paragraph we briefly review the class field theory for global and local fields of positive characteristic.

The Case of Local Fields

We will start from the description of local aspects of the class field theory. Let L be a local field of positive characteristic $p > 0$. In other words L is a completion of a global function field K with respect to the discrete valuation associated to the place v of K. The field L is isomorphic to the field of Laurant series with constant field $\mathbb{F}_{q^n}$ and the corresponding ring of integers $\mathcal{O}_L$ is the ring of formal power series: $L \simeq \mathbb{F}_{q^n}((x))$, $\mathcal{O}_L \simeq \mathbb{F}_{q^n}[[x]]$. One way to construct abelian extensions of L is to take the algebraic closure $\overline{\mathbb{F}_{q^n}}$ of the constant field $\mathbb{F}_{q^n}$ which has Galois group $\mathrm{Gal}(\overline{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}) \simeq \widehat{\mathbb{Z}}$. This is the maximal unramified abelian extension of L.

Denoting by $I_L = \mathrm{Gal}^{ram}(L^{ab} : L)$ the inertia subgroup of $\mathcal{G}_L^{ab}$ we have the following split exact sequence:

$$1 \to I_L \to \mathcal{G}_L^{ab} \to \widehat{\mathbb{Z}} \to 1.$$

Recall that we also have the split exact sequence given via the valuation map:

$$1 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 1.$$

The local Artin map: $L^\times \to \mathcal{G}_L^{ab}$ induces isomorphism of topological groups between the pro-finite completion $\widehat{L^\times}$ of $L^\times$ and $\mathcal{G}_L^{ab}$ such that two exact sequences are isomorphic:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \widehat{\mathcal{O}_L^\times} \simeq \mathcal{O}_L^\times & \longrightarrow & \widehat{L^\times} & \longrightarrow & \widehat{\mathbb{Z}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I_L & \longrightarrow & \mathcal{G}_L^{ab} & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}) & \longrightarrow & 1 \end{array}$$

The Case of Global Fields

It is possible to give a similar description of $\mathcal{G}_K^{ab}$ in the case where K is a global function field via the so-called idèle-class group. First we note that for a global function field K there also exists the maximal unramified abelian extension M of K. The Galois group $\mathrm{Gal}(M:K)$ is isomorphic to the direct sum $\widehat{\mathbb{Z}} \oplus \mathrm{Gal}(H_K:K)$, where $\widehat{\mathbb{Z}}$ corresponds to the constant field extension and H_K is maximal unramified geometric extension of K. The Galois group $\mathrm{Gal}(H_K:K)$ is finite and one of the theorems of the class field theory establishes an isomorphism of abelian groups:

$$\mathrm{Gal}(H_K:K) \simeq \mathrm{Cl}^0(K),$$

where $\mathrm{Cl}^0(K)$ denotes the ideal class group of K.

Let $\mathcal{I}_K$ denotes the multiplicative group of idèles of K. This is the restricted direct product $\mathcal{I}_K = \prod_v' K_v^\times$, where the product is taken over places v of K with respect to $\mathcal{O}_v^\times$. One defines the basic open sets as $U = \prod_v' U_v$, where U_v open in $K_v^\times$ and for almost all v we have $U_v = \mathcal{O}_v^\times$. Under the topology generated by such U this becomes a topological group. The multiplicative group $K^\times$ is embedded to $\mathcal{I}_K$ diagonally as a discrete subgroup and the quotient $\mathcal{C}_K$ is the *idèle class group* of K. This is a topological group, but it is not pro-finite.

Proof of Theorem 5.6. One defines the global Artin map $\mathcal{C}_K \to \mathcal{G}_K^{ab}$. This map is injective, but not surjective. Similar to the local case it induces isomorphism of the pro-finite completion of $\mathcal{C}_K$ and $\mathcal{G}_K^{ab}$ as topological groups: $\widehat{\mathcal{C}_K} \simeq \mathcal{G}_K^{ab}$, see theorem 6, chapter 9 of [59].

Recall from the introduction that we have a split exact sequence:

$$0 \to \mathcal{C}_K^0 \to \mathcal{C}_K \xrightarrow{\deg} \mathbb{Z} \to 0,$$

where the map from $\mathcal{C}_K$ to $\mathbb{Z}$ is the degree map and $\mathcal{C}_K^0$ is the degree zero part of the idèle class group. We have that $\mathcal{C}_K^0$ is pro-finite, hence complete and therefore $\widehat{\mathcal{C}_K} \simeq \mathcal{C}_K^0 \oplus \widehat{\mathbb{Z}}$. □

5.3.3 Deriving the main exact sequence

Now our goal is to prove lemma 5.8. Let $\mathcal{I}_K^0$ be the group of degree zero idèles of K, i.e. means the kernel of the degree map from $\mathcal{I}_K$ to $\mathbb{Z}$. We have:

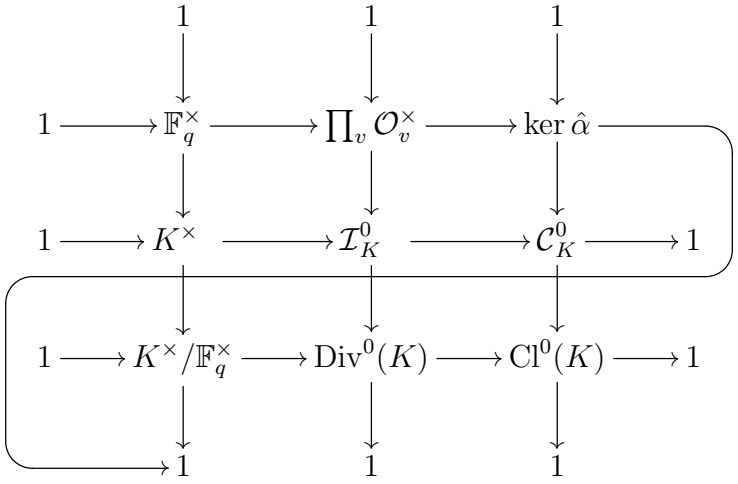
$$1 \to K^\times \to \mathcal{I}_K^0 \to \mathcal{C}_K^0 \to 1.$$

Let $\mathrm{Div}(K)$ denote the divisor group and let $\mathrm{Div}^0(K)$ be the subgroup of degree zero divisors. We also have the natural exact sequence, where $\mathbb{F}_q$ is exact field of constants of K:

$$1 \to \mathbb{F}_q^\times \to K^\times \to \mathrm{Div}^0(K) \to \mathrm{Cl}^0(K) \to 1.$$

There is a surjective homomorphism α of topological groups from $\mathcal{I}_K^0$ to $\mathcal{P}^0(K)$, sending an idèle $(a_{P_1}, a_{P_2}, \dots)$ to the divisor $\sum v_{P_i}(a_{P_i}) \cdot P_i$. This is well-defined since for a given idèle almost all $a_P \in \mathcal{O}_{v_P}^\times$. The kernel of this map is $\prod_v \mathcal{O}_v^\times$. Moreover, this map sends principal

idèle to principal ideals and hence induces the surjective quotient map $\hat{\alpha}$ from $\mathcal{C}_K^0$ to $\mathrm{Cl}^0(K)$. We have the following snake-lemma diagram:



And therefore we have:

$$1 \to \mathbb{F}_q^\times \to \prod_v \mathcal{O}_v^\times \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1.$$

This proves lemma 5.8.

5.3.4 On the Structure of the Kernel

Now we will give an explicit description of the group $\ker \hat{\alpha} \simeq (\prod_v \mathcal{O}_v^\times)/\mathbb{F}_q^\times$. If v is a place of degree n of a global function field K with exact constant field $\mathbb{F}_q$, then K_v is the field of Laurant series with constant field $\mathbb{F}_{q^n}$ and $\mathcal{O}_v$ is the ring of formal power series: $K_v \simeq \mathbb{F}_{q^n}((x))$, $\mathcal{O}_v \simeq \mathbb{F}_{q^n}[[x]]$. A formal power series is invertible if and only if it has non-zero constant term and therefore:

$$\mathcal{O}_v^\times \simeq \mathbb{F}_{q^n}^\times \times (1 + t\mathbb{F}_{q^n}[[t]]).$$

Lemma 5.17. *We have an isomorphism of topological groups:* $1 + t\mathbb{F}_{q^n}[[t]] \simeq \mathbb{Z}_p^\infty$, *where* ∞ *means the countable cardinal number.*

Proof. See [36], section on local fields. □

Denoting by $\mathcal{T}_K$ the group $(\prod_v \mathbb{F}_{q^{\deg(v)}}^\times)/\mathbb{F}_q^\times$, we obtain:

$$(\prod_v \mathcal{O}_v^\times)/\mathbb{F}_q^\times \simeq \mathcal{T}_K \times \mathbb{Z}_p^\infty.$$

Description of $\mathcal{T}_K$

At the first time it seems that the group $\mathcal{T}_K$ depends on K since the product $\prod_v \mathcal{O}_v^\times$ is taken over all places of K. Our first goal is to show that it actually depends only on q.

Recall the following classical statement needed in the proof:

Lemma 5.18. *For a fixed global function field K there exists a natural number N such that for every $n \in \mathbb{N}$, $n \geq N$ there exists a place of K of degree n.*

Proof. See chapter 5 of [42]. □

Consider the group $A_K = \prod_v \mathbb{F}^{\times}_{q^{\deg(v)}}$. By the Chinese reminder theorem we have:

$$A_K = \prod (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}},$$

where $a_{l,m}$ is either a non-negative integer or infinite countable cardinal number. Since $\mathbb{F}^{\times}_{q^n}$ is a cyclic group of order $q^n - 1$ we have the direct description of $a_{l,m}$: it is the cardinality of the set $\{v \in \mathrm{Pl}(K) | \, \mathrm{ord}_l(q^{\deg(v)} - 1) = m\}$. Note that $a_{p,m} = 0$ for all $m \in \mathbb{N}$.

Lemma 5.19. *Each $a_{l,m}$ is either 0 or infinity.*

Proof. Suppose that there exists a place v of degree n such that $\mathrm{ord}_l(q^n - 1) = m$. We will show that then there are infinitely many such v. Our assumption implies that $q^n = 1 \mod l^m$, but $q^n \neq 1 \mod l^{m+1}$. The order of the group $(\mathbb{Z}/l^{m+1}\mathbb{Z})^{\times}$ is $\phi(l^{m+1}) = l^{m+1} - l^m$, where ϕ denotes the Euler ϕ-function. It means if q^n satisfies our condition then for any $k \in \mathbb{N}$ the quantity $q^{n+k\phi(l^{m+1})}$ also satisfies our condition. In other words, this condition depends only on $n \mod \phi(l^{m+1})$. Since by lemma 5.18 each function field K has places of all except finitely many degrees if there is one v with $\mathrm{ord}_l(q^{\deg(v)} - 1) = m$ then there are infinitely many such places. □

Now, given $l \neq p$ we would like to understand for how many m we have $a_{l,m} = 0$. First we will prove the following elementary number theory lemma.

