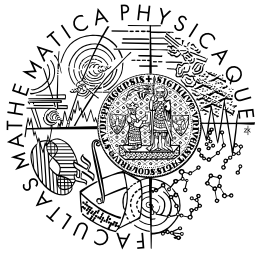

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Alexandr Beneš

Counting extensions of imaginary quadratic fields

Department of Algebra

Supervisor of the bachelor thesis: Mgr. Vítězslav Kala, Ph.D.
Study programme: Mathematics
Study branch: General Mathematics

Prague 2020

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

I would like to thank my supervisor Vítězslav Kala for his patience and helpful advice during the writing of this thesis.

Title: Counting extensions of imaginary quadratic fields

Author: Alexandr Beneš

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: The goal of this thesis is to determine the asymptotic behaviour of the number of quadratic extensions of a number field in terms of the discriminant. We will be particularly interested in extensions of imaginary quadratic number fields with odd class number. For a given number field K we will define the group of ideles $\mathbb{I}_K$ and the idele class group C_K, which capture the local behaviour of a number field. Then we use the Artin reciprocity theorem to give a correspondence of quadratic extensions and quadratic characters on C_K. When the class number is odd, quadratic characters on C_K reduce to characters on the product of groups of units of local fields. These characters can be given explicitly and we compute the discriminant of the corresponding extension from their local conductors. We put this information together in the form of a zeta function and finally use a Tauberian theorem to compute the asymptotic behaviour.

Keywords: algebraic number theory, class field theory, Cohen-Lenstra heuristics

Contents

Introduction

For every prime $\mathfrak{p}$ of a number field K we can define a local field $K_\mathfrak{p}$, which is a finte extension of the p-adic numbers $\mathbb{Q}_p$. We can put them all together to form the group of idèles $\mathbb{I}_K$. Class field theory tells us that there is a canonical homomorphism

$$\mathbb{I}_K/K^\times \to \mathrm{Gal}(\overline{K}/K)^{ab}.$$

This gives us a way to transform questions about extensions of K to questions about local fields, which we are able to solve. We can use this to count abelian extension of a number field K. Using this theorem one can estimate the asymptotic behavior of the function $a_K(n)$ which is the number of abelian extensions of K with discriminant $\leq n$ satisfying certain properties. For example in chapter 8 of [Woo14] it is shown using the Artin reciprocity that the function $a_K(n)$ for the number of quadratic extensions of $K = \mathbb{Q}$ grows as

$$a_\mathbb{Q}(n) = \frac{6}{\pi^2}n + o(n).$$

In this thesis we will extend this theorem for K an imaginary quadratic field with odd class number. We will find that

$$a_K(n) = Cn + o(n).$$

where C is a constant we can write exactly using the Dedekind zeta function of K. Simial method can be used to count cubic or higher degree extension or count extensions with certain splitting properties at a set of primes.
The main idea is to view quadratic extensions of K as open index 2 subgroups of the absolute Galois group of K (the Galois group of the algebric closure of K) and use the Artin reciprocity to transform them to subgrups of the group of idèles. These can also be seen as kernels of certain homomorphism from idèles to $\mathbb{Z}/2\mathbb{Z}$. If K has odd class number, then all such homomorphisms can be constructed as sums of homomorphisms from local fields to $\mathbb{Z}/2\mathbb{Z}$ such that they send all units of $\mathcal{O}_K$ to 0.
If the class number is odd, then there are two problems. Firstly there are homomorphisms from the class group Cl_K to $\mathbb{Z}/2\mathbb{Z}$, which would have to be taken to account. Also there would be more homomorphisms from local fields than homomorphisms from the idèles, because a certain group $\mathrm{Ext}^1(Cl_K, \mathbb{Z}/2\mathbb{Z})$ would be nonzero and to calculate it, we would need to know nontrivial information about the structure of the class group. This theorem can't also be easily extended to real quadratic fields, because the group of units of $\mathcal{O}_K$ is infinite and we would need to know, what elements generate it.
The discriminant of each extensions can be computed from the local homomorphisms. The information about the extension can be put into one function called the *counting function*. The asymptotic behaviour is then estimated from the counting function using a Tauberian theorem, if we rewrite the counting function using certain zeta and L-functions.

1. Preliminaries

We first we recall some commutative algebra and algebraic number theory and then we take a brief introduction to local fields and the group of idèles, to get our main result. A short summary is in the following sections. All proofs and more details can be found in [NS99] Chapter II.

1.1 Commutative algebra

The *localization* of a ring R by a multiplicatively closed subset S containing 1 is the ring of fractions $\frac{a}{s}$ $a \in R, s \in S$ modulo the relation $\frac{r}{d} \sim \frac{s}{e}$ iff $x(er - ds) = 0$ for some $x \in S$. The localization is denoted $S^{-1}R$. The prime ideals of $S^{-1}R$ correspond to the prime ideals of R disjoint from S by sending $S^{-1}R \supset I \mapsto I \cap R$. It also preserves the Noetherian property (i.e. if every ideal of R is finitely generated, then every ideal of $S^{-1}R$ is finitely generated). See Proposition 38(c) and (d) in Chapter 15.4 of [DF04] for the proofs.
For two k-algebras A and B, we can define their tensor product $A \otimes_k B$ as the product $A \times B$ modulo the ideal generated by elements of the form $(ra, b) - (a, rb), (a + a', b) - (a, b) - (a', b), (a, b + b') - (a, b - (a, b'))$ for all $a, a' \in A, b, b' \in B, r \in k$. This is also a k-algebra, for more information see Section 10.4 in [DF04].
The *algebraic closure* of a field K is an algebraic extension $\overline{K}/K$, where $\overline{K}$ is algebraically closed (every polynomial has a root). For a field of characteristic 0, there always exist an algebraic closure and all closures are isomorphic.

1.2 Algebraic number theory

We will review some basic algebraic number theory, see for example Chapter I. in [NS99]. Recall that for an extension of L/K of number fields with rings of integers $\mathcal{O}_L, \mathcal{O}_K$, a prime $\mathfrak{p}$ of K is nonzero prime ideal of $\mathcal{O}_K$. Since every nonzero ideal in the ring of integers factors uniquely as a product of prime ideals, the ideal $\mathfrak{p}\mathcal{O}_L$ factors as $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}$ for some distinct prime ideals $\mathfrak{q}_i$ of L. In this case we say that the $\mathfrak{q}_i$ are above $\mathfrak{p}$. The numbers e_i are called the ramification degrees and the numbers $f_i = [(\mathcal{O}_L/\mathfrak{q}_i)/(\mathcal{O}_K/\mathfrak{p})]$ (which are finite) are called degrees of inertia. For every extension L/K we have $\sum e_i f_i = [L/K]$. In particular for quadratic extensions we have three cases for every prime $\mathfrak{p}$, either $e_i = 1, f_i = 1$ or $e_i = 1, f_i = 2$ or $e_i = 2, f_i = 1$. In these cases we call the prime split, inert or ramified, respectively.
To every number field K we associate the multiplicative free abelian group generated by the nonzero prime ideals of $\mathcal{O}_K$, denoted J_K. Its elements are also called the fractional ideals. Let $c \in K$ be a nonzero element. It can be written as $\frac{a}{b}$ with $a, b \in \mathcal{O}_K$. The elements a, b define ideals with unique factorizations into distinct prime ideals $(a) = \prod_i \mathfrak{p}_i^{d_i}$ and $(b) = \prod_j \mathfrak{q}_j^{k_j}$. The nonzero ideals of $\mathcal{O}_K$ are elements of this group. Then we have a group homomorphism $K^\times \to J_K$, $c \mapsto \prod_i \mathfrak{p}_i^{d_i} \times \prod_j \mathfrak{q}_j^{-k_j}$. Elements in the image are called principal fractional ideals and the cokernel is called the *ideal class group* denoted Cl_K and a famous theo-

rem in algebraic number theory says that it is finite (Theorem 6.3 in Chapter I. [NS99]). The size of Cl_K is called the *class number* h_K.
For a number field extension L/K the *relative norm* $N_{L/K}(-)$ of a nonzero prime ideal $\mathfrak{q}$ in $\mathcal{O}_L$ is defined by $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^f$ where $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{q}$ and f is the degree of inertia of $\mathfrak{q}$ over $\mathfrak{p}$. The norm is extended to every ideal by defining the norm of an ideal as the product of norms of the prime ideals in its decomposition. The norm of the extension $K/\mathbb{Q}$ is called the *absolute norm* $N(-)$ and it is an ideal of $\mathbb{Z}$, so we can identify it with a natural number.
A number field K has r_1 embeddings into the real numbers $\tau_i : K \to \mathbb{R}$ and r_2 pairs of conjugate embeddings to the complex numbers $\sigma_j, \overline{\sigma}_j : K \to \mathbb{C}$. Then there is a homomorphism $\log_K : K \to \mathbb{R}^{r_1+2r_2}$ defined by
$a \mapsto (\log|\tau_i(a)|, \log|\mathrm{Re}(\sigma_j(a))|, \log|\mathrm{Im}(\sigma_j(a))|)$. If H is the subspace $H = \{h_i \in \mathbb{R}^{r_1+2r_2} | \sum_i h_i = 0\}$, then the unit group $\mathcal{O}_K^\times$ maps to H under $\log_K$ and the image is a complete lattice $\mathbb{Z}^{r_1+2r_2-1}$. The area of the fundamental mesh of this lattice divided by $\sqrt{r_1 + r_2}$ is called the *regulator* Reg_K of K. See [NS99] Chapter I., Sections 5 and 7 for more information.

