Global fields and their L-functions

Solomatin, P.

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.*

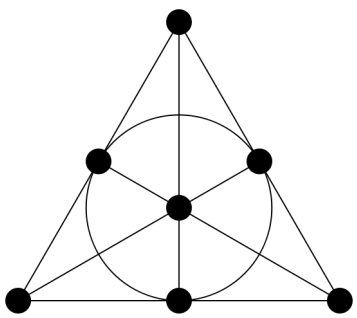
then any Gassmann triple (G, H, H') is trivial.

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:

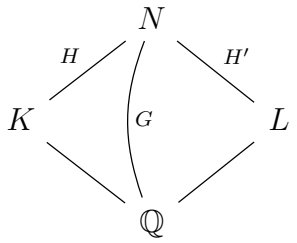
Lemma 1.22. *For a given natural number n there exists a group G with a sequence of at least 2^n pairwise non-conjugate subgroups sharing the same isomorphism class of the permutation representations.*

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.*

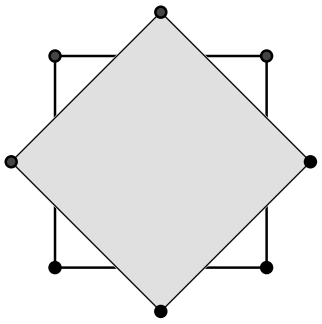
It is more convenient to provide another example of such a family for degree eight.

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

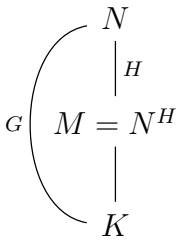
Now we state the basic properties of L-functions needed for further investigation. Let N be a finite Galois extension of a number field K. As usual we denote by G the Galois group $\mathrm{Gal}(N : K)$.

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:

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

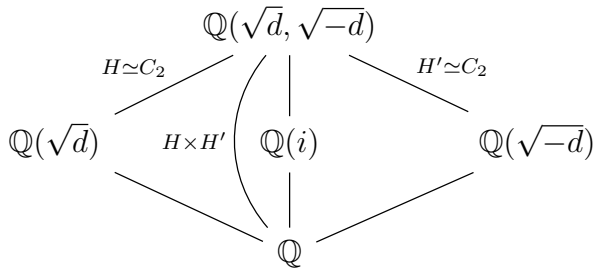
By representation theory one has $\mathrm{Ind}_{\{1\}}^G = 1 \oplus \chi$, where 1, χ denote trivial and non-trivial representations of G respectively. Therefore by the additivity property:

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

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:

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

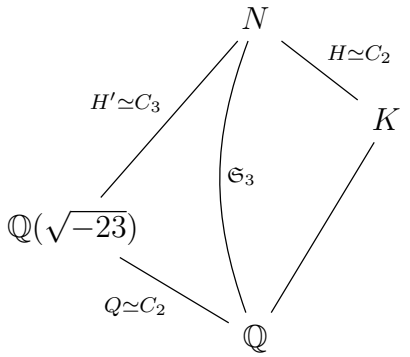
Such kind of relations were generalized by Brauer and now called Brauer relations, see [23].

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].