Lemma 5.20. *Let a be a positive integer such that $\mathrm{ord}_l(a-1) = n \geq 1$ for some prime number l. Then if $l \neq 2$ or $n \geq 2$ we have $\mathrm{ord}_l(a^l - 1) = n + 1$.*

Proof. By the assumption of the lemma there exists an integer b such that $\gcd(b, l) = 1$ and $a = 1 + bl^n \mod l^{n+1}$. Suppose that $l \neq 2$. For some integer c we have:

$$a^l = (1 + bl^n + cl^{n+1})^l = 1 + l(bl^n + cl^{n+1}) + \frac{l(l-1)}{2}(bl^n + cl^{n+1})^2 + \cdots =$$

$$= 1 + l^{n+1}(b + cl) + \frac{l(l-1)}{2} l^{2n}(b + cl)^2 + \ldots.$$

Since $l \neq 2$ we have $a^l = 1 + bl^{n+1} \mod l^{n+2}$.

Now let $l = 2$ and $n \geq 2$. We have: $a = 1 + 2^n + b2^{n+1} \mod 2^{n+2}$ and therefore $a^2 = 1 + 2^{n+1} \mod 2^{n+2}$. □

Lemma 5.21. *For each odd prime number l different from p there exists $N(l)$ such that $a_{l,m}$ is infinite if and only if $m \geq N(l)$. Moreover $N(l)$ depends only on q and not on K.*

Proof. Let $d = l-1$ and $N(l) = \mathrm{ord}_l(q^d - 1)$. Then $q^d = 1$ in the group $(\mathbb{Z}/l^{N(l)}\mathbb{Z})^\times$, but $q^d \neq 1$ in the group $(\mathbb{Z}/l^{N(l)+1}\mathbb{Z})^\times$. Therefore, for each $u \in \mathbb{N}$ such that $u = d \mod \phi(l^{N(l)+1})$ we have: $\mathrm{ord}_l(q^u - 1) = N(l)$. Since K has places of almost all degrees the set $\{v \in \mathrm{Pl}(K) | \deg(v) = d \mod \phi(l^{N(l)+1})\}$ is infinite and hence $a_{l,N(l)} \neq 0$. We would like to show that if $a_{l,m} \neq 0$ then $a_{l,m+1} \neq 0$. We know that there exists a place of the degree d_0 such that $\mathrm{ord}_l(q^{d_0} - 1) = m$. By the previous lemma we have $\mathrm{ord}_l(q^{ld_0} - 1) = m + 1$. Then for any place v from the set $\{v \in \mathrm{Pl}(K) | \deg(v) = ld_0 \mod \phi(l^{m+2})\}$ we have $\mathrm{ord}_l(q^{\deg(v)} - 1) = m + 1$. This shows that if $m \geq N(l)$ then $a_{l,m}$ is infinite.

The last step is to show that $a_{l,m} = 0$ if m is less than $\mathrm{ord}_l(q^d - 1)$. Indeed, the order a of q in the group $\mathbb{F}_l^\times$ divides $(l-1)$ and then $\mathrm{ord}_l(q^a - 1) = \mathrm{ord}_l(q^{a\frac{l-1}{a}} - 1) = \mathrm{ord}_l(q^{l-1} - 1)$, since $\frac{l-1}{a}$ is co-prime to l. It means that if for some u we have $q^u = 1 \mod l$, then $u = ab$ and $\mathrm{ord}_l(q^u - 1) = \mathrm{ord}_l(q^{ab} - 1) \geq \mathrm{ord}_l(q^a - 1) = \mathrm{ord}_l(q^{l-1} - 1)$.

□

Lemma 5.22. *For $l = 2$ the following holds.*

1. *If $p = 2$, then $a_{2,m} = 0$ for all m;*
2. *if $q = 1 \mod 4$, then there exists $N(2)$ such that $a_{2,m}$ is infinite if and only if $m \geq N(2)$;*
3. *if $q = 3 \mod 4$, then there exists $N(2)$ such that $a_{2,m}$ is infinite if and only if $m \geq N(2)$ or $m = 1$;*

Proof. The first statement is trivial. For the second one let $N(2) = \mathrm{ord}_2(q-1)$, then $N(2) \geq 2$. As before we have $q = 1 \mod 2^{N(2)}$, but $q \neq 1 \mod 2^{N(2)+1}$. The group $(\mathbb{Z}/2^{N(2)+1}\mathbb{Z})^\times$ has order $\phi(2^{N(2)+1})$ and hence, for each m such that $m = 1 \mod \phi(2^{N(2)+1})$ we have that $q^m = 1 \mod 2^{N(2)}$, but $q \neq 1 \mod 2^{N(2)+1}$. Since K has places of almost all degrees the set $\{v \in \mathrm{Pl}(K) | \deg(v) = 1 \mod \phi(l^{N(2)+1})\}$ is infinite and hence $a_{2,N(2)} \neq 0$. Now, as in the previous lemma if $a_{l,m} \neq 0$, then $a_{l,m+1}$ is not zero and obviously if $m < N(2)$ we have $a_{2,m} = 0$, here we use the fact that $m \geq 2$.

Finally suppose that $q = 3 \mod 4$. By the same argument as before we have that $a_{2,1}$ is infinite, but then $q^2 = 1 \mod 8$ and hence $a_{2,2} = 0$. Let $N(2) = \mathrm{ord}_2(q^2 - 1) \geq 3$. We have that for $a_{2,N(2)}$ is infinite and for all k such that $1 < k < N(2)$ we have $a_{2,k} = 0$. Because of the same argument as before $a_{2,m}$ is infinite for all $m \geq N(2)$.

□

The next step is to show that $T_q \simeq A_q$. In order to do that we need one elementary lemma.

Lemma 5.23. *For a given prime power q there are infinitely many integer numbers n such that $\gcd(\frac{q^n-1}{q-1}, q-1) = 1$.*

Proof. Consider the factorization of $q-1$ into different prime factors: $q - 1 = l_1^{k_1} \dots l_m^{k_m}$. We know that $q = 1 \mod l_i^{k_i}$ and $q \neq 1 \mod l_i^{k_i+1}$, for all i in $\{1, \dots, m\}$. In other words there exists a natural number a_i co-prime to l_i such that $q = 1 + a_i l_i^{k_i} \mod l_i^{k_i+1}$. Therefore if the natural number n is co-prime to $q-1$ then $q^n = 1 + a_i n l_i^{k_i} \mod l_i^{k_i+1}$ and then $\gcd(\frac{q^n-1}{q-1}, q-1) = 1$. □

Corollary 5.24. *We have an isomorphism $A_q \simeq \mathcal{T}_q$. The characteristic p of the constant field of K is determined by $\mathcal{T}_q$.*

Proof. For the first statement recall that $\mathbb{F}_q^\times$ is embedded diagonally to the product $\prod_v \mathbb{F}_{q^{\deg(v)}}^\times$. Now pick any prime β of K of degree m such that $\gcd(\frac{q^m-1}{q-1}, q-1) = 1$ and split the last product into two parts $\mathbb{F}_{q^m}^\times \oplus \prod_{v\neq\beta} \mathbb{F}_{q^{\deg(v)}}^\times$. Note that $\mathbb{F}_q^\times$ is a subgroup of $\mathbb{F}_{q^m}^\times$ which is direct summand. Since all these finite groups have the discrete topology, the quotient $\prod_{v\neq\beta} \mathbb{F}_{q^{\deg(v)}}^\times \oplus (\mathbb{F}_{q^m}^\times/\mathbb{F}_q^\times)$ is topologically isomorphic to $\mathcal{T}_q$. Finally, since each $a_{n,l}$ is either zero or infinity we have that $A_q \simeq \mathcal{T}_q$.

For the second statement note that p is unique prime such that $a_{p,m} = 0$ for all $m \in \mathbb{N}$.

□

Lemma 5.25. *For odd prime number l we have $N(l) = \mathrm{ord}_l(p^{l-1} - 1) + \mathrm{ord}_l\, d_K$.*

Proof. Recall the isomorphism $\mathbb{Z}_l^\times \simeq (\mathbb{Z}_l)_{\mathrm{tors}}^\times \times (1 + l\mathbb{Z}_l)$, for any odd prime number l. The multiplicative group $1 + l\mathbb{Z}_l$ has the following filtration:

$$\mathbb{Z}_l^\times \supset 1 + l\mathbb{Z}_l \supset 1 + l^2\mathbb{Z}_l \supset \dots$$

For fixed q and $l \neq p$ let d be the order of $q \mod l$. Then by the proof of lemma 5.21 we have: $N(l)$ is the greatest integer such that $q^d \in 1 + l^{N(l)}\mathbb{Z}_l$. Raising q to the power p doesn't change its position in the filtration. On the other hand, lemma 5.20 shows that raising q to the power l shifts the position of q in the filtration exactly by one. Hence for $q = p^{d_K p^n}$, $\gcd(d_K, p) = 1$ we have:

$$N(l) = \mathrm{ord}_l(q^{l-1} - 1) = \mathrm{ord}_l(p^{(l-1)d_K p^k} - 1) = \mathrm{ord}_l(p^{l-1} - 1) + \mathrm{ord}_l(d_K)$$

□

Recall that for a prime number l different from p we define $s_l(\mathcal{T}_q)$ to be the least integer k such that T_q has direct summand of the form $\mathbb{Z}/l^k\mathbb{Z}$. Obviously, if $l \neq 2$ then $s_l(T_q) = N(l)$. More generally, we have:

Lemma 5.26. *For a prime number l different from p the order $\mathrm{ord}_l(d_K)$ is given by the following formula:*

$$\mathrm{ord}_l(d_K) = \begin{cases} 0, & \text{if } (l = 2 \text{ and } s_2 = 1) \\ s_l(\mathcal{T}_q) - \mathrm{ord}_l((p^\star)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

Proof. The case of the odd l is clear, since $p^\star = (-1)^{\frac{p-1}{2}} p$ if p is odd and hence for $l = 1 \mod 2$ we have $(p^\star)^{l-1} = p^{l-1}$. If $l = 2$ then there are two cases. If $p = 1 \mod 4$ then $s_2(T_q) = N(2)$ and obviously $p^\star = p$, hence our formula holds trivially. If $p = 3 \mod 4$ then either $q = 3 \mod 4$ or $q = 1 \mod 4$. In the first case we have $d_K = 1 \mod 2$ and $s_2(\mathcal{T}_q) = 1$ which leads to the our "exceptional case": $l = 2$, $s_2 = 1$. In the second case we have $d_K = 0 \mod 2$ and then $N(2) = s_2(T_q) \geq 2$ and hence $s_2(T_q) = \mathrm{ord}_2(q-1) = \mathrm{ord}_2(p^{p^k d_K} - 1) = \mathrm{ord}_2(p^{2\frac{d_K}{2}} - 1) = \mathrm{ord}_2(p^2 - 1) + \mathrm{ord}_2(d_K) - 1 = \mathrm{ord}_2(p+1) + \mathrm{ord}_2(d_K) = \mathrm{ord}_2(p^\star - 1) + \mathrm{ord}_2(d_K)$, since in this case $p^\star = -p$. □

Now we are able to prove our main result concerning the isomorphism type of the abelian group $\mathcal{T}_q$. For a prime power $q = p^n$ we define d_q to be the non-p part of n : $d_q = \frac{n}{p^{\mathrm{ord}_p n}}$. Trivially, for a function field K with exact constant field $\mathbb{F}_q$ we have $d_K = d_q$.