1.3 Local fields

A valuation on a field A is a surjective function $\nu : A^\times \to \mathbb{Z}$ satisfying these conditions:

- $\nu(ab) = \nu(a) + \nu(b)$
- $\nu(a + b) \geq \min(\nu(a), \nu(b))$

One usually defines $\nu(0) = \infty$. Every valuation defines an absolute value (or norm) on A by $|a| = q^{-\nu(a)}$ for some $q > 1$. It is discrete (meaning its image in $\mathbb{R}$ is discrete outside of 0) and defines a topology on A. We say two absolute values are equivalent if they define the same topology. Choosing different q gives equivalent absolute values.
The topology defined may not be complete, but there always exists a completion $\tilde{A}$ with dense homomorphism $A \to \tilde{A}$ (Theorem 7.23 in [Mil17]). This can be done by setting $\tilde{A}$ to be the field of all Cauchy sequences module an equivalence $a \equiv b \iff a - b$ is a sequence going to zero. The absolute value on A extends to $\tilde{A}$ and is also discrete (because the absolute value of element in $\tilde{A}$ is a limit of elements in $|A|$ which is discrete).
The p-adic absolute value on $\mathbb{Q}$ for a prime p is defined for a by writing a as the product of distinct prime powers $a = p^d q_1^{e_1} \dots q_n^{e_n}$ and setting $|a| = p^{-d}$ and $|0| = 0$.

Rational numbers are not complete with respect to the p-adic absolute value. Their completion is called the p-adic numbers and denoted $\mathbb{Q}_p$. Every element of $\mathbb{Q}_p$ can be uniquelly written as an infinite sum $\sum_{n=k}^{\infty} a_n p^n$ where $k \in \mathbb{Z}$ and $a_i \in \{0, 1, \dots, p-1\}$.

Theorem 1 (Ostrowski)**.** *The only nontrivial absolute values up to equivalence on $\mathbb{Q}$ are the standard absolute value and the p-adic ones for all primes p.*

Proof. Theorem 4.2 in Chapter II. in [NS99]. □

Fields with an absolute value that possess nice properties are called local fields.

Definition 2. *A local field is a field with a nontrivial absolute value such that it is locally compact, i.e. every point has an open neighborhood the closure of which is compact.*

A field together with the topology defined by a complete valuation is a local field. We will call a local field non-archimedean if it satisfies a stronger version of the triangle inequality: $|a+b| \leq \max(|a|, |b|)$ otherwise it is archimedean.

Theorem 3. *Every local field A of one of the following types*

- *if A is archimedean, then it is isomorphic to $\mathbb{R}$ or $\mathbb{C}$*
- *if A is non-archimedean and of characteristic 0, then it is isomorphic to a finite extension of some $\mathbb{Q}_p$*
- *if A is non-archimedean and of characteristic p, then it is isomorphic to a finite extension of $\mathbb{F}_p((t))$ (the ring of formal Laurent series with coefficients in $\mathbb{F}_p$)*

Proof. Proposition 5.2 in Chapter II. in [NS99]. □

For a non-archimedean local field A we define the ring of integers $\mathcal{O}_A = \{x \in A : |x| \leq 1\}$, its maximal ideal $\mathfrak{m} = \{x \in A : |x| < 1\}$ and the residue field $\kappa_A = \mathcal{O}_A/\mathfrak{m}_A$ which is finite. The discreteness of the norm implies that the maximal ideal is principal and its generator is called uniformizer π. The absolute value is usually normalized so that the uniformizer has norm q^{-1} where q is the cardinality of the residue field. The units in $\mathcal{O}_A$ are exactly the elements with $|a| = 1$. For example for $\mathbb{Q}_p$ the ring of integers is called the p-adic integers $\mathbb{Z}_p$ and the maximal ideal is generated by p.

1.4 Groups of units of local fields

For our main result we will need to know more about the structure of the group of units of local fields. For a local field A we define the n-th unit group $\mathcal{U}^{(n)} = 1+\mathfrak{m}^n$ and $\mathcal{U} = \mathcal{O}^\times = \mathcal{U}^{(0)}$.

Theorem 4. *We have $A^\times \cong (\pi) \times \mathcal{U} \cong (\pi) \times \mathcal{U}/\mathcal{U}^{(1)} \times \mathcal{U}^{(1)}$ and the quotients*

$$\mathcal{U}/\mathcal{U}^{(n)} \cong (\mathcal{O}/\mathfrak{m}^n)^\times \text{ and } \mathcal{U}^{(n)}/\mathcal{U}^{(n+1)} \cong \mathcal{U}/\mathfrak{m}$$

for $n \geq 1$.

Proof. See 3.10 and 5.3 in Chapter II. in [NS99]. □

Theorem 5. *For a non-archimedean local field A of characteristic 0 there is an isomorphism*

$$\exp : \mathcal{U}^{(n)} \to \mathfrak{m}^n$$

with the inverse log *for* $n > \frac{e}{p-1}$ *where* p *is the characteristic of the residue field and* e *is the normalized valuation of* p*. The functions are given by the power series*

$$\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}, \quad \log(1+x) = \sum_{k=0}^{\infty} \frac{(-1)^k x^k}{k}$$

which converge on their domain of definition.

Proof. Propositition 5.5 in Chapter II: in [NS99]. □

We can put this together with the fact $\mathfrak{m}^n = (\pi^n)\mathcal{U} \cong \mathcal{O} \cong \mathbb{Z}_p^{[A/\mathbb{Q}_p]}$ as additive groups to get

Theorem 6. *For a local field* A *of characteristic 0 and its ring of integers* $\mathcal{O}_A$ *we have:*

$$A^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/(p^a)\mathbb{Z} \times \mathbb{Z}_p^d$$
$$\mathcal{O}_A^\times \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/(p^a)\mathbb{Z} \times \mathbb{Z}_p^d$$

where p *is the characteristic of the residue field and* q *is its order,* d *is the degree of* A *over* $\mathbb{Q}_p$ *and* a *is some integer.*

Proof. Proposition 5.7 in Chapter II. in [NS99]. □

1.5 Places

We will denote a number field by K and its ring of integers by $\mathcal{O}_K$ or just $\mathcal{O}$. Recall that a ring being Noetherian means that every ideal is finitely generated. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ consider the localization $\mathcal{O}_\mathfrak{p} = (\mathcal{O}\backslash\mathfrak{p})^{-1}\mathcal{O}$. The ring $\mathcal{O}$ is Noetherian, integrally closed and is of Krull dimension 1 (every nonzero prime ideal is maximal). The local ring $\mathcal{O}_\mathfrak{p}$ is Noetherian since localization preserves this property. The prime ideals of $S^{-1}R$ correspond to the prime ideals of R disjoint from S. Therefore the only prime ideals of $\mathcal{O}_\mathfrak{p}$ are the zero ideal and $\mathfrak{p}\mathcal{O}_\mathfrak{p}$, in other words $\mathcal{O}_\mathfrak{p}$ is a local Noetherian domain. It is also integrally closed since if $\frac{a}{b}$ in the field of fractions of $\mathcal{O}$ is a root of $x^n + \frac{c_1}{s_1}x^{n-1} + \cdots + \frac{c_n}{s_n} = 0$ where $s_i \notin \mathfrak{p}$ then $\frac{sa}{b}$, where $s = \prod s_i$, solves a monic polynomial with coefficients in $\mathcal{O}$ and so $\frac{sa}{b} = \sigma \in \mathcal{O}$ and $\frac{a}{b} = \frac{\sigma}{s} \in \mathcal{O}_\mathfrak{p}$. Thus R satisfies one of the equivalent conditions of being a discrete valuation ring (DVR), defined by the equivalent conditions below.

Theorem 7. *The following are equivalent:*

- R *is a local Noetherian domain of Krull dimension 1 and integrally closed*
- R *is a unique factorization domain with one irreducible element up to associates*

Proof. Theorem 7 in Chapter 16.2 in [DF04]. □

This means R only has one prime ideal $\mathfrak{p}$ which is principal and every ideal is its power. We can define a discrete valuation on $\mathcal{O}$ by setting $\nu(x)$ to be such that $(x) = \mathfrak{p}^{\nu(x)}$. It can be extended to K by $\nu(a/b) = \nu(a) - \nu(b)$. We can complete K with respect to the absolute value induced by this valuation and we get a non-archimedean characteristic 0 local field $K_\mathfrak{p}$.

Prime ideals of $\mathcal{O}$ are also called finite places. We can also define infinite places:

Definition 8. *A real infinite place of K is an embedding $\tau : K \to \mathbb{R}$. A complex infinite place is a pair of conjugate embeddings $\sigma, \bar{\sigma} : K \to \mathbb{C}$ that are not real.*

Note that the number of real plus twice the number of complex embeddings is equal to the degree of the number field K. To each infinite place we associate the local field $\mathbb{R}$ or $\mathbb{C}$ if it is real or complex respectively. The number field is embedded in the local field by the corresponding embedding.

1.6 Extensions of local fields

For an extension of number fields L/K and primes $\mathfrak{q}$ of L above $\mathfrak{p}$ (this means that $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{q}$), the local fields $L_\mathfrak{q}$ and $K_\mathfrak{p}$ form an extension with properties that tells us information about the primes. For proofs of these theorems see Chapter 7 and 8 of [Mil17].

Definition 9. *If A/B is an extension of non-archimedean characteristic 0 local fields with normalized valuations and uniformizers π_A, π_B,*
then we define the degree of inertia as the degree of the extension of finite fields $f_{A/B} = [\kappa_A/\kappa_B] = [(\mathcal{O}_A/(\pi_A))/(\mathcal{O}_B/(\pi_B))]$ and the ramification index as $e_{A/B} = \nu_A(\pi_B)$. An extension is unramified *if the degree of ramification is 1.*

Theorem 10 (Local field extensions)**.** *For an extension of number fields L/K and nonzero primes $\mathfrak{p} \subset \mathcal{O}_K$ and $\mathfrak{q} \subset \mathcal{O}_L$ such that $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$ we have an extension of local fields $L_\mathfrak{q}/K_\mathfrak{p}$. If $\mathfrak{q}_i$ are all the primes of L above $\mathfrak{p}$, then $L \otimes_K K_\mathfrak{p} \cong \prod L_{\mathfrak{q}_i}$. Furthermore the degree of inertia of the local field extension is equal to the degree of inertia of the primes and the same for the ramification index.*

Proof. See Proposition 8.2 in [Mil17]. □

Theorem 11. *Finite unramified extensions L/K of non-archimedean local field K correspond to finite extensions of the residue field $\kappa_K = \mathcal{O}_K/(\pi_K)$ by sending $L \mapsto \kappa_L = \mathcal{O}_L/(\pi_L)$ and if $\kappa_L = \kappa_K[X]/(f(X))$, then $L = K[X]/(\overline{f}(X))$ for some lift $\overline{f}(X)$ of $f(X)$ to $K[X]$.*

Proof. Proposition 7.50 in [Mil17]. □

1.7 Idèles

We follow Chapter VI of [NS99]. We have a number field K and the set of its places $\mathfrak{p}$ and the corresponding local fields $K_\mathfrak{p}$. The group of idèles is an object $\mathbb{I}_K$ that collects all the local fields into one.

Definition 12. *The group of idèles is defined*

$$\mathbb{I}_K = \hat{\prod}_{\mathfrak{p}\ places} K_{\mathfrak{p}}^{\times} = \{(a_{\mathfrak{p}}) \in \prod_{\mathfrak{p}\ places} K_{\mathfrak{p}}^{\times} | \textit{all but finitely many } a_{\mathfrak{p}} \textit{ are in } \mathcal{U}_{\mathfrak{p}}\}$$

We can put a topology on idèles by defining a system of neighbourhoods of 1 to be the sets:

$$\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} \mathcal{U}_{\mathfrak{p}}$$

where S is a finite set of places including the infinite ones and $W_{\mathfrak{p}}$ are systems of neighbourhoods of 1 in $K_{\mathfrak{p}}^{\times}$. Systems of neighbourhoods of other points are obtained by translations.
From the inclusions $K \subset K_{\mathfrak{p}}$ we get the diagonal embedding $K^{\times} \to \mathbb{I}_K$. The quotient $\mathbb{I}_K/K$ is called the idèle class group C_K and it inherits the quotient topology from $\mathbb{I}_K$ (open sets in C_K are the ones whose preimage is open in $\mathbb{I}_K$). There is a natural homomorphism $\mathbb{I}_K \to J_K, (a_i) \mapsto \prod_{\mathfrak{p}\text{ finite}} \mathfrak{p}^{\nu_{\mathfrak{p}}(a_{\mathfrak{p}})}$. It is obviously surjective. This homomorphism factorizes to a surjection $C_K \to Cl_K$ since $K^{\times}$ maps exactly to principal fractional ideals.

For a set of places S we have a subgroup of idèles $\mathbb{I}_K^S = \prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}\notin S} \mathcal{U}_{\mathfrak{p}}$. If S is the set of infinite places we will denote it by $\mathbb{I}_K^{\infty}$.

Theorem 13. *There is an exact sequence*

$$0 \longrightarrow \mathbb{I}_K^{\infty} K^{\times}/K^{\times} \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0$$

Proof. See Proposition 1.3 in Chapter VI. in [NS99]. □

Note that by the second isomorphism theorem $\mathbb{I}_K^{\infty} K^{\times}/K^{\times} \cong \mathbb{I}_K^{\infty}/(\mathbb{I}_K^{\infty} \cap K^{\times})$.

Definition 14. *The absolute Galois group $G(K)$ of a field K of characteristic 0 is the Galois group of the algebraic closure $\overline{K}$. It can be given a topology whose open neighbourhoods of 1 are the subgroups $\mathrm{Gal}(\overline{K}/L)$ where L is a finite Galois extension of K. This makes $G(K)$ into a topological group (multiplication and inversion are continuous). Open subgroups of $G(K)$ correspond to finite extensions of K and closed subgroups correspond to all extensions of K. For more details see Chapter 7 of [Mil20].*

Definition 15. *For a group G its* abelization *G^{ab} is its largest abelian quotient, that is if $[G,G]$ is the commutator subgroup, then $G^{ab} = G/[G,G]$. It is clearly abelian and there is a surjection $G \to G^{ab}$ and every group homomorphism $G \to H$ to an abelian group H factors through G^{ab}.*

Idèles can be used to conveniently formulate the main result of class field theory: the global Artin reciprocity.

Theorem 16 (Artin reciprocity)**.** *There is a continuous homomorphism from the idèle class group of a number field to the abelization of its absolute Galois group*

$$C_K \to \mathrm{Gal}(K)^{ab}$$

called the Artin map. In particular every subgroup of C_K of finite index corresponds to an abelian extension L/K. Furthermore this homomorphism is surjective and its kernel is the largest connected component of C_K that includes 1.

Proof. Chapter V.5 of [Mil13]. □

This powerful result tells us that abelian extensions of K can be described by the idèle class group.

2. Counting extensions

2.1 Field extensions

In this section we will assume that K is an imaginary quadratic number field and that the class number of K is odd. We will use some basic abelian group cohomology, an introduction to which can be found in Chapter 17 of [DF04]. For an exact sequence of abelian groups

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

and another abelian group D the contravariant functor $\mathrm{Hom}(-, D)$ is left exact, that is the sequence

$$0 \longrightarrow \mathrm{Hom}(C, D) \longrightarrow \mathrm{Hom}(B, D) \longrightarrow \mathrm{Hom}(A, D)$$

is exact. There exist functors $\mathrm{Ext}^i(-, D), i \geq 0$, where $\mathrm{Ext}^0(-, D) = \mathrm{Hom}(-, D)$, such that we have a long exact sequence

$$0 \xrightarrow{c_0} \mathrm{Hom}(C, D) \xrightarrow{b_0} \mathrm{Hom}(B, D) \xrightarrow{a_0} \mathrm{Hom}(A, D) \xrightarrow{c_1}$$

$$\xrightarrow{c_1} \mathrm{Ext}^1(C, D) \xrightarrow{b_1} \mathrm{Ext}^1(B, D) \xrightarrow{a_1} \mathrm{Ext}^1(A, D) \xrightarrow{c_2}$$

$$\cdots$$

$$\xrightarrow{c_i} \mathrm{Ext}^i(C, D) \xrightarrow{b_i} \mathrm{Ext}^i(B, D) \xrightarrow{a_i} \mathrm{Ext}^i(A, D) \xrightarrow{c_{i+1}} .$$

The functors $\mathrm{Ext}^i(A, D)$ can be computed via a free resolution of A

$$\cdots \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} A \longrightarrow 0$$

by applying the functor $\mathrm{Hom}(-, D)$

$$0 \longrightarrow \mathrm{Hom}(F_0, D) \xrightarrow{g_0} \mathrm{Hom}(F_1, D) \xrightarrow{g_1} \mathrm{Hom}(F_2, D) \xrightarrow{g_2} \cdots .$$

The groups Ext^i are the cohomology groups of this complex, that is $\mathrm{Ext}^i(A, D) = \mathrm{im}(g_i)/\ker(g_{i-1})$.