Theorem 5.27. *Given two powers of p: $q_1 = p^{n_1}$ and $q_2 = p^{n_2}$ groups $\mathcal{T}_{q_1}$ and $\mathcal{T}_{q_2}$ are isomorphic if and only if $d_{q_1} = d_{q_2}$, i.e. $\frac{n_1}{n_2} \in p^{\mathbb{Z}}$.*

Proof. The only invariants of T_q are the sequence of coefficients $a_{l,m}$ for different l, m. We will show that they coincide for all l, m if and only if the condition of the our theorem holds.

First we will prove the if part. We assume that $d_{q_1} = d_{q_2}$. Let l be an odd prime number different from p, then by the formula from the above lemma $s_l(\mathcal{T}_{q_1}) = s_l(\mathcal{T}_{q_2})$ and we have $a_{l,m} = 0$ if and only if $m < s_l(\mathcal{T}_{q_1})$ which shows that coefficients $a_{m,l}$ coincide for $\mathcal{T}_{q_1}$ and $\mathcal{T}_{q_2}$. Suppose that $l = 2$. If $p = 2$ then $a_{2,m} = 0$ for all m in both groups. If $p = 1 \mod 4$ or $d_{q_1} = 0 \mod 2$ then as before $a_{2,m} = 0$ if and only if $m < N_2(l) = s_2(T_{q_1}) = \mathrm{ord}_2(d_{q_1}) + \mathrm{ord}_2(p-1)$ and hence $a_{2,m}$ coincide for both groups. Finally, if $p = 3 \mod 4$ and $d_{q_1} = d_{q_2} = 1 \mod 2$ then $a_{2,m} = 0$ if and only if either $m = 1$ or $m > N(2) = \mathrm{ord}_2(q_1^2 - 1) = \mathrm{ord}_2(q_2^2 - 1)$. The equality $\mathrm{ord}_2(q_1^2 - 1) = \mathrm{ord}_2(q_2^2 - 1)$ holds since: $\mathrm{ord}_2(q_1^2 - 1) = \mathrm{ord}_2(q_1 + 1) + 1 = \mathrm{ord}_2(p^{d_{q_1} p^k} + 1) + 1 = \mathrm{ord}_2(p + 1) + 1$.

Now, suppose that $T_{q_1} \simeq T_{q_2}$. Then by the formula from lemma 5.26 for any odd prime number l different from p we have $\mathrm{ord}_l(d_{q_1}) = \mathrm{ord}_l(d_{q_2})$. By definition we have $\mathrm{ord}_p(d_{q_1}) = \mathrm{ord}_p(d_{q_2}) = 0$. Finally, for $l = 2$ there are two cases. Either both groups contain direct summand of the form $\mathbb{Z}/2\mathbb{Z}$ and then $\mathrm{ord}_2(d_{q_1}) = \mathrm{ord}_2(d_{q_2}) = 0$, or otherwise the formula from lemma 5.26 holds and then $\mathrm{ord}_2(d_{q_1}) = \mathrm{ord}_2(d_{q_2})$. □

This already gives some important corollary. If $q = 2^{2^k}$ for some non-negative integer k, then coefficients $a_{l,m}$ defined as follows:

$$a_{l,m} = \begin{cases} \mathbb{N}, & \text{if } l \neq 2 \text{ and } m \geq \mathrm{ord}_l(2^{l-1} - 1) \\ 0, & \text{otherwise.} \end{cases} \tag{5.3}$$

Corollary 5.28. *Each of the following function fields K satisfies: $\mathcal{G}_K^{ab} \simeq \prod_{l,m} (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}} \times \prod_{\mathbb{N}} \mathbb{Z}_2 \oplus \widehat{\mathbb{Z}}$, where $a_{l,m}$ are given by the formula 5.3 :*

1. *The rational function field with $g = 0$ over $\mathbb{F}_{2^{2^k}}$, for any non-zero integer k;*
2. *The elliptic function field $y^2 + y = x^3 + x + 1$, with $g = 1$ over $\mathbb{F}_2$;*
3. *The hyper elliptic function field $y^2 + y = x^5 + x^3 + 1$, with $g = 2$ over $\mathbb{F}_2$;*
4. *The hyper elliptic function field $y^2 + y = (x^3 + x^2 + 1)(x^3 + x + 1)^{-1}$, with $g = 2$ over $\mathbb{F}_2$;*
5. *The function field of the plane quartic $y^4 + (x^3 + x + 1)y + (x^4 + x + 1) = 0$, with $g = 3$ over $\mathbb{F}_2$.*
6. *The elliptic function field $y^2 + y = x^3 + \mu$, with $g = 1$ over $\mathbb{F}_4$, where μ is the generator of $\mathbb{F}_4^{\times}$.*

In particular, the genus, the constant field and the zeta-function of K are not determined by G_K^{ab}.

Proof. All these fields have trivial $\mathrm{Cl}^0(K)$, see [28]. Because of Theorem 5.27 we have $\mathcal{T}_2 \simeq \mathcal{T}_{2^{2^k}}$. It means that for any K listed above $\mathcal{C}_K^0 \simeq \mathcal{T}_2 \times \prod_{\mathbb{N}} \mathbb{Z}_2$. □

Remark: For given q we will call a prime l *exceptional* if $N(l) > 1$. The question which l are exceptional seems to be very difficult. Of course, if $l^2|(q-1)$, then $a_{l,1} = 0$, so $N(l) \geq 2$. For example if $q = 9$ then $a_{2,1} = a_{2,2} = 0$. But also there are exceptional primes l with $\gcd(l, q-1) = 1$. For example if $q = 7$ and $l = 5$. Then $7^d = 1 \mod 5$ if and only if $d = 4k$, $k \in \mathbb{Z}$, but then $7^d = 49^{2k} = (-1)^{2k} = 1 \mod 25$. This means that 5 is exceptional. We expect that for a given q there are infinitely many exceptional primes, but we have no idea how to prove it even for the case $q = 2$: the first exceptional prime for this case is 1093. This phenomena is closely related to the so-called *Wieferich primes*.

Our next goal is to understand what happens with the exact sequence:

$$1 \to \mathcal{T}_q \times \mathbb{Z}_p^\infty \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1,$$

when $\mathrm{Cl}^0(K)$ is not trivial. Since we are working with infinite groups $\mathcal{C}_K^0$ can still be isomorphic to $\mathcal{T}_q \times \mathbb{Z}_p^\infty$. In the next paragraph we will show that all torsion elements of $\mathcal{C}_K^0$ are in $\mathcal{T}_q$.

5.3.5 On the torsion of $\mathcal{C}_K^0$

Theorem 5.29. *All the torsion elements of $\mathcal{C}_K^0$ are in $\mathcal{T}_q$ and the exact sequence 5.1 is totally non-split. Moreover, the topological closure of the torsion subgroup of $\mathcal{C}_K^0$ is $\mathcal{T}_q$.*

Proof. Suppose that there exists a non-zero $x \in \mathcal{C}_K^0$ such that $x^l = 1$ for some prime number l. We will show that this element has trivial image in the class group. Pick a representative $(x_{v_1}, x_{v_2}, \dots)$ for x as element of $\mathcal{I}_K$, we know that almost all i we have $x_{v_i} \in \mathcal{O}_{v_i}^\times$ and that $x^l = (x_{v_1}^l, x_{v_2}^l, \dots)$ is a principal idèle. Let a be the element of $K^\times$ whose image in $\mathcal{I}_K$ is x^l. We have that a is locally an l-th power and hence by Theorem 1, chapter 9 from [2] we have that a is globally an l-th power and hence x is a principal idèle up to multiplication by the element $(\zeta_{v_1}, \zeta_{v_2}, \dots) \in \mathcal{T}_q$, where each ζ_{v_i} denotes an l-th root of unity in $K_{v_i}^\times$ and hence its image in the class group is trivial.

Since $\mathbb{Z}_p$ is torsion free we have that all the torsion of $\mathcal{C}_K^0$ lies in $\mathcal{T}_q$. Note that each element of the direct sum $\oplus_{l,m}(\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}}$ is an element of finite order in $\mathcal{T}_q$ and closure of this direct sum is $\mathcal{T}_q$ itself. □

As it was mentioned in the introduction this statement implies the "only if" part of our main Theorem 5.1.

5.3.6 Proof of the inverse implication

Our task in this section is for given K show that the data $\mathrm{Cl}^0_{\text{non-}p}(K), \mathcal{T}_q$ determines $\mathcal{C}_K^0$ up to isomorphism.

The p-part

Our first goal is to show that the p-part of $\mathcal{C}_K^0$ is isomorphic to $\mathbb{Z}_p^\infty$.

We start from an easy example. Consider the exact sequence: $0 \to \mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z} \to 0$, where the second map is multiplication by p^k. This sequence is totally non-split. We claim that $\mathbb{Z}_p$ is the unique group which can occur in the middle of such a sequence. More concretely:

Example 5.30. *Let A be an abelian pro-p group such that the following sequence is totally non-split: $0 \to \mathbb{Z}_p \to A \to \mathbb{Z}/p^k\mathbb{Z} \to 0$, then $A \simeq \mathbb{Z}_p$.*

Proof. Since $\mathbb{Z}_p$ is torsion free and the sequence is totally non-split then A is also torsion free. Let us denote the quotient map $A \to \mathbb{Z}/p^k\mathbb{Z}$ by ϕ. There exists $x \in A$ such that $\phi(x)$ is the generator of $\mathbb{Z}/p^k\mathbb{Z}$. Moreover, since A is torsion free we know that $p^k x$ is a non-zero element a of $\mathbb{Z}_p$. We claim that the first non-zero coefficient in the p-adic expression $a = a_0 + a_1 p + a_2 p^2 + \dots$ is a_0. Indeed, if a is divisible by p then $p(p^{k-1}x - \frac{a}{p}) = 0$ and hence $p^{k-1}x = \frac{a}{p} \in \mathbb{Z}_p$ since A is torsion free. But then $\phi(p^{k-1}x) = 0$, which contradicts to the our choice of x and hence $a_0 \neq 0$. Then A is generated by $\{x, \mathbb{Z}_p\}$ with the relation $p^k x = a$. Consider the map $\psi : A \to \mathbb{Z}_p$, which sends element x to a and $\mathbb{Z}_p \to p^k\mathbb{Z}_p$. Then ψ is homomorphism: $\psi(p^k x) = \psi(a) = p^k a = p^k \psi(x)$. The kernel of this map is trivial and since $a_0 \neq 0$ then this map is onto. □

This example gives an idea how to prove the following:

Lemma 5.31. *Let A be an abelian pro-p group and let B be a finite abelian p-group such that the following sequence is totally non-split: $0 \to \mathbb{Z}_p^\infty \to A \to B \to 0$. Then $A \simeq \mathbb{Z}_p^\infty$.*

Proof. Since the sequence is totally non-split and $\mathbb{Z}_p$ is torsion free, then A is torsion free also. This means that multiplication by any natural number is injective. It means that Pontryagin dual $A^\vee$ of A is torsion (since A is pro-finite) and divisible (since the dual to the injection is surjection). Consider the dual sequence: $0 \to B^\vee \to A^\vee \to \oplus Z(p^\infty) \to 0$. By the structure theorem of divisible groups $A^\vee$ is isomorphic to the direct sum of copies of $Z(p^\infty)$ and $\mathbb{Q}$. But $A^\vee$ is torsion and hence $A \simeq \mathbb{Z}_p^\infty$. □

This shows that the isomorphism class of $\mathcal{C}_{K,p}^0$ depends only on p. Therefore given two global function fields K_1, K_2 with isomorphic groups $\mathcal{T}_{q_1} \simeq \mathcal{T}_{q_2}$ they share the same characteristic p and hence the p-parts of their *idèle*-class groups are isomorphic: $\mathcal{C}_{K_1,p}^0 \simeq \mathcal{C}_{K_2,p}^0$.

The non p-part

Now we pick the prime number $l \neq p$ and consider the l-part $\mathcal{C}_{K,l}^0$ of $\mathcal{C}_K^0$. If l is such that $\mathrm{Cl}_l^0(K) \simeq \{0\}$ then obviously $\mathcal{T}_{q,l} \simeq \mathcal{C}_{K,l}^0$. Let l be a prime such that $\mathrm{Cl}_l^0(K)$ is not trivial. We know that the following sequence is totally non-split:

$$1 \to \mathcal{T}_{q,l} \to \mathcal{C}_{K,l}^0 \to \mathrm{Cl}_l^0(K) \to 1.$$

Fix a natural number n. Then multiplication by l^n map induces the following commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{T}_{q,l}[l^n] & \hookrightarrow & \mathcal{C}^0_{K,l}[l^n] & \xrightarrow{0} & \mathrm{Cl}^0_l(K)[l^n] & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{T}_{q,l} & \longrightarrow & \mathcal{C}^0_{K,l} & \longrightarrow & \mathrm{Cl}^0_l(K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle l^n} & & \downarrow{\scriptstyle l^n} & & \downarrow{\scriptstyle l^n} & & \\
1 & \longrightarrow & \mathcal{T}_{q,l} & \longrightarrow & \mathcal{C}^0_{K,l} & \longrightarrow & \mathrm{Cl}^0_l(K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathcal{T}_{q,l}/l^n\mathcal{T}_{q,l} & \longrightarrow & \mathcal{C}^0_{K,l}/l^n\,\mathcal{C}^0_{K,l} & \longrightarrow & \mathrm{Cl}^0_l(K)/l^n\,\mathrm{Cl}^0_l(K) & \longrightarrow & 1
\end{array}$$

Since our main sequence is totally non-split the map from $\mathcal{C}^0_{K,l}[l^n]$ to $\mathrm{Cl}^0_l(K)[l^n]$ is the zero map and the map from $T_{q,l}[l^n]$ to $\mathcal{C}^0_{K,l}[l^n]$ is an isomorphism. Now applying Pontryagin duality to the above diagram we get:

$$\begin{array}{ccccccccc}
1 & \longleftarrow & (\mathcal{T}_{q,l}[l^n])^\vee & \twoheadleftarrow & (\mathcal{C}^0_{K,l}[l^n])^\vee & \xleftarrow[0]{} & (\mathrm{Cl}^0_l(K)[l^n])^\vee & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longleftarrow & (\mathcal{T}_{q,l})^\vee & \longleftarrow & (\mathcal{C}^0_{K,l})^\vee & \longleftarrow & (\mathrm{Cl}^0_l(K))^\vee & \longleftarrow & 1 \\
 & & \uparrow{\scriptstyle l^n} & & \uparrow{\scriptstyle l^n} & & \uparrow{\scriptstyle l^n} & & \\
1 & \longleftarrow & (\mathcal{T}_{q,l})^\vee & \longleftarrow & (\mathcal{C}^0_{K,l})^\vee & \longleftarrow & (\mathrm{Cl}^0_l(K))^\vee & \longleftarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & (\mathcal{T}_{q,l}/l^n\mathcal{T}_{q,l})^\vee & \longleftarrow & (\mathcal{C}^0_{K,l}/l^n\,\mathcal{C}^0_{K,l})^\vee & \longleftarrow & (\mathrm{Cl}^0_l(K)/l^n\,\mathrm{Cl}^0_l(K))^\vee & \longleftarrow & 1
\end{array}$$

Because of the construction of $\mathcal{T}_{q,l}$ the group $(\mathcal{T}_{q,l})^\vee$ is isomorphic to the direct sum of finite cyclic groups, for example for $l \neq 2$ we have $(\mathcal{T}_{q,l})^\vee \simeq \oplus_{k \geq N(l)} \oplus_{\mathbb{N}} \mathbb{Z}/l^k\mathbb{Z}$, and therefore $\cap_n l^n(\mathcal{T}_{q,l})^\vee = \{0\}$. It means we have $(\cap_n l^n(\mathcal{C}^0_{K,l})^\vee) \subset (\mathrm{Cl}^0_l(K))^\vee$. Our goal is to show that $(\cap_n l^n(\mathcal{C}^0_{K,l})^\vee) = (\mathrm{Cl}^0_l(K))^\vee$.

Lemma 5.32. *Given any non-zero element x of $(\mathrm{Cl}^0_l(K))^\vee \subset (\mathcal{C}^0_{K,l})^\vee$ and any natural number n there exists an element $c_x \in (\mathcal{C}^0_{K,l})^\vee$ such that $l^n c_x = x$.*

Proof. For fixed n consider the above diagram. Since the second row is exact the image of x in $(\mathcal{T}_{q,l})^\vee$ is zero. Then its image in $(\mathcal{T}_{q,l}[l^n])^\vee$ is also zero. Since $(\mathcal{T}_{q,l}[l^n])^\vee \simeq (\mathcal{C}^0_{K,l}[l^n])^\vee$ it means that image of the non-zero element x in $(\mathcal{C}^0_{K,l}[l^n])^\vee$ is zero. Since the second column is exact this means that x lies in the image of the multiplication by l^n map from $(\mathcal{C}^0_{K,l})^\vee$ to $(\mathcal{C}^0_{K,l})^\vee$ and therefore there exists c_x such that $l^n c_x = x$. □

It means that we have proved:

Corollary 5.33. *The exact sequence $1 \leftarrow (\mathcal{T}_{q,l})^\vee \leftarrow (\mathcal{C}^0_{K,l})^\vee \leftarrow (\mathrm{Cl}^0_l(K))^\vee \leftarrow 1$ satisfies conditions of Theorem 5.14.*

In order to finish our proof of Theorem 5.1 we will to prove theorem 5.14.

Proof of Theorem 5.14

First, let us recall the settings.

Theorem 5.34. *Let $\{C_i\}$ be a countable set of finite cyclic abelian l-groups with orders of C_i are not bounded as i tends to infinity and let A be any finite abelian l-group. Then up to isomorphism there exists a unique torsion abelian l-group B satisfying two following conditions:*

1. *There exists an exact sequence: $1 \to A \to B \to \oplus_{i\geq 1} C_i \to 1$;*
2. *A is the set of all divisible elements of B: $A = \cap_{n\geq 1} nB$.*

Proof of the existence. Given a group A and $\oplus_{i\geq 1} C_i$ let k_i denotes the order of the group C_i. Because of the assumptions of the Theorem, the sequence of orders k_i is not bounded and hence for each natural number N there exists i such that $k_i \geq N$. Let us pick an increasing sequence of indexes j_i, $i \in \mathbb{N}$ such that $k_{j_i} \geq l^i$. Let $\alpha_0, \ldots, \alpha_{n-1}$ be any finite set of generators of A. Consider the sequence a_m of elements of A defined as follows:

$$a_m = \begin{cases} \alpha_i \mod n, & \text{if } m = j_i \\ 0, & \text{otherwise.} \end{cases}$$

Consider the abelian group B which is the quotient of the direct sum $A \oplus (\oplus_{i\in\mathbb{N}} X_i\mathbb{Z})$ of countably many copies of $\mathbb{Z}$ and one copy of A by the relations $k_i X_i = a_i$. We have that B contains A as a subgroup and the quotient of B by A is isomorphic to $\oplus_i C_i$. This means that the group B satisfies the first condition of the theorem. Now, consider the group $Z = \cap_{n\geq 1} nB$. Obviously, $Z \subset A$ and we would like to show that actually $Z = A$. This follows from the fact that for any fixed number $N > 1$ the set $\{k_{j_i} X_{j_i} | i \geq \log_l N\}$ generates A and satisfies $k_{j_i} \geq l^i \geq l^{\log_l(N)} \geq N$.

Proof of the uniqueness. Suppose we are given an abelian torsion l-group B which satisfies both conditions of the our theorem. Denote the map from B to $\oplus_{i\geq 1} C_i$ by ϕ. Let $\tilde{x}_i$ denotes a generator of the cyclic group C_i and let k_i denotes the order of C_i. Let x_i be an element of B such that $\phi(x_i) = \tilde{x}_i$, then $k_i x_i \in A$.

Lemma 5.35. *For any positive integer M which is a power of l the set $A_M = \{k_i x_i | k_i \geq M\}$ generates A.*

Proof. Without loss of generality we assume that $M \geq \#A$. Pick a non-zero element $a \in A$. Because of the second property a can be written as $M^2 y$, where $y \in B$. Since the sequence $1 \to A \to B \to \oplus_{i\geq 1} C_i \to 1$ is exact we can write y as finite $\mathbb{Z}$-linear combination of x_{i_j} and an element of A: $y = b_{i_1} x_{i_1} + b_{i_2} x_{i_2} + \cdots + b_{i_n} x_{i_n} + a_0$. Pick the subset S of $i_1, \ldots, i_n$ consisting of indexes of i_j such that $k_{i_j} \geq M$. Since $M^2 x_{i_j} = 0$ if $k_{i_j} < M$ we have : $M^2 \sum_{j\in S} b_{i_j} x_{i_j} = a$. On the other hand $0 = \phi(a) = M^2 \sum_{j\in S} b_{i_j} \tilde{x}_{i_j}$ and hence $M^2 b_{i_j}$ is divisible by k_{i_j} and $a = \sum_{j\in S} \frac{b_{i_j} M^2}{k_{i_j}} k_{i_j} x_{i_j}$. This means that $\{k_i x_i | k_i \geq M\}$ generates A. □

Remark: consider the sequence $a_i = k_i x_i$ of elements of A from the above lemma. We will say that this sequence (a_i) *strongly generates* A, i.e. that for any integer M the set $S_M = \{a_i | i \in S, k_i \geq M\}$ generates A.