We can use the Artin reciprocity to classify all quadratic extensions of an imaginary quadratic number field K. All quadratic extensions are abelian. By Galois theory they correspond to index 2 (necessarily normal) open subgroups of $G(K)$, the absolute Galois group of K. All finite extensions of K correspond to open subgroups of $G(K)$ with finite index. Its commutator $\Gamma = [G(K), G(K)]$ is a normal subgroup which is contained in all normal subgroups H such that $G(K)/H$ is abelian. So all index 2 open subgroups correspond to index 2 open subgroups that lie in $G(K)^{ab} = G(K)/\Gamma$ or equivalently continuous surjective homomorphisms that lie in $\mathrm{Hom}(G(K)^{ab}, \mathbb{Z}/2\mathbb{Z})$. We will call $\mathrm{Hom}_c(G(K)^{ab}, \mathbb{Z}/2\mathbb{Z})$ the subgroup of continuous homomorphisms. Now we use the Artin reciprocity to transform this to homomorphisms to $\mathbb{Z}/2\mathbb{Z}$ from the idèle class group.

Theorem 17. *The inclusion $\mathbb{I}_K^\infty K^\times/K^\times \to C_K$ induces an isomorphism* $\mathrm{Hom}(C_K, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}(\mathbb{I}_K^\infty K^\times/K^\times, \mathbb{Z}/2\mathbb{Z})$ *for K with odd class number (not necessarily imaginary quadratic).*

Proof. We have the exact sequence

$$0 \longrightarrow \mathbb{I}_K^\infty K^\times/K^\times \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0.$$

We will apply the left exact functor $\mathrm{Hom}(-, \mathbb{Z}/2\mathbb{Z})$ to the sequence and use the property of Ext functors:

$$\mathrm{Hom}(Cl_K, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathrm{Hom}(C_K, \mathbb{Z}/2\mathbb{Z}) \longrightarrow$$

$$\longrightarrow \mathrm{Hom}(\mathbb{I}_K^\infty K^\times/K^\times, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathrm{Ext}^1(Cl_K, \mathbb{Z}/2\mathbb{Z})$$

The edge terms are 0 as we will now show. Because Cl_K is finite and of odd order $Cl_K \cong \prod_{i=1}^n \mathbb{Z}/p_i^{a_i}\mathbb{Z}$, so we have a free resolution

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^n \longrightarrow Cl_K$$

where M is the diagonal matrix $M = \mathrm{diag}(p_1^{a_1}, \ldots, p_n^{a_n})$.
By applying $\mathrm{Hom}(-, \mathbb{Z}/2\mathbb{Z})$ to the resolution we get:

$$0 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^n \xrightarrow{\tilde{M}} (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow 0$$

The map $\tilde{M}$ takes $h \in \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^n$ to $h \circ M \in \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^n$. This map is the identity because M has odd numbers on the diagonal and multiplication by odd numbers is the identity on $\mathbb{Z}/2\mathbb{Z}$. So the cohomology groups of the chain above are 0 (it is exact), which are exactly $\mathrm{Ext}^0(Cl_K, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Hom}(Cl_K, \mathbb{Z}/2\mathbb{Z})$ and $\mathrm{Ext}^1(Cl_K, \mathbb{Z}/2\mathbb{Z})$. □

We need to restrict ourselves to continuous homomorphisms. The topology on $\mathbb{I}_K$ induces the subset topology on $\mathbb{I}_K^\infty$ (open sets are the sets that are intersections of open sets in $\mathbb{I}_K$ with $\mathbb{I}_K^\infty$) and the quotient topology on $\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times)$ (open sets are those whose preimage is open in $\mathbb{I}_K^\infty$). Note that we have $\mathbb{I}_K^\infty K^\times/K^\times \cong \mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times)$.

Theorem 18. *There is an isomorphism of continuous homomorphisms* $\mathrm{Hom}_c(C_K, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}_c(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z})$ *for K with odd class number, where* $\mathrm{Hom}_c(A, B)$ *is the group of continuous homomorphisms from A to B.*

Proof. From the previous theorem we have a bijection of all homomorphisms $\mathrm{Hom}(C_K, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}(\mathbb{I}_K^\infty K^\times/K^\times, \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Hom}(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z})$. The inclusion map $\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times) \to C_K$ is continuous, so a continuous homomorphism maps to a continuous homomorphism. So there is a map $\mathrm{Hom}_c(C_K, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}_c(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z})$ and it is injective.
If the preimage of $\chi \in \mathrm{Hom}_c(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z}) \subset \mathrm{Hom}(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z})$ is $\nu \in \mathrm{Hom}(C_K, \mathbb{Z}/2\mathbb{Z})$, it is enough to prove that the kernel of ν is open so that ν is continuous. Because $\mathbb{I}_K^\infty$ is open in $\mathbb{I}_K$ (every point $a \in \mathbb{I}_K^\infty$ has an open neighbourhood $a \prod_{\mathfrak{p} \text{ infinite}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p} \text{ finite}} \mathcal{U}_\mathfrak{p}$), we have that $\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times)$ is open in C_K (its preimage in $\mathbb{I}_K$ is $\mathbb{I}_K^\infty$). The kernel H of χ is open in $\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times)$ and thus in C_K. The kernel of ν includes H and so it is a union of cosets of H in C_K and therefore open. □

Lemma 19. *There is a bijection between quadratic extensions of any number field K and continuous surjective homomorphisms $C_K \to \mathbb{Z}/2\mathbb{Z}$ given by the Artin map.*

Proof. Quadratic extensions of K correspond to open index 2 subgroups of $G(K)$. If $\mathcal{O}$ is the connected component of 1 in C_K, then the Artin map gives an isomorphism $C_K/\mathcal{O} \to G(K)$. This gives correspondence of open index 2 subgroups of $G(K)$ and $C_K/\mathcal{O}$. These subgroups of $C_K/\mathcal{O}$ can be seen as kernels of continuous surjective homomorphisms $C_K/\mathcal{O} \to \mathbb{Z}/2\mathbb{Z}$. These correspond to continuous surjective homomorphisms $C_K \to \mathbb{Z}/2\mathbb{Z}$ since the connected component of 1 is always mapped to 0 by continuity. □

We will now look at $Hom(\mathbb{I}_K^\infty, \mathbb{Z}/2\mathbb{Z})$ with $\mathbb{I}_K^\infty \cap K^\times$ in the kernel. The elements of $\mathbb{I}_K^\infty \cap K^\times$ all generate the unit ideal. Therefore they are exactly the units of $\mathcal{O}_K$ which are $\{+1, -1\}$ if $K \neq \mathbb{Q}[i], \mathbb{Q}[e^{2\pi/3}]$.

Lemma 20. *For an imaginary quadratic number field K, continuous homomorphisms $\mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$ are finite sums of local homomorphisms $\mathcal{U}_\mathfrak{p} \to \mathbb{Z}/2\mathbb{Z}$ for some distinct primes $\mathfrak{p}$ of K. More explicitely $\chi = \sum_\mathfrak{p} \chi_\mathfrak{p}$ where $\chi_\mathfrak{p}$ is χ composed with the inclusion $\mathcal{U}_\mathfrak{p} = (1, \dots, \mathcal{U}_\mathfrak{p}, \dots, 1) \to \mathbb{I}_K^\infty$.*

Proof. Composition with the inclusion $\mathcal{U}_\mathfrak{p} = (1, \dots, \mathcal{U}_\mathfrak{p}, \dots, 1) \to \mathbb{I}_K^\infty$ induces homomorphisms $\chi_\mathfrak{p} : \mathcal{U}_\mathfrak{p} \to \mathbb{Z}/2\mathbb{Z}$. The kernel of the homomorphism $\chi : \mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$ is open, so there is a finite set S of primes such that the kernel includes $\prod_{\mathfrak{p}\in S} W_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} \mathcal{U}_\mathfrak{p}$, so all but finitely many $\chi_\mathfrak{p}$ are trivial and $\chi(\dots, a_\mathfrak{p}, \dots) = \prod_\mathfrak{p} \chi_\mathfrak{p}(a_\mathfrak{p})$. The local field at the infinite place $\mathbb{C}^\times$ is always mapped to 0 (since every element in $\mathbb{C}^\times$ has a square root), so the sum only includes finite primes.
Conversely every finite sum of local homomorphisms gives a continuous homomorphism as we will show. Let $\chi = \sum_{\mathfrak{p}\in S} \chi_\mathfrak{p}$. As we will see in Lemma 23, every local homomorphism $\chi_\mathfrak{p} : \mathcal{U}_\mathfrak{p} \to \mathbb{Z}/2\mathbb{Z}$ has some subgroup $\mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})}$ in the kernel and if S is the set of primes in the sum, then every element g in the kernel has an open neighbourhood $g \prod_{\mathfrak{p}\in S} \mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})} \times \prod_{\mathfrak{p}\notin S} \mathcal{U}_\mathfrak{p}$, so the kernel is open. □

All these theorems can be summarized as:

Theorem 21. *Quadratic extensions of an imaginary quadratic number field K with odd class number are in bijection with finite sums $\chi : \mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$, that can be written as sums $\chi = \sum_\mathfrak{p} \chi_\mathfrak{p}$ of homomorphisms $\chi_\mathfrak{p} : \mathcal{U}_\mathfrak{p} \to \mathbb{Z}/2\mathbb{Z}$ with $\mathbb{I}_K^\infty \cap K^\times$ in the kernel of χ and $\chi_\mathfrak{p}$ is χ composed with the inclusion $\mathcal{U}_\mathfrak{p} = (1, \dots, \mathcal{U}_\mathfrak{p}, \dots, 1) \to \mathbb{I}_K^\infty$.*

2.2 Conductors

Now we need to know how can we compute the discriminant of a number field defined by such homomorphisms. We can do it using conductors.