Note that B as abstract abelian group is isomorphic to the group generated by elements X_i and a_i such that $k_iX_i = a_i$: $B = \langle X_i, a_i\rangle/\langle k_iX_i - a_i\rangle$. Given another abelian group B' satisfying conditions of our theorem we know that $B' = \langle X'_i, a'_i\rangle/\langle k_iX'_i - a'_i\rangle$. If for any i we have $a_i = a'_i$ as elements of A then, obviously $B \simeq B'$. Our goal is to show that $B \simeq B'$ in any case.

Definition 5.36. *Given two such groups B, B' with generating sequences (a_i), (a'_i) consider the set $S = \{i|a_i = a'_i\}$. We will say that (a_i) and (a'_i) have* large overlap *if the set $\{a_i|i \in S\}$ strongly generates A.*

We have the following observation:

Lemma 5.37. *If two generating sequences (a_i), (a'_i) of groups B and B' have large overlap, then groups B and B' are isomorphic.*

Proof. For each index i consider the difference $a_i - a'_i$. Since B and B' have large overlap, we can write this difference as finite sum $\sum_{m\in S}\lambda^i_m k_m X'_m$ with $k_m \geq k_i$, $\lambda^i_m \in \mathbb{Z}$. Since both k_m and k_i are powers of l the ratio $\frac{k_m}{k_i}$ is an integer. Consider the map ψ from B to B' defined as follows. The map ψ is identity on A. If $i \in S$ then $\psi(X_i) = X'_i$, otherwise $\psi(X_i) = X'_i + \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m$. We claim that ψ is a homomorphism: if $i \in S$ then $a_i = \psi(k_iX_i) = k_i\psi(X_i) = k_iX'_i = a'_i$. If $i \notin S$, we have $a_i = \psi(k_iX_i) = k_i(X'_i + \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m) = k_i(X'_i) + \sum_{m\in S}\lambda^i_m k_m X'_m = a'_i + (a_i - a'_i) = a_i$. In other words it sends generators of B to elements of B' preserving all relations. We claim moreover that the map ψ is an isomorphism since we will construct the inverse map ϕ from B' to B as follows. The map ϕ is identity on A. For $i \in S$ we have $\phi(X'_i) = X_i$ and for $i \notin S$ we have $\phi(X'_i) = X_i - \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X_m$. Then, for $i \notin S$ we have:

$$\phi(\psi(X_i)) = \phi(X'_i + \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m) = \phi(X'_i) + \phi(\sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m) =$$

$$= (X_i - \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X_m) + (\sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X_m) = X_i.$$

In a similar way one shows that $\psi(\phi(X'_i)) = X'_i$. □

Now we will prove:

Corollary 5.38. *Two groups B and B' satisfying conditions of the above theorem are isomorphic.*

Proof. Suppose that there exists a partition of the set of positive integers $\mathbb{N}$ on two sets $\mathbb{N} = I_1 \cup I_2$, $I_1 \cap I_2 = \emptyset$ such that each of the set $\{a_i|i \in I_1\}$ and $\{a'_i|i \in I_2\}$ strongly generates A. Then we define abelian group D to be the quotient of the direct sum $A \oplus (\oplus_{i\in\mathbb{N}}X_i\mathbb{Z})$ of countably many copies of $\mathbb{Z}$ and one copy of A by the relations $k_iX_i = a_i$, $i \in I_1$ and $k_iX_i = a'_i$, $i \in I_2$. Obviously D also satisfies conditions of Theorem 5.34. Moreover D and B and also D and B' have large overlap, therefore by the lemma 5.37 we have: $B \simeq D \simeq B'$.

Now we will show that such partition exists. We will construct this partition inductively. Let $N_0 = 0$ and let N_1 be the minimal integer such that elements of the set $S_1 = \{a_i|i \leq N_1$ and $k_i \geq l\}$ generate A. The reason for this number to exists is the following. The sequence a_i

strongly generates A which implies that there exist indexes i with $k_i \geq l$ such that a_i generate A, but A is a finite group and hence we can pick a finite number of elements with $k_i \geq l$ generating A. Note that dropping out finitely many indexes doesn't affect the fact that each of the sequences a_i and a'_i strongly generates A. Suppose we've constructed the number N_m then let N_{m+1} be a minimal integer such that elements of the set

$$S_{m+1} = \begin{cases} \{a'_i | N_m < i \leq N_{m+1} \text{ and } k_i \geq l^{m+1}\}, & \text{if } m \text{ is odd} \\ \{a_i | N_m < i \leq N_{m+1} \text{ and } k_i \geq l^{m+1}\}, & \text{otherwise.} \end{cases}$$

generate A. Finally, we define $I_1 = \cup_{m\geq 0}\{i \in \mathbb{N} | N_{2m} < i \leq N_{2m+1}\}$ and $I_2 = \cup_{m\geq 1}\{i \in \mathbb{N} | N_{2m-1} < i \leq N_{2m}\}$. □

5.4 Proof of Corollaries

In this section we will prove corollaries 5.3, 5.4 and 5.5. The first two will follow from the existence for a given constant field $k = \mathbb{F}_q$ an elliptic curve E over k with the group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points having order q, since in the case of elliptic curves we have $E(\mathbb{F}_q) \simeq \mathrm{Cl}^0(K_E)$, where K_E denotes the associated to E global function field.

Definition 5.39. *Fix a finite field $\mathbb{F}_q$. Let N be an integer number in the Hasse interval: $N \in [-2\sqrt{q}; 2\sqrt{q}]$. We will call it admissible if there exists an elliptic curve E over $\mathbb{F}_q$ with $q + 1 - \#E(\mathbb{F}_q) = N$.*

The following statement is a part of the classical statement due to Waterhouse [45]:

Theorem 5.40 (Waterhouse)**.** *If $\gcd(p, N) = 1$ then the number N is admissible.*

Corollary 5.41. *Given a finite field $\mathbb{F}_q$ there exists an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q$.*

The above remarks finish the proof of corollaries 5.3 and 5.4. Now we will discuss the proof of the corollary 5.5. Our goal is to show :

Theorem 5.42. *Given a constant field $k = \mathbb{F}_q$ with characteristic $p \neq 2$ there are infinitely many non-isomorphic curves X over k with different two-parts of the group of k-rational points on the Jacobian varieties associated to them.*

Proof. For any positive integer N there exists a monic irreducible polynomial of degree N with coefficients in $\mathbb{F}_q$. Let us pick any sequence of such polynomials $D_n(x)$, $n \in \mathbb{N}$ with the property that $\deg(D_n(x)) = n+2$. Consider the family of affine curves defined by the equation $C_m : y^2 = D_1(x)D_2(x)\dots D_m(x)$. Since D_i, $i \in \mathbb{N}$ are mutually distinct these affine curves are smooth. Let X_m denotes the normalization of the projective closure of C_m. Then X_m is a hyper-elliptic curve of the genus $g_m = \lfloor \frac{\deg(D_1(x))+\dots+\deg(D_m(x))-1}{2} \rfloor$. The Weil-bound insures that the order of the group of $\mathbb{F}_q$-rational points of the Jacobian variety J_m associated to X_m satisfies the following:

$$(\sqrt{q} - 1)^{2g_m} \leq \#J_m(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g_m},$$

and therefore the two-part of $J_m(\mathbb{F}_q)$ is bounded from above by $(\sqrt{q}+1)^{2g_m}$. On the other hand theorem 1.4 from [7] states that the two-rank of $J_m(\mathbb{F}_q)$ is at least $m-2$. Therefore, among the family X_m there are infinitely many curves with different two-part of the group $J_m(\mathbb{F}_q)$ and therefore their function fields K_m have non-isomorphic $\mathcal{G}_{K_m}^{ab}$. □

Chapter 6

On Abelianized Absolute Galois groups of Imaginary Quadratic Fields

6.1 Introduction

The main purpose of the present chapter is to use techniques from the previous chapter in order to extend results of the paper [1]. We would like to emphasise that results and proofs in this chapter are parallel to those of the previous chapter. In particular, we use similar notations here.

6.1.1 Results of the Chapter

Let K be an imaginary quadratic field different from $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$. Let $\mathcal{T} = \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ and let $\mathrm{Cl}(K)$ denote the ideal class group of K. Let $\mathcal{G}_K^{ab}$ denote the abelianized absolute Galois group of K. Summarising the results of [1] we have:

Theorem 6.1. *In the above setting the following holds:*

1. *There exists an exact sequence of topological groups:* $0 \to \widehat{\mathbb{Z}}^2 \times \mathcal{T} \to \mathcal{G}_K^{ab} \to \mathrm{Cl}(K) \to 0$*;*
2. *The topological closure* $\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]}$ *of the torsion subgroup of* $\mathcal{G}_K^{ab}$ *is* $\mathcal{T}$*;*
3. *The torsion subgroup of the quotient* $\mathcal{G}_K^{ab}/\mathcal{T}$ *is trivial if and only if* $\mathcal{G}_K^{ab} \simeq \widehat{\mathbb{Z}}^2 \times \mathcal{T}$*;*
4. *There exist an injective map from* $(\mathcal{G}_K^{ab}/\mathcal{T})[\mathrm{tors}]$ *to* $\mathrm{Cl}(K)$ *and an algorithm, which on input* K *decides whether the group* $(\mathcal{G}_K^{ab}/\mathcal{T})[\mathrm{tors}]$ *is trivial or not.*

Proof. See theorem 3.5, 4.4 and 5.1 from [1]. □

Let us denote the image of $(\mathcal{G}_K^{ab}/\mathcal{T})[\mathrm{tors}]$ in $\mathrm{Cl}(K)$ by $\mathrm{Cl}^{split}(K)$. Roughly speaking our main result states that the isomorphism type of $\mathcal{G}_K^{ab}$ is uniquely determined by the isomorphism type of $\mathrm{Cl}^{split}(K)$. More concretely, first we will prove:

Theorem 6.2. *Given the group* $\mathcal{T}$ *and a finite abelian group* A *there exists a unique isomorphism type of a pro-finite abelian group* $\mathcal{D}_A$ *such that the following holds:*

1. *There exists an exact sequence:* $0 \to \mathcal{T} \to \mathcal{D}_A \to A \to 0$*;*