Definition 22. *For a homomorphism $\chi_\mathfrak{p} : \mathcal{U}_\mathfrak{p} \to \mathbb{C}^\times$ we define the local Artin conductor to be the smallest integer $f_{\chi_\mathfrak{p}}$ such that $\mathcal{U}_\mathfrak{p}^{(f_{\chi_\mathfrak{p}})} \subset \ker \chi_\mathfrak{p}$. We define the global Artin conductor $\mathfrak{f}$ of a homomorphism $\chi : G(K)^{ab} \to \mathbb{C}^\times$ as $\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{p}^{\mathfrak{f}_{\chi_\mathfrak{p}}}$ where $\chi_\mathfrak{p}$ are the homomorphisms induced from χ by the map $\mathcal{U}_\mathfrak{p} = (1, \dots, \mathcal{U}_\mathfrak{p}, \dots, 1) \to \mathbb{I}_K \to C_K \to G(K)^{ab}$.*

We can interprete the group $\mathbb{Z}/n\mathbb{Z}$ as a subgroup of $\mathbb{C}^\times$ generated by the n-th roots of unity. In our case χ is a homomorphism $\chi : G(K)^{ab} \to \mathbb{Z}/2\mathbb{Z} \cong \{+1, -1\} \subset \mathbb{C}^\times$.

Lemma 23. *For a character $\chi : \mathcal{U}_\mathfrak{p} \to \mathbb{Z}/n\mathbb{Z}$ the conductor is finite.*

Proof. We have to show that some $\mathcal{U}_\mathfrak{p}^{(m)}$ is in the kernel of χ. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, the power $(\mathcal{U}_\mathfrak{p})^n$ is in the kernel. From Theorem 5 there is an isomorphism $\log : \mathcal{U}_\mathfrak{p}^{(k)} \cong (\pi)^k$ for k larger than some constant l, where π is the uniformizer of $K_\mathfrak{p}$. We find that $\mathcal{U}_\mathfrak{p}^{(k)} \subset (\mathcal{U}_\mathfrak{p})^n$ since every element $\log(a) \in (\pi)^k$ has an n-th root $\log(a)/n \in (\pi)^{k-\nu_\mathfrak{p}(n)} \cong \mathcal{U}_\mathfrak{p}^{(k-\nu_\mathfrak{p}(n))}$ if we choose k so that $k - \nu_\mathfrak{p}(n) > l$. Therefore all elements in $\mathcal{U}_\mathfrak{p}^{(k)}$ are n-th powers, so $\mathcal{U}_\mathfrak{p}^{(k)} \subset (\mathcal{U}_\mathfrak{p})^n$. □

If the character is a sum, the conductor is computable from the summands.

Theorem 24. *Let χ be a sum of local characters $\chi = \sum_\mathfrak{p} \chi_\mathfrak{p}$ over distinct primes, like in Theorem 21. The conductor of χ is $\prod_\mathfrak{p} \mathfrak{p}^{f_\mathfrak{p}}$, where $f_\mathfrak{p}$ is the local conductor of $\chi_\mathfrak{p}$.*

Proof. The characters $\chi_\mathfrak{p}$ are obtained from χ by composition with the inclusion $\mathcal{U}_\mathfrak{p} = (1, \ldots, \mathcal{U}_\mathfrak{p}, \ldots, 1) \to \mathbb{I}_K$, so this holds by the definition of the conductor. □

Definition 25. *The relative discriminant of a Galois number field extension L/K is the ideal $\mathfrak{d}_{L/K}$ of $\mathcal{O}_K$ generated by $d(b_1, b_2, \ldots, b_n)$ where b_i is an basis of L over K with $b_i \in \mathcal{O}_L$ and $d(b_1, b_2, \ldots, b_n)$ is the determinant $\det(\sigma_i(b_j))^2$ with $\sigma_i \in \mathrm{Gal}(L/K)$. The relative discriminant $\mathfrak{d}_{K/\mathbb{Q}}$ is a principal ideal of $\mathbb{Z}$ and we can interprete it as a natural number called the absolute discriminant of K.*

The relationship between conductor and discriminant is given by the following formula.

Theorem 26. *For an abelian number field extension L/K the relative discriminant $\mathfrak{d}_{L/K}$ is given by*

$$\mathfrak{d}_{L/K} = \prod_{\chi \in \mathrm{Char}(\mathrm{Gal}(L/K))} \mathfrak{f}_\chi$$

where $\mathrm{Char}(G)$ is the set of characters of G, that is homomorphisms $G \to \mathbb{C}^\times$.

Proof. Can be found in [NS99], VII.11.9. □

If L/K is a quadratic extension, $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ and there are only 2 characters with one trivial. The trivial character has conductor 1. If $\chi : G(K) \to \mathbb{Z}/2\mathbb{Z}$ is a continuous character and L is the number field corresponding to the open subgroup $\ker(\chi)$ by the Galois correspondence, then it factors as $G(K) \to G(K)/\ker(\chi) = \mathrm{Gal}(L/K) \to \mathbb{Z}/2\mathbb{Z}$ and hence χ gives the nontrivial character on $\mathrm{Gal}(L/K)$ so we can compute its conductor locally and thus get the relative discriminant of L/K. The absolute discriminant of L is then easily computable.

Theorem 27. *Given a tower of number fields $L/K/S$ then the relative discriminant of L/S can be computed as*

$$\mathfrak{d}_{L/S} = N_{K/S}(\mathfrak{d}_{L/K}) \mathfrak{d}_{K/S}^{\deg L/K}$$

where $N_{K/S}(-)$ is the ideal norm of K/S.

Proof. See [NS99] III.2.10. □

Let's calculate the conductor of local fields for our quadratic imaginary number field K. We will start with the odd primes.

Lemma 28. *If $\mathfrak{p}$ is a prime of K not above 2 (i.e. $\mathfrak{p} \cap \mathbb{Z} = (p)$ for an odd prime p), then $\mathcal{U}_\mathfrak{p} \cong \mathbb{Z}/(p^i-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ where i is the degree of inertia of $\mathfrak{p}$ in $K/\mathbb{Q}$. The number d is 1 if $\mathfrak{p}$ is split and 2 if inert or ramified and a is some integer.*

Proof. We know from Theorem 10 that $K_\mathfrak{p}$ is an extension of $\mathbb{Q}_p$ and the degree of inertia and ramification is the same as for $\mathfrak{p}$ in $K/\mathbb{Q}$. We will use Theorem 6. From this theorem we know that i is the degree of inertia. The number d is the degree of $K_\mathfrak{p}/\mathbb{Q}_p$ is using Theorem 10 the ramification degree times the inertia degree. □

We can see that there are only 2 local characters for primes not above 2:

Lemma 29. *If $\mathfrak{p}$ is a prime not above 2, then there are two characters on $\mathcal{U}_\mathfrak{p}$ one of which is trivial.*

Proof. There are no nontrivial homomorphisms to $\mathbb{Z}/2\mathbb{Z}$ from $\mathbb{Z}/p^a\mathbb{Z}$ since it has odd size and neither from $\mathbb{Z}_p$, since $\frac{1}{2} \in \mathbb{Z}_p$ because $\frac{1}{2} \in \mathbb{Q}_p$ and $\nu_p(\frac{1}{2}) = 0$ for odd p. Finally there is a nontrivial homomorphism from $\mathbb{Z}/(p^i-1)\mathbb{Z}$ with kernel $\frac{(p^i-1)}{2}\mathbb{Z}/(p^i-1)\mathbb{Z}$ since $2|(p^i-1)$. □

The conductors of these local characters are easily computable:

Lemma 30. *If $\mathfrak{p}$ is prime not above 2, then the local conductor of the trivial local character on $\mathcal{U}_\mathfrak{p}$ is 0 and for the nontrivial one with kernel $\frac{(p^i-1)}{2}\mathbb{Z}/(p^i-1)\mathbb{Z}$ it is 1.*

Proof. The trivial one has kernel $\mathcal{U}_\mathfrak{p} = \mathcal{U}_\mathfrak{p}^{(0)}$ and the nontrivial one factors through $\mathcal{U}_\mathfrak{p}^{(1)}$ since $\mathcal{U}_\mathfrak{p}/\mathcal{U}_\mathfrak{p}^{(1)} \cong \mathbb{Z}/(p^i-1)\mathbb{Z}$ by Theorem 4. □

If $\mathfrak{p}$ is above 2, then we have three cases depending whether 2 is split, ramified or inert in K. Notice that 2 can't be ramified if K is imaginary quadratic with odd class number unless $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$.