2. *All torsion elements of* $\mathcal{D}_A$ *are in* $\mathcal{T}$*.*

Proof. See section 6.2. □

Then the main result of the present chapter could be stated as:

Theorem 6.3. *Let* K *be an imaginary quadratic field different from* $\mathbb{Q}(i)$*,* $\mathbb{Q}(\sqrt{-2})$*. There exists an isomorphism of topological groups* $\mathcal{G}_K^{ab} \simeq \mathcal{D}_A \times \widehat{\mathbb{Z}}^2$*, with* $A \simeq \mathrm{Cl}^{split}(K)$*.*

Proof. See section 6.2. □

The above theorem extends results of Theorem 6.1 as follows:

Corollary 6.4. *For a fixed prime number* p *and an imaginary quadratic field* K *with class number* $h_K = p$ *there are only two isomorphism types of* $\mathcal{G}_K^{ab}$ *which could occur: either* $\mathrm{Cl}^{split}(K) = 0$ *or* $\mathrm{Cl}^{split}(K) \simeq \mathbb{Z}/p\mathbb{Z}$*. In particular, it was shown in [1] that imaginary quadratic fields with the discriminant* D_K *occurring in the list* $\{-35, -51, -91, -115, -123, -187, -235, -267, -403, -427\}$ *all have class-number 2 and have non-trivial* $\mathrm{Cl}^{split}(K)$*, therefore they all share the same isomorphism class of* $\mathcal{G}_K^{ab}$*.*

Also we will use Theorem 6.3 in order to prove:

Corollary 6.5. *There are infinitely many isomorphism types of pro-finite groups which occur as* $\mathcal{G}_K^{ab}$ *for some imaginary quadratic fields.*

Proof. See section 6.3. □

6.2 The Proof of the Theorem

Our goal in this section is to prove Theorem 6.3. We will do this in three steps. First we will prove the group-theoretical Theorem 6.2. Secondly, in lemma 6.8 we will show that given an imaginary quadratic field $K \neq \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ there exist a pro-finite group $\mathcal{D}_K$ and an isomorphism $\mathcal{G}_K^{ab} \simeq \mathcal{D}_K \times \widehat{\mathbb{Z}}^2$. Finally, in lemma 6.9 we will show that the group $\mathcal{D}_K$ satisfies conditions of Theorem 6.2 with $A \simeq \mathrm{Cl}^{split}(K)$. Therefore the isomorphism class of $\mathcal{D}_K$ is uniquely determined by the isomorphism class of the abelian group $\mathrm{Cl}^{split}(K)$ and hence we obtain a proof of Theorem 6.3.

Remark: Since each pro-finite abelian group is isomorphic to the limit of finite abelian groups, by the Chinese remainder theorem we have that it is also isomorphic to the product over prime numbers of its primary components. We will work with these components separately instead of working with the whole group.

Proof of Theorem 6.2

As in the previous sections for a pro-finite abelian group G and a prime number l we denote by G_l the l-primary component $G \otimes \mathbb{Z}_l$ of G. In the setting of Theorem 6.2 the multiplication by l^n map induces the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{T}_l[l^n] & \hookrightarrow & \mathcal{D}_l[l^n] & \xrightarrow{0} & A[l^n] & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{T}_l & \longrightarrow & \mathcal{D}_l & \longrightarrow & A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle l^n} & & \downarrow{\scriptstyle l^n} & & \downarrow{\scriptstyle l^n} & & \\
0 & \longrightarrow & \mathcal{T}_l & \longrightarrow & \mathcal{D}_l & \longrightarrow & A & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathcal{T}_l/l^n\mathcal{T}_l & \longrightarrow & \mathcal{D}_l/l^n\mathcal{D}_l & \longrightarrow & A/l^nA & \longrightarrow & 0
\end{array}$$

Since any torsion element x of $\mathcal{D}_l$ is in $\mathcal{T}_l$ the map from $\mathcal{D}_l[l^n]$ to $A[l^n]$ is the zero map and the map from $\mathcal{T}_l[l^n]$ to $\mathcal{D}_l[l^n]$ is an isomorphism. Now applying the Pontryagin duality to the above diagram we get:

$$\begin{array}{ccccccccc}
0 & \longleftarrow & (\mathcal{T}_l[l^n])^\vee & \twoheadleftarrow & (\mathcal{D}_l[l^n])^\vee & \xleftarrow[0]{} & (A[l^n])^\vee & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longleftarrow & (\mathcal{T}_l)^\vee & \longleftarrow & (\mathcal{D}_l)^\vee & \longleftarrow & (A)^\vee & \longleftarrow & 0 \\
 & & \uparrow{\scriptstyle l^n} & & \uparrow{\scriptstyle l^n} & & \uparrow{\scriptstyle l^n} & & \\
0 & \longleftarrow & (\mathcal{T}_l)^\vee & \longleftarrow & (\mathcal{D}_l)^\vee & \longleftarrow & (A)^\vee & \longleftarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & (\mathcal{T}_l/l^n\mathcal{T}_l)^\vee & \longleftarrow & (\mathcal{D}_l/l^n\mathcal{D}_l)^\vee & \longleftarrow & (A/l^nA)^\vee & \longleftarrow & 0
\end{array}$$

Note that $(\mathcal{T}_l)^\vee$ is isomorphic to the direct sum of cyclic groups $(\mathcal{T}_l)^\vee \simeq \oplus_{k\in\mathbb{N}}\mathbb{Z}/l^k\mathbb{Z}$ and therefore $\cap_n l^n(\mathcal{T}_l)^\vee = \{0\}$. It means we have $(\cap_n l^n(\mathcal{D}_l)^\vee) \subset (A)^\vee$. Our goal is to show that $(\cap_n l^n(\mathcal{D}_l)^\vee) = (A)^\vee$.

Lemma 6.6. *Given any non-zero element x of $(A)^\vee \subset (\mathcal{D}_l)^\vee$ and any natural number n there exists an element $c_x \in (\mathcal{D}_l)^\vee$ such that $l^n c_x = x$.*

Proof. For fixed n consider the above diagram. Since the second row is exact the image of x in $(\mathcal{T}_l)^\vee$ is zero. Then its image in $(\mathcal{T}_l[l^n])^\vee$ is also zero. Since $(\mathcal{T}_l[l^n])^\vee \simeq (\mathcal{D}_l[l^n])^\vee$ it means that image of the non-zero element x in $(\mathcal{D}_l[l^n])^\vee$ is zero. Since the second column is exact this means that x lies in the image of the multiplication by l^n map from $(\mathcal{D}_l)^\vee$ to $(\mathcal{D}_l)^\vee$ and therefore there exists c_x such that $l^n c_x = x$. □

It means that we have proved:

Corollary 6.7. *The exact sequence $0 \leftarrow (\mathcal{T}_l)^\vee \leftarrow (\mathcal{D}_l)^\vee \leftarrow (A)^\vee \leftarrow 0$ satisfies conditions of Theorem 5.14.*

and therefore $\mathcal{D}_l$ is uniquely determined since its Pontryagin dual $(\mathcal{D}_l)^\vee$ is uniquely determined by Theorem 5.14.

6.2.1 Proof of Theorem 6.3

Consider the exact sequence mentioned in Theorem 6.1:

$$0 \to \widehat{\mathbb{Z}}^2 \times \mathcal{T} \to \mathcal{G}_K^{ab} \to \mathrm{Cl}(K) \to 0. \tag{6.1}$$

Taking a prime number l we get the following exact sequence of pro-l abelian groups:

$$0 \to {\mathbb{Z}_l}^2 \times \mathcal{T}_l \to \mathcal{G}_{K,l}^{ab} \to \mathrm{Cl}_l(K) \to 0, \tag{6.2}$$

where $\mathcal{T}_l = \prod_{k\in\mathbb{N}} \mathbb{Z}/l^k\mathbb{Z}$ and $\mathbb{Z}_l$ denotes the group of l-adic integers. If $\mathrm{Cl}_l(K)$ is the trivial group then obviously $\mathcal{G}_{K,l}^{ab} \simeq {\mathbb{Z}_l}^2 \times \mathcal{T}_l$. Our goal is to describe the isomorphism type of $\mathcal{G}_{K,l}^{ab}$ in the case when $\mathrm{Cl}_l(K)$ is not trivial.

Lemma 6.8. *There exists a pro-finite abelian group $\mathcal{D}_l$ such that $\mathcal{G}_{K,l}^{ab} \simeq \mathcal{D}_l \times \mathbb{Z}_l^2$.*

Proof. By Theorem 6.1 we know that $\mathcal{T}_l$ is the closure of the torsion subgroup of $\mathcal{G}_{K,l}^{ab}$. Note that $\mathcal{T}_l$ is a closed subgroup and hence the quotient is also pro-l group. Taking the quotient of the sequence 6.2 by $\mathcal{T}_l$ we obtain:

$$0 \to {\mathbb{Z}_l}^2 \to \mathcal{G}_{K,l}^{ab}/\mathcal{T}_l \to \mathrm{Cl}_l(K) \to 0.$$

Since $\mathbb{Z}_l$ is torsion free, $(\mathcal{G}_{K,l}^{ab}/\mathcal{T}_l)[\mathrm{tors}]$ maps invectively to $\mathrm{Cl}_l(K)$ which is finite. Denoting the group $\mathcal{G}_{K,l}^{ab}/\mathcal{T}_l$ by B_l we get isomorphism of topological groups[1]: $B_l \simeq B_l[\mathrm{tors}] \oplus B_l'$, where B_l' denotes the non-torsion part of B_l. Since $\mathbb{Z}_l$ is torsion free we also have the following exact sequence:

$$0 \to {\mathbb{Z}_l}^2 \to B_l' \to \mathrm{Cl}_l(K)/\phi(B_l[\mathrm{tors}]) \to 0.$$

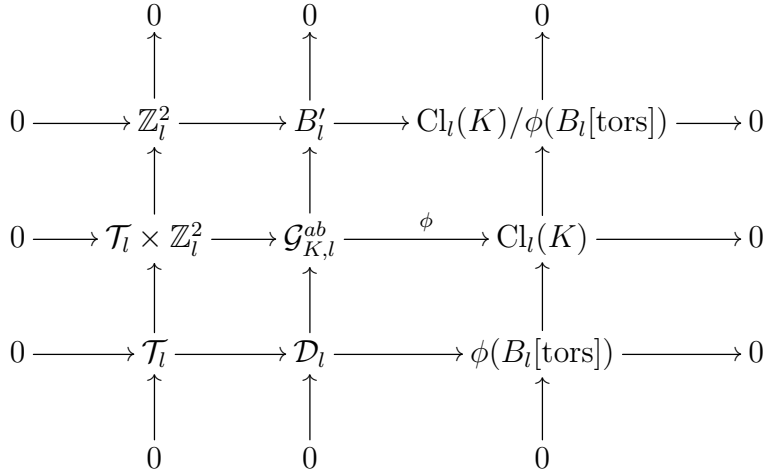
Since B_l' is torsion free this exact sequence implies that B_l' is a free $\mathbb{Z}_l$-module of rank two and hence $B_l' \simeq \mathbb{Z}_l^2$.

Let us denote the quotient map $\mathcal{G}_{K,l}^{ab} \to \mathrm{Cl}_l(K)$ by ϕ. In notations from the introduction, $\phi(B_l[\mathrm{tors}]) = \mathrm{Cl}^{split}(K)$. Consider the pre-image $\mathcal{D}_l \subset \mathcal{G}_{K,l}^{ab}$ of the group $\phi(B_l[\mathrm{tors}]) \subset \mathrm{Cl}_l(K)$. Note that $\mathcal{D}_l$ is a closed subgroup and we have the following exact sequence:

$$0 \to \mathcal{T}_l \to \mathcal{D}_l \to \phi(B_l[\mathrm{tors}]) \to 0.$$

[1]This is true because $B_l[\mathrm{tors}]$ is finite.

Summing up we have the following commutative diagram of pro-l abelian groups:



Now consider the exact sequence coming from the middle column of the above diagram:

$$0 \to \mathcal{D}_l \to \mathcal{G}_{K,l}^{ab} \to B_l' \to 0.$$

We know that $B_l' \simeq \mathbb{Z}_l^2$, but $\mathbb{Z}_l$ is a projective module and hence we could split this sequence to obtain an isomorphism $\mathcal{G}_{K,l}^{ab} \simeq \mathcal{D}_l \times B_l' \simeq \mathcal{D}_l \times \mathbb{Z}_l^2$.

□

In order to finish our proof we will show:

Lemma 6.9. *The group $\mathcal{D}_l$ is determined uniquely by the isomorphism type of $\phi(B_l[\mathrm{tors}]) = \mathrm{Cl}^{split}(K)$.*

Proof. Consider the exact sequence:

$$0 \to \mathcal{T}_l \to \mathcal{D}_l \to \mathrm{Cl}^{split}(K) \to 0.$$

We know that the closure of the torsion subgroup of $\mathcal{G}_{K,l}^{ab}$ is $\mathcal{T}_l$, and therefore $\mathcal{D}_l$ contains no torsion elements apart from elements of $\mathcal{T}_l$. I.e. that the group $\mathcal{D}_l$ satisfies both conditions of Theorem 6.2 and hence its isomorphism class is uniquely determined by $\mathrm{Cl}^{split}(K)$. □

6.3 Corollaries

In this section we will prove corollary 6.5. First of all, we already showed that given two imaginary quadratic fields K, K' different from $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ the following implication holds:

$$\mathrm{Cl}^{split}(K) \not\simeq \mathrm{Cl}^{split}(K') \Rightarrow \mathcal{G}_K^{ab} \not\simeq \mathcal{G}_{K'}^{ab}.$$

This statement allows us to reduce our question to construction of a sequence of imaginary quadratic fields K_i with $\#\,\mathrm{Cl}^{split}(K_i) \to \infty$ as $i \to \infty$. Given a finite abelian group A we denote by $r_l(A)$ the rank of its l-part i.e. the dimension of the vector space A_l over $\mathbb{Z}/l\mathbb{Z}$, where A_l is the l-primary component of A. Given an imaginary quadratic field K different from $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ we have:

Lemma 6.10. *The following inequalities hold:*

$$0 \leq r_l(\mathrm{Cl}(K)) - r_l(\mathrm{Cl}^{split}(K)) \leq 2.$$

Proof. Consider the exact sequence:

$$0 \to \mathrm{Cl}_l^{split}(K) \to \mathrm{Cl}_l(K) \to \mathrm{Cl}_l(K)/\,\mathrm{Cl}_l^{split}(K) \to 0.$$

Which implies:

$$r_l(\mathrm{Cl}(K)) = r_l(\mathrm{Cl}^{split}(K)) + r_l(\mathrm{Cl}_l(K)/\,\mathrm{Cl}_l^{split}(K)).$$

The first inequality is then obvious. For the second inequality, consider an exact sequence:

$$0 \to \mathbb{Z}_l^2 \to B_l' \to \mathrm{Cl}_l(K)/\,\mathrm{Cl}_l^{split}(K) \to 0,$$

which shows us $r_l(\mathrm{Cl}_l(K)/\,\mathrm{Cl}_l^{split}(K)) \leq 2$ and hence we are done. □

Because of the previous lemma it is enough to show that we can construct a sequence K_i with $r_2(\mathrm{Cl}(K_i)) \to \infty$. This easily follows from the following statement which goes back to Gauss' genus theory; see [19]:

Lemma 6.11. *The two rank of the class group* $\mathrm{Cl}(K)$ *of an imaginary quadratic field* $K = \mathbb{Q}(\sqrt{-d})$ *is* $\omega(d) - 1$*, where* $\omega(d)$*, denotes the number of different prime divisors of* d*.*

Finally summing up all together we obtain:

Corollary 6.12. *Let* p_n *denote the* n*-th prime number. Led* $d_n = \prod_{i=1}^{n} p_i$*. Among elements of the sequence* $K_n = \mathbb{Q}(\sqrt{-d_n})$ *of imaginary quadratic fields there are infinitely many fields with pairwise non-isomorphic abelianized absolute Galois groups* $\mathcal{G}_{K_n}^{ab}$*.*

Abstract

Artin L-functions associated to continuous representations of the absolute Galois group $\mathcal{G}_K$ of a global field K capture a lot of information about $\mathcal{G}_K$ as well as arithmetic properties of K. In the first part of the present thesis we develop basic aspects of this framework, starting from the well-known theory of arithmetically equivalent number fields which corresponds to the case of permutation representations of $\mathcal{G}$. Then, based on work of Bart de Smit, we show how to completely recover the isomorphism class of K using Artin L-functions of monomial representations, i.e. representations induced from abelian characters. This allows us to provide an alternative approach to the famous Neukirch-Uchida theorem, which is a central result in anabelian geometry. In the second part of the thesis we shift our attention towards the case of global function fields and show two different approaches to possible generalizations of the results from the first part. Finally in the last part of the dissertation we study invariants of the maximal abelian quotient $\mathcal{G}_K^{ab}$ of $\mathcal{G}$. In particular, we provide more examples of non-isomorphic imaginary quadratic number fields K whose $\mathcal{G}_K^{ab}$ share the same isomorphism class and also prove that infinitely many non-isomorphic pro-finite groups occur as $\mathcal{G}_K^{ab}$ for some K. We finish the section with a complete classification of $\mathcal{G}_K^{ab}$ in the case of global function fields.

Résumé

Les fonctions L d'Artin associées aux représentations continues du groupe de Galois absolu $\mathcal{G}_K$ d'un corps global K capturent beaucoup d'information sur $\mathcal{G}_K$ ainsi que sur les propriétés arithmétiques de K. Dans la première partie de cette thèse, nous dévelopons ce cadre, en commençant par la théorie bien connue des corps de nombres arithmétiquement équivalents, qui correspondent aux représentations de permutation de $\mathcal{G}_K$. Ensuite, en s'appuyant sur les travaux de Bart de Smit, nous montrons comment retrouver la classe d'isomorphisme de K en utilisant les fonctions L d'Artin de représentations monomiales, c'est-à-dire induites de caractères abéliens. Ceci nous permet une approche alternative au famaux théorème de Neukirch-Uchida, qui est un résultat central en géométrie anabelienne. Dans la deuxième partie de la thèse, nous nous tournons vers le cas des corps de fonctions d'une variable sur un corps fini et indiquons deux approches différentes pour des généralisations possibles des résultats de la première partie. Finalement, dans la dernière partie de la thèse, nous étudions les invariants du quotient abélien maximal $\mathcal{G}_K^{ab}$ de $\mathcal{G}_K$. En particulier, nous donnons de nouveaux examples de corps quadratiques imaginaires K non isomorphes tels que les groupes $\mathcal{G}_K^{ab}$ soient isomorphes et démontrons qu'une infinité de classes d'isomorphismes de groupes profinis apparaissent comme $\mathcal{G}_K^{ab}$ pour un certain K. Nous concluons cette section par une classification complète des $\mathcal{G}_K^{ab}$ dans le cas des corps de fonctions d'une variable sur un corps fini.

Samenvatting

Artin L -functies die zijn gekoppeld aan continue representaties van de absolute Galois-groep $\mathcal{G}_K$ van een globaal lichaam K leggen veel informatie vast over $\mathcal{G}_K$ en ook arithmetische eigenschappen van K. In het eerste deel van dit proefschrift ontwikkelen we basisaspecten van dit raamwerk uitgaande van de bekende theorie van arithmetisch equivalente getallenlichamen die overeenkomt met het geval van permutatie-representaties van $\mathcal{G}$. Vervolgens laten we, op basis van het werk van Bart de Smit, zien hoe de isomorfieklasse van K volledig geconstrueerd kan worden met behulp van Artin L-functies van monomiale representaties, d.w.z. representaties die zijn geïnduceerd door abelse karakters. Dit stelt ons in staat om een alternatieve benadering te bieden voor de beroemde stelling van Neukirch-Uchida, die een centraal resultaat is in de anabelse meetkunde. In het tweede deel van het proefschrift verleggen we onze aandacht naar het geval van globale functielichamen en laten we twee verschillende benaderingen zien voor mogelijke generalisaties van de resultaten uit het eerste deel. Ten slotte bestuderen we in het laatste deel van het proefschrift invarianten van het maximale abelse quotiënt $\mathcal{G}_K^{ab}$ van $\mathcal{G}_K$. We geven in het bijzonder meer voorbeelden van niet-isomorfe imaginaire kwadratische getallenlichamen K waarvan $\mathcal{G}_K^{ab}$ dezelfde isomorfismeklasse delen en we bewijzen ook dat er oneindig veel niet-isomorfe pro-eindige groepen voorkomen als $\mathcal{G}_K^{ab}$ voor zulke K. We eindigen de sectie met een volledige beschrijving van $\mathcal{G}_K^{ab}$ in het geval van globale functielichamen.

Acknowledgements

The present thesis has been written with the kind support of a huge number of unique people. The total amount of members in this group is so big that it would not be possible to name each and every one here, but nevertheless, I am going to make a desperate attempt to thank people who contributed the most to the existence of the present text.

First and foremost I would like to say thank you to my principal advisor, professor Bart de Smit. Bart's contribution to the text cannot be overestimated: he was always open to guide me by lighting the way in the dark wood of my mathematical adventure towards the final goal: to become an independent researcher. I agree that it is by no means an easy job to do, but I think we enjoyed every moment of our collaboration when we were working together on various mathematical puzzles that appeared attractive to us.

Secondly, I would like to express my gratitude to my co-advisor professor Karim Belabas and the reading committee members, namely professors Elisa Lorenzo García, Marc Hindry and Michael Tsfasman. I appreciate the brave decision you made to read this manuscript and I want to emphasise that it was a big pleasure for me to receive your valuable comments.