Theorem 31. *The prime 2 is not ramified in the extension $K/\mathbb{Q}$, where K is quadratic imaginary with odd class number unless $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$.*

Proof. We will show that the ideal $2\mathcal{O}_k$ cannot be written as a principal ideal squared. If the only units in $\mathcal{O}_K$ are +1,-1, then 2 is associated with a square only if $2 = x^2$ or $-2 = x^2$ for some $x \in \mathcal{O}_K$. The first case is not possible since K is imaginary and the second case is possible only in $\mathbb{Q}(\sqrt{-2})$. If there are more units then $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$ and for $\mathbb{Q}(\sqrt{-3})$ 2 is inert. If $(2) = \mathfrak{q}^2$ for some non-principal ideal $\mathfrak{q}$, then it has order 2 in the class group, which is a contradiction. □

Lemma 32. *If 2 is split, we have two primes $\mathfrak{p}$ and $\mathfrak{q}$ above 2 and $\mathcal{U}_I \cong \mathbb{Z}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ for $I = \mathfrak{p}, \mathfrak{q}$. If 2 is inert, we have $\mathcal{U}_2 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$.*

Proof. We can use Theorem 10 to see that K_I is isomorphic to $\mathbb{Q}_2$ if I is split and K_2 is an unramified degree 2 extension of $\mathbb{Q}_2$ if it is inert.
If 2 is split we can use Theorem 6 and the fact that $\mathcal{O}_I$ is isomorphic to $\mathbb{Z}_2$. The exponent a at $\mathbb{Z}/2^a\mathbb{Z}$ is 1 since $-1 \in \mathbb{Z}_2$, but $x^2 = -1$ has no solution in $\mathbb{Z}_2$ (it doesn't have a solution in $\mathbb{Z}/4\mathbb{Z}$), so there is a second primitive root of unity in $\mathbb{Z}_2$, but no primitive forth root of unity.
If 2 is inert we use the same theorem, $\mathcal{O}_2$ is the ring of units of an unramified degree 2 extension of $\mathbb{Z}_2$. From Theorem 11 it can be written as $\mathbb{Q}_2[X]/(f(X))$ where $f(X)$ is a polynomial such that $\mathbb{Z}/2\mathbb{Z}[X]/(f(X))$ is a degree two field extension of the local field $\mathbb{Z}/2\mathbb{Z}$, i.e. it is irreducible in $\mathbb{Z}/2\mathbb{Z}$. This polynomial is $f(X) = X^2 + X + 1$. So the local field is isomorphic to $\mathbb{Q}_2[X]/(X^2 + X + 1)$ and $\mathcal{O}_2 \cong \mathbb{Z}_2[X]/(X^2 + X + 1)$ (the elements with valuation ≥ 0). We also have $a = 1$ since $x^2 = -1$ doesn't have a solution in $\mathbb{Z}/4\mathbb{Z}[X]/(X^2 + X + 1)$, so there is no primitive forth root of unity. □

Lemma 33. *There is an isomorphism* $(\mathbb{Z}/4\mathbb{Z}[X]/(X^2 + X + 1))^\times \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

Proof. The invertible elements in $\mathbb{Z}/4\mathbb{Z}[X]/(X^2+X+1)$ are of the form $AX+B$ where both A, B are not zero divisors in $\mathbb{Z}/4\mathbb{Z}$, that is 0 or 2. Therefore there are $4 \cdot 4 - 4 = 12$ elements, so the group is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The elements $2X + 1, 2X + 3$ and 3 have order 2 and so the group must be isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Lemma 34. *There is an isomorphism* $(\mathbb{Z}/8\mathbb{Z}[X]/(X^2 + X + 1))^\times \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$

Proof. The invertible elements in $\mathbb{Z}/8\mathbb{Z}[X]/(X^2+X+1)$ are of the form $AX+B$ where both A, B are not zero divisors in $\mathbb{Z}/8\mathbb{Z}$, that is 0,2,4 or 6. Therefore there are $8 \cdot 8 - 4 \cdot 4 = 48$ elements. Every element can be multiplied by one of $1, X, X^2$ so that it is of the form $2AX + B$. It can then be multiplied by one of $+1, -1$ so that B is $1 + 4C$. These elements $2AX + 4C + 1$ form a subgroup with $4 \cdot 2 = 8$ elements and it has an element $2X+1$ of order 4 and 3 elements $5, 4X+1, 4X+5$ of order 2, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. □

It is now possible to determine all characters for even primes.

Lemma 35. *For split primes over 2 we have 3 nontrivial characters with local conductors 2,3 and 3. If 2 is inert we have 7 nontrivial characters, 3 of them with local conductor 3 and 4 with local conductor 3.*

Proof. There are two homomorphism $\mathbb{Z}_2 \to \mathbb{Z}/2\mathbb{Z}$. One is trivial and the other one is nontrivial with kernel $2\mathbb{Z}_2$ (because $2\mathbb{Z}_2$ is always in the kernel and so the homomorphism is determined by the image of 1).
For split primes we have $\mathcal{U}_I \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ using Lemma 32 so there are $2 \times 2 = 4$ characters of which 3 are nontrivial (with kernels $(0, 2\mathbb{Z}_2), (\mathbb{Z}/2\mathbb{Z}, 0), (\mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z}_2)$). Also $\mathcal{U}_I/\mathcal{U}_I^{(2)} \cong (\mathbb{Z}_2/4\mathbb{Z}_2)^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ using Theorem 4, so one of them has conductor 2 (a character factorizes through $\mathcal{U}/\mathcal{U}^{(n)}$ iff it has local conductor $\leq n$). We also have $\mathcal{U}_I/\mathcal{U}_I^{(3)} \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and so there are 3 nontrival characters with local conductors ≤ 3. One of them has local conductor 2, so the other two have local conductor 3.

From the proof of Lemma 32, for inert prime 2 the local field is isomorphic to $\mathcal{O}_2 \cong \mathbb{Z}_2[X]/(X^2+X+1)$. The group of units is $\mathcal{U}_2 \cong (\mathbb{Z}_2[X]/(X^2+X+1))^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$ using Theorem 6. So there are 7 nontrivial characters total. Using Theorem 4 and 33, we can see that $\mathcal{U}_2/\mathcal{U}_2^{(2)} \cong (\mathbb{Z}/4\mathbb{Z}[X]/(X^2+X+1))^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ so 3 of them have conductor 2 and $\mathcal{U}_2/\mathcal{U}_2^{(3)} \cong (\mathbb{Z}/8\mathbb{Z}[X]/(X^2+X+1))^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ using Lemma 34, so all other characters factorize through $\mathcal{U}_2^{(3)}$ and so have conductor 3. □

2.3 Counting function

We put all information about quadratic extensions of a number field K into one function. We still assume that K is imaginary quadratic with odd class number. In this chapter we will assume that $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$.

Definition 36. *The counting function $f_K(s)$ of a number field K is a function of a complex variable s defined as the series*

$$f_K(s) = \sum_{n=0}^{\infty} a_n n^{-s}$$

where a_n is the number of quadratic field extensions of K with absolute discriminant n.

We have already seen in Theorem 19 that quadratic extensions correspond to nontrivial continuous homomorphisms $\mathbb{I}_K^\infty K^\times/K^\times \cong \mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times) \to \mathbb{Z}/2\mathbb{Z}$. If $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, we have $\mathcal{O}_K^\times = \{+1, -1\}$. Let's first look at homomorphisms $\mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$.
In our case of an imaginary quadratic field we have $\mathbb{I}_K^\infty = \mathbb{C}^\times \times \prod_{\mathfrak{p} \text{ finite}} \mathcal{U}_\mathfrak{p}$. We know from Theorem 21 that each character is a sum of a finite number of homomorphisms $\mathcal{U}_\mathfrak{p} \to \mathbb{Z}/2\mathbb{Z}$.
We will see that the counting function can be written as a product of local factor over the primes. For convenience we will define the *absolute conductor* of a character as the norm of the conductor of the character, which is natural number instead of an ideal.

Definition 37. *We define the local factor $g_\mathfrak{p}(s)$ at a prime $\mathfrak{p}$ to be the function*

$$g_\mathfrak{p}(s) = \sum_{\chi_i \text{ characters on } \mathcal{U}_\mathfrak{p}} N(\mathfrak{p})^{-f_i s}$$

where f_i is the local conductor of χ_i

From Lemma 30 we get that:

Theorem 38. *For primes $\mathfrak{p}$ not above 2 the local factor is*

$$g_\mathfrak{p}(s) = (1 + N(\mathfrak{p})^{-s})$$

Similarly from Lemma 35 we get

Theorem 39. *If 2 is inert, then the local factor $g_2(s)$ is:*

$$g_2(s) = (1 + 3N(2)^{-2s} + 4N(2)^{-3s})$$

and if 2 is split, then for the primes I above 2 we have

$$g_I(s) = (1 + N(I)^{-2s} + 2N(I)^{-3s}).$$

First we show that a simplified counting function can be written as a product of local factors.

Theorem 40. *The counting function $f_0(s) = \sum_{n\geq 1} a_n n^{-s}$ where a_n is the number of continuous characters $\mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$ with absolute conductor n can be written as*

$$f_0(s) = \prod_{\mathfrak{p} \text{ primes of } K} g_\mathfrak{p}(s) = \prod_{\mathfrak{p} \text{ primes above 2}} g(s)_\mathfrak{p} \times \prod_{\mathfrak{p} \text{ other primes of } K} (1 + N(\mathfrak{p})^{-s}).$$

Furthermore it converges for $\mathrm{Re}(s) > 1$.

Proof. Notice that the function $f_0(s)$ can also be written as a sum over ideals of $\mathcal{O}_K$, that is $f_0(s) = \sum_{I \text{ ideal of } \mathcal{O}_K} a_I N(I)^{-s}$, where a_I is the number of homomorphisms with conductor I. This is the same sum, we are just indexing the terms by the conductors (ideals) instead of their norms (natural numbers).
Using the theorems in Section 2.1, we know that every nontrivial homomorphism $\chi : \mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$ can be uniquely written as a sum of finitely many homomorphisms $\chi_\mathfrak{p} : \mathcal{U}_\mathfrak{p} \to \mathbb{Z}/2\mathbb{Z}$ over distinct primes. Denote D_k the set of primes of $\mathcal{O}_K$ with norm less than k and H_k the set of ideals, that can be written as products of prime ideals from D_k. The set D_k is finite, beacuse the are only finitely many ideals with norm less then some number ([Mil17] Theorem 4.4). Every character χ whose conductor is in H_k can be written as a sum of local characters over primes in D_k. This is because the absolute conductor of a sum of local homomorphisms over distinct primes $\sum_\mathfrak{p} \chi_\mathfrak{p}$ is $\prod_\mathfrak{p} N(\mathfrak{p})^{f_\mathfrak{p}}$, by 24.
We have $\sum_{I \in H_k} a_I N(I)^{-s} = \prod_{\mathfrak{p} \in D_k} g_\mathfrak{p}(s)$ as we will show. The local factors $g_\mathfrak{p}(s)$ are sums of the terms $N(\mathfrak{p})^{-f_\mathfrak{p} s}$ for all local characters $\chi_\mathfrak{p}$ on $\mathcal{U}_\mathfrak{p}$ to the power $-s$ (here $f_\mathfrak{p}$ is the local conductor of $\chi_\mathfrak{p}$). If we multiply out all the local factors for primes in D_k, we get exactly the sum of absolute conductors of all sums of local characters of primes in D_k to the power $-s$. Therefore the product is $\sum_{\chi \text{ character with conductor in } H_k} N(I_\chi)^{-s} = \sum_{I \in H_k} a_I N(I)^{-s}$ where I_χ is the conductor of χ.

From this and the form of the factors $g_\mathfrak{p}(s)$, we can see that a_I is at most 4, so the sum $f_0(s) = \sum_{I \text{ ideal of } \mathcal{O}_K} a_I N(I)^{-s}$ converges for $\mathrm{Re}(s) > 1$. We get the inequality

$$|f_0(s) - \prod_{\mathfrak{p} \in D_k} g_\mathfrak{p}(s)| \leq \sum_{I \notin H_k} a_I N(I)^{-\mathrm{Re}(s)}.$$

So on the halfplane $\mathrm{Re}(s) > 1$ the product converges to $f_0(s)$ by letting k go to infinity. □

The counting function looks like an Euler product for the Dedekind zeta function as defined below.

Theorem 41. *The Dedekind zeta function of the number field K is the complex function*

$$\zeta_K(s) = \sum_{I \text{ nonzero ideals in } \mathcal{O}_K} \frac{1}{N(I)^s}$$

which converges to a holomorphic function for $\mathrm{Re}(s) > 1$. *It can also be given as the Euler product*

$$\zeta_K(s) = \prod_{\mathfrak{p} \text{ nonzero prime ideals of } K} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

Furthermore, it can be analytically extended to a holomorphic function on $\mathbb{C}\backslash\{1\}$ *with a simple pole at 1 and* $\zeta_K(s)$ *is nonzero for* $\mathrm{Re}(s) > 1$ *(none of the factors are zero there).*

Proof. See theorems in [NS99], Section 5, Chapter VII. □

In fact, we have

Theorem 42. *The function* $f_0(s)$ *can be expressed as*

$$f_0(s) = \frac{\zeta_K(s)}{\zeta_K(2s)} \times \prod_{\mathfrak{p} \text{ primes above } 2} \frac{g(s)_\mathfrak{p}}{(1 + N(\mathfrak{p})^{-s}}$$

and therefore can be analytically extended to a holomorphic function for $\mathrm{Re}(s) > 1/2, s \neq 1$ *with a simple pole at 1.*

Proof. We can write

$$\begin{aligned} f_0(s) &= \prod_{\mathfrak{p} \text{ primes above } 2} g(s)_\mathfrak{p} \times \prod_{\mathfrak{p} \text{ other primes of } K} (1 + N(\mathfrak{p})^{-s}) = \\ &= \prod_{\mathfrak{p} \text{ primes above } 2} \frac{g(s)_\mathfrak{p}}{(1 + N(\mathfrak{p})^{-s}} \times \prod_{\mathfrak{p} \text{ all primes of } K} (1 + N(\mathfrak{p})^{-s}) = \\ &= \prod_{\mathfrak{p} \text{ primes above } 2} \frac{g(s)_\mathfrak{p}}{(1 + N(\mathfrak{p})^{-s}} \times \prod_{\mathfrak{p} \text{ all primes of } K} \frac{(1 - N(\mathfrak{p})^{-2s})}{(1 - N(\mathfrak{p})^{-s})} = \\ &= \prod_{\mathfrak{p} \text{ primes above } 2} \frac{g(s)_\mathfrak{p}}{(1 + N(\mathfrak{p})^{-s}} \times \frac{\zeta_K(s)}{\zeta_K(2s)}. \end{aligned}$$

The function ζ_K is holomorphic outside 1 with a simple pole at 1. It also has no zeros for $\mathrm{Re}(s) > 1$ so the function $\frac{1}{\zeta_K(2s)}$ is holomorphic on the halfplane $\mathrm{Re}(s) > 1/2$. There are only 1 or 2 primes above 2, so the first factor is holomorphic on $\mathbb{C}$. □

From Theorem 21 we know that quadratic extensions of K correspond to homomorphisms from $\mathbb{I}_K^\infty$ to $\mathbb{Z}/2\mathbb{Z}$ with $\mathbb{I}_K^\infty \cap K^\times$ in the kernel. So far we have only looked at homomorphisms $\mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$, so we need to figure out which ones send $\mathbb{I}_K^\infty \cap K^\times$ to $0 \in \mathbb{Z}/2\mathbb{Z}$. As we saw just before Lemma 20, we have $\mathbb{I}_K^\infty \cap K^\times = \{+1, -1\}$. So the characters need to send -1 to 0. We will call a character *even* is it does send -1 to 0 and *odd* otherwise.

Definition 43. *We define the odd local factor $g_-(s)_\mathfrak{p}$ at a prime $\mathfrak{p}$ to be the function*

$$g_\mathfrak{p}(s) = \sum_{\chi_i \text{ characters on } \mathcal{U}_\mathfrak{p}} \sigma_i N(\mathfrak{p})^{-f_i s}$$

where f_i is the local conductor of χ_i and σ_i is 1 if the character is even and -1 if it is odd.

From Lemma 30 we get that:

Theorem 44. *For primes $\mathfrak{p}$ not above 2 the odd local factor is*

$$g_-(s)_\mathfrak{p} = (1 + N(\mathfrak{p})^{-s})$$

if $\mathfrak{p}$ is inert or the prime p (where $\mathfrak{p}$ is above p) is 1 mod 4 and

$$g_-(s)_\mathfrak{p} = (1 - N(\mathfrak{p})^{-s})$$

if it is not inert and p is 3 mod 4.

Proof. Same as for the ordinary local factor, but now we have to look where is -1 sent by the nontrivial character on $\mathcal{U}_\mathfrak{p}$. From 28 we get that $\mathcal{U}_K \cong \mathbb{Z}/(p^i - 1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$. The element -1 is mapped to $(\frac{(p^i-1)}{2}, 0, 0)$ by the isomorphism. If $\mathfrak{p}$ is inert, then $i = 2$ and $4|(p^i - 1)$, so -1 is mapped to 0 by the nontrivial character. This is also the case if $4|(p - 1)$. Otherwise -1 is sent to $1 \in \mathbb{Z}/2\mathbb{Z}$ and the nontrivial character on $\mathcal{U}_\mathfrak{p}$ is odd. □

We will write S for the set of primes that satisfy the first condition in the previous theorem.
Similarly from Lemma 35 we get