Another round of applause goes to all the faculty members of the Mathematical Institute, who surrounded and supported me during my studies at Leiden University. In particular I would like to mention professors of the research group "Algebra and Geometry", namely Bas Edixhoven, Peter Stevenhagen, Marco Streng, Hendrik Lenstra, Peter Bruin, Ronald van Luijk and professor of the probability research group Evgeny Verbitskiy from whom I learned a lot about various kinds of impressive mathematical results both directly and indirectly.

Besides the long list of professors mentioned above, the mathematical community formed around Leiden University brought to my life many exciting connections. Along the way some of these professional connections actually transformed to the form of close friendship. Just to name a few of them: Alexey Beshenov, Abtien Javanpeykar, Carlo Pagano, Maxim Mornev, Dima Shvetsov, Rosa Winter, Richard Griffon, Evgeny Goncharov, Garnet Akeyr, Liza Arzhakova and many many others. Thank you all guys for being around all this time.

Last but not least, I need to emphasise the role of the non-mathematical community whose love and care supported me during my studies. Of course, the biggest gratitude goes to my family and especially to my mother Elena who devoted a huge amount of efforts to educate me, despite all the difficulties that we were experiencing in our life. It is also hard to estimate how much I gained from the friends of mine even if sometimes hundreds or even thousands of kilometres were between us. I am immensely grateful to you: Alexey, Nikolay, Shayekh, Gerben, Tatiana, Michael, Ivan and Flera.

Curriculum Vitae

Pavel Solomatin was born on May 14, 1991 in Moscow, Russian Federation. Started from 2004 he attended experimental division of the mathematical high school No. 179, with the curriculum focusing on both computer science and mathematics.

Upon graduating in 2008 he went on to obtain a bachelor diploma in pure mathematics from the National Research University Higher School of Economics (HSE). There he fell in love with number theory and defended his bachelor thesis titled "*On Arithmetic Properties of Abelian Varieties over Finite Fields*" under scientific direction of professor Alexey Zykin.

In 2012 Pavel enrolled in the master program at HSE math department, graduating in 2014 with the thesis titled "*Curves with Many Points over Finite Fields: The Class Field Theory Approach*", which was also written under kind Alexey's guidance. During his master studies Pavel's research received support from the grant "*Arithmetic Properties of Abelian Varieties over Finite and Function Fields*" issued by the Russian Academy of Science. Directly after graduation in 2014 he received an ALGANT scholarship which allowed him to continue his mathematical studies as a Ph.D. candidate under scientific direction of professor Bart de Smit (Leiden University) and professor Karim Belabas (University of Bordeaux). Besides the scientific research Pavel was also devoting efforts to teaching various kinds of mathematical disciplines for graduate and undergraduate students. For this job he received the "*Best teacher 2013–2014*" award according to the choice of students from the HSE-NES joint bachelor program in economics. While staying in the Netherlands his teaching duties were related to assistance for multiple courses of the Dutch "Master in Mathematics" program, such as "Number Theory" and "Elliptic Curves".

Starting from February 2018 he is working full-time as a software engineer at a Dutch IT-company called Ortec. There he is applying his passion for mathematics in order to improve our world.

Bibliography

[1] Athanasios Angelakis and Peter Stevenhagen. Imaginary quadratic fields with isomorphic abelian Galois groups. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 21–39. Math. Sci. Publ., Berkeley, CA, 2013.

[2] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[3] Andrea Bandini, Ignazio Longhi, and Stefano Vigni. Torsion points on elliptic curves over function fields and a theorem of Igusa. *Expo. Math.*, 27(3):175–209, 2009.

[4] W. Bosma and J. Cannon. *Discovering Mathematics with Magma: Reducing the Abstract to the Concrete*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2007.

[5] Wieb Bosma and Bart de Smit. On arithmetically equivalent number fields of small degree. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 67–79. Springer, Berlin, 2002.

[6] John Conway, John McKay, and Allan Trojan. Galois groups over function fields of positive characteristic. *Proc. Amer. Math. Soc.*, 138(4):1205–1212, 2010.

[7] Gunther Cornelissen. Two-torsion in the Jacobian of hyperelliptic curves over finite fields. *Archiv der Mathematik*, 77(3):241–246, 2001.

[8] Gunther Cornelissen, Aristides Kontogeorgis, and Lotte van der Zalm. Arithmetic equivalence for function fields, the Goss zeta function and a generalisation. *J. Number Theory*, 130(4):1000–1012, 2010.

[9] Bart de Smit. Generating arithmetically equivalent number fields with elliptic curves. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 392–399. Springer, Berlin, 1998.

[10] Bart de Smit and Robert Perlis. Zeta functions do not determine class numbers. *Bull. Amer. Math. Soc. (N.S.)*, 31(2):213–215, 1994.

[11] Bart de Smit and Pavel Solomatin. On abelianized absolute Galois group of global function fields. *https://arxiv.org/abs/1703.05729*, 2017.

[12] Bart de Smit and Pavel Solomatin. A remark on abelianized absolute Galois group of imaginary quadratic fields. *https://arxiv.org/abs/1703.07241*, 2017.

[13] Gunther Cornelissen; Bart de Smit; Xin Li; Matilde Marcolli; Harry Smit. Reconstructing global fields from Dirichlet L-series. *arXiv: https://arxiv.org/abs/1706.04515*, 2017.

[14] Michael DiPasquale. On the order of a group containing nontrivial Gassmann equivalent subgroups. *Rose-Hulman Undergraduate Math Journal*, 10(1), 2009.

[15] Kevin D. Doerksen. On the arithmetic of genus two curves with (4,4)-split Jacobians. *PhD thesis*, 2011.

[16] Bosco Fotsing and Burkhard Külshammer. Modular species and prime ideals for the ring of monomial representations of a finite group. *Comm. Algebra*, 33(10):3667–3677, 2005.

[17] Gerhard Frey and Ernst Kani. Curves of genus 2 with elliptic differentials and associated Hurwitz spaces. In *Arithmetic, geometry, cryptography and coding theory*, volume 487 of *Contemp. Math.*, pages 33–81. Amer. Math. Soc., Providence, RI, 2009.

[18] László Fuchs. *Abelian groups*. Springer Monographs in Mathematics. Springer, Cham, 2015.

[19] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[20] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996.

[21] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier (Grenoble)*, 59(1):239–289, 2009.

[22] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[23] Ernst Kani. Discriminants of Hermitian $R[G]$-modules and Brauer's class number relation. In *Algebra and number theory (Essen, 1992)*, pages 43–135. de Gruyter, Berlin, 1994.

[24] Ernst Kani. Elliptic curves on abelian surfaces. *Manuscripta Math.*, 84(2):199–223, 1994.

[25] Ernst Kani. The number of curves of genus two with elliptic differentials. *J. Reine Angew. Math.*, 485:93–121, 1997.

[26] Irving Kaplansky. *Infinite abelian groups*. Revised edition. The University of Michigan Press, Ann Arbor, Mich., 1969.

[27] Norbert Klingen. *Arithmetical similarities*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998. Prime decomposition and finite group theory, Oxford Science Publications.

[28] James R. C. Leitzel, Manohar L. Madan, and Clifford S. Queen. Algebraic function fields with small class number. *J. Number Theory*, 7:11–27, 1975.

[29] Sidney A. Morris. *Pontryagin duality and the structure of locally compact abelian groups*. Cambridge University Press, Cambridge-New York-Melbourne, 1977. London Mathematical Society Lecture Note Series, No. 29.

[30] M. Ram Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

[31] M.R. Murty and V.K. Murty. *Non-vanishing of L-Functions and Applications*. Modern Birkhäuser Classics. Springer Basel, 2012.

[32] Kiyoshi Nagata. Artin's L-functions and Gassmann equivalence. *Tokyo J. Math.*, 9(2):357–364, 1986.

[33] Władysł aw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[34] J. Neukirch. Kennzeichnung der endlich-algebraischen Zahlkorper durch die Galoisgruppe der maximal auflosbaren Erweiterungen. *Journal fr die reine und angewandte Mathematik*, 238:135–147, 1969.

[35] J. Neukirch. Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. *Invent. Math.*, 6:296–314, 1969.

[36] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[37] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[38] Midori Onabe. On the isomorphisms of the Galois groups of the maximal Abelian extensions of imaginary quadratic fields. *Natur. Sci. Rep. Ochanomizu Univ.*, 27(2):155–161, 1976.

[39] Robert Perlis. On the class numbers of arithmetically equivalent fields. *J. Number Theory*, 10(4):489–509, 1978.

[40] Dipendra Prasad. A refined notion of arithmetically equivalent number fields, and curves with isomorphic Jacobians. *Advances in Mathematics*, 312:198 – 208, 2017.

[41] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2010.

[42] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[43] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[44] R.Perlis. On the equation $\zeta_k(s) = \zeta'_k(s)$. *Journal of Number Theory,Volume 9, Issue 3, Pages 342-360*, 1977.

[45] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[46] Jean-Pierre Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.

[47] Pavel Solomatin. L-functions of genus two abelian coverings of elliptic curves over finite fields. *arXiv: https://arxiv.org/abs/1601.05941*, 2016.

[48] Pavel Solomatin. On artin L-functions and Gassmann equivalence for global function fields. *arXiv: https://arxiv.org/abs/1610.05600*, 2016.

[49] Pavel Solomatin. A note on number fields sharing the list of Dedekind zeta-functions of abelian extensions with some applications towards the Neukirch-Uchida Theorem. *https://arxiv.org/abs/1901.09243*, 2019.

[50] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[51] D. Stuart and R. Perlis. A new characterization of arithmetic equivalence. *J. Number Theory*, 53(2):300–308, 1995.

[52] Andrew V. Sutherland. Arithmetic equivalence and isospectrality. *MIT Lecture Notes of Mini-Course in Topics in Algebra (18.708)*, 2018.

[53] H. Toyokazu and S. Seiken. *Introduction To Non-abelian Class Field Theory, An: Automorphic Forms Of Weight 1 And 2-dimensional Galois Representations*. Series On Number Theory And Its Applications. World Scientific Publishing Company, 2016.

[54] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[55] Stuart Turner. Adele rings of global field of positive characteristic. *Bol. Soc. Brasil. Mat.*, 9(1):89–95, 1978.

[56] Kôji Uchida. Isomorphisms of Galois groups. *J. Math. Soc. Japan*, 28(4):617–620, 1976.

[57] Kôji Uchida. Isomorphisms of Galois groups of algebraic function fields. *Ann. of Math. (2)*, 106(3):589–598, 1977.

[58] André Weil. Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:33–53, 1957.

[59] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

[60] Jared Weinstein. Reciprocity laws and Galois representations: recent breakthroughs. *Bull. Amer. Math. Soc. (N.S.)*, 53(1):1–39, 2016.