Theorem 45. *If 2 is inert, then the odd local factor $g_-(s)_2$ is:*

$$g_-(s)_2 = (1 + N(2)^{-2s} - 2N(2)^{-2s} + 2N(2)^{-3s} - 2N(2)^{-3s})$$

and is 2 s split, then for the primes I above 2 we have

$$g_-(s)_I = (1 - N(I)^{-2s} - N(I)^{-3s} + N(I)^{-3s}).$$

Proof. Same as for the ordinary local factor, but we use Lemmas 33 and 34 to figure out what characters are odd.
If 2 is split, then -1 maps to $1 \in \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathcal{U}/\mathcal{U}^{(2)}$ and to $(1, 0) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathcal{U}/\mathcal{U}^{(3)}$, so one character of local conductor 2 is odd and two characters of local conductor at most 3 are odd, onee of them has local conductor 2. In total there is one odd character of local conductor 2 and one odd character of local conductor 3. Thus the local factor, denoted $g_-(s)_I$, is $(1 - N(I)^{-2s} - N(I)^{-3s} + N(I)^{-3s})$.
If 2 is inert, -1 maps to $(0, 1, 0) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathcal{U}/\mathcal{U}^{(2)}$ and to $(0, 1, 0, 0) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathcal{U}/\mathcal{U}^{(3)}$ and we can see that two characters of conductor 2 are odd, and two characters of conductor 3 are odd, and thus the local factor is $(1 + N(2)^{-2s} - 2N(2)^{-2s} + 2N(2)^{-3s} - 2N(2)^{-3s})$.
□

Theorem 46. *The counting function $f_-(s) = \sum_{n\geq 1} b_n n^{-s}$ where b_n is the number of continuous characters $\mathbb{I}_k^\infty \to \mathbb{Z}/2\mathbb{Z}$ with absolute conductor n that are even minus the number characters with conductor n that are odd, can be written as*

$$f_-(s) = \prod_{\mathfrak{p} \text{ primes of } K} g_-(s)_\mathfrak{p} =$$
$$= \prod_{\mathfrak{p} \text{ primes above 2}} g_-(s)_\mathfrak{p} \prod_{\mathfrak{p}\notin S \text{ and not above 2}} (1 + N(\mathfrak{p})^{-s}) \prod_{\mathfrak{p}\in S} (1 - N(\mathfrak{p})^{-s})$$

Furthermore it converges for $\mathrm{Re}(s) > 1$.

Proof. The proof is similar to the one for the counting function $f_0(s)$. If we write a character on $\mathbb{I}_K^\times$ as a sum of local characters on $\mathcal{U}_\mathfrak{p}$, than the character is even iff there is an even number of odd characters in the sum, since -1 is then mapped to 0 in $\mathbb{Z}/2\mathbb{Z}$. If we multiply out the product, the terms correspond to sums of local characters and the sign is positive if the sum has even number of odd local characters and negative if it has an odd number of odd local characters. □

Finally the counting fuunction of K is expressed as:

Theorem 47. *The counting function $f_K(s)$ can be written as*

$$f_K(s) = \mathfrak{d}_K^{-2s} \frac{1}{2}(f_0(s) + f_-(s)) - \mathfrak{d}_K^{-2s}$$

where K is a quadratic imaginary number field with odd class number different from $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ and $\mathfrak{d}_K$ is the discriminant of K as a natural number.

Proof. We know from Theorem 21 that quadratic extensions of K correspond to nontrivial continuous on $\mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z}$ with $(\mathbb{I}_K^\infty \cap K^\times)$ in the kernel. We have $(\mathbb{I}_K^\infty \cap K^\times) = \{+1, -1\}$ for our K and so the extensions correspond to even nontrivial continuous characters. Furthermore the absolute discriminant of the extension corresponding to the character χ is from Theorem 27 equal to $N(I_\chi)\mathfrak{d}_K^2$ where I_χ is the conductor of χ.
The function f_0 counts all characters, and the function f_- counts even characters minus odd characters. Therefore adding them with a factor of one half counts only even characters. The terms in this counting function have terms $N(I)^{-s}$, so we have to multiply it by $\mathfrak{d}_K^{-2s}$ to get terms with the absolute discriminant. The term $-\mathfrak{d}_K^{-2s}$ is the eliminate the trivial character which correspond to the extension K/K which we don't count.

□

2.4 Asymptotical distribution of number fields

We can use the counting function to get the asymptotical distribution of quadratic extensions of K.
Recall the little o notation, a positive real function $f(s)$ is $o(g(s))$ iff $\lim_{s\to\infty} \frac{f(s)}{g(s)} = 0$.

Theorem 48. *Let* $f(s) = \sum_{n\geq 1} a_n n^{-s}$ *be convergent for* $\mathrm{Re}(s) > a > 0$. *Assume that in the domain of convergence* $f(s) = g(s)(s-a)^{-w} + h(s)$ *holds, where* $g(s)$,$h(s)$ *are holomorphic functions in the closed half plane* $\mathrm{Re}(s) \geq a$, *and* $g(a) \neq 0$, *and* $w > 0$. *Then*

$$\sum_{1\leq n\leq X} a_n = \frac{g(a)}{a\Gamma(w)} X^a (\log X)^{w-1} + o(X^a (\log X)^{w-1})$$

As a special case, if $f(s)$ *converges for* $\mathrm{Re}(s) > 1$ *and has meromorphic continuation to* $\mathrm{Re}(s) \geq 1$ *with a simple pole at* $s = 1$ *with residue* r, *then*

$$\sum_{1\leq n\leq X} a_n = rX + o(X)$$

Proof. Corollary on page 121 of [Nar83] □

We know that the function $f_0(s)$ is up to some simple factors equal to $\frac{\zeta_K(s)}{\zeta_K(2S)}$. This function satisfies the special case of the previous theorem, we just have to compute the residue. The residue is $\mathrm{Res}_{s=1}\frac{\zeta_K(s)}{\zeta_K(2s)} = \frac{\mathrm{Res}_{s=1}\zeta_K(s)}{\zeta_K(2)}$. The residue of the Dedekind zeta function is given by the class number formula.

Theorem 49. *The residue of the Dedekind zeta function of the number field* K *is*

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2_1^r (2\pi)^{r_2} \mathrm{Reg}_K h_K}{w_K \sqrt{\mathfrak{d}_K}}$$

where r_1 *and* r_2 *is the number of real and complex places respectively,* Reg_K *is the regulator of* K, h_K *is the class number and* w_K *is the number of roots of unity in* K. *In particular, for an imaginary quadratic number field* $r_1 = 0, r_2 = 1$ *and* $\mathrm{Reg}_K = 1$

Proof. See [NS99] VII. 5.11. □

The value $\zeta_K(2)$ for imaginary quadratic number field is calculated in [Zag86] Theorem 2.

$$\zeta_K(2) = \frac{\pi^2}{6\sqrt{\mathfrak{d}_K}} \sum_{0<n<\mathfrak{d}_K} \left(\frac{-\mathfrak{d}_K}{n}\right) A\left(\cot(\frac{\pi n}{\mathfrak{d}_K})\right)$$

where the function $A(x)$ is defined as

$$A(x) = 2\int_0^\infty \frac{t\mathrm{d}t}{x\sinh^2 t + x^{-1}\cosh^2 t}$$

and $(\frac{a}{b})$ is the Kronecker symbol.

Now for the function $f_-(s)$. We can express it using Dirichlet L-functions. A Dirichlet character is a homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. We can extend it to $\mathbb{Z}$ by defining $\chi(a) = 0$ if $\gcd(m, a) \neq 1$. For example we have a character $\chi_4 : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}$ where $\chi_4(3) = -1$. For an imaginary quadratic number field K there is a character (the Kronecker symbol $(\frac{-\mathfrak{d}_K}{x})$) $\chi_K : (\mathbb{Z}/\mathfrak{d}_K\mathbb{Z})^\times \to \mathbb{C}$ such that $\chi_K(p)$ is 1 if p splits in K and -1 if p is inert in K.

For every character we have an L-function

Definition 50. *If $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ is the Dirichlet character, we define a function*

$$L(\chi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}}$$

which converges to a holomorphic function for $\mathrm{Re}(s) > 1$. *If χ is not the trivial character, then $L(\chi, s)$ can be extended to a holomorphic function on the entire complex plane. See Section 2 in Chapter VII. in [NS99].*

If we ignore the factors from primes above 2, the function $f_-(s)$ is equal to (recall that S is the set of primes not above 2 that are inert, or 1 mod 4)

$$\prod_{\mathfrak{p} \notin S \text{ and not above } 2} (1 + N(\mathfrak{p})^{-s}) \prod_{\mathfrak{p} \in S} (1 - N(\mathfrak{p})^{-s}) =$$
$$= \prod_{p \text{ inert}} (1 + p^{-2s}) \prod_{p \text{ splits and is 1 mod 4}} (1 + p^{-s})^2 \prod_{p \text{ splits and is 3 mod 4}} (1 - p^{-s})^2 \times R(s)$$

since the norm of a prime ideal $\mathfrak{p}$ above p is p^2 if it is inert and p otherwise and p is odd in all products. Here $R(s)$ is the factor for the (finitely many) ramified primes $R(s) = \prod_{\mathfrak{p} \text{ ramified, 1 mod 4}}(1 + N(\mathfrak{p})^{-s}) \times \prod_{\mathfrak{p} \text{ ramified, 3 mod 4}}(1 - N(\mathfrak{p})^{-s})$.

We will denote I, S, R the set of inert, split and ramified primes of K not above 2 and I_i, S_i, R_i $i = 1, 3$ the subset of primes that are i mod 4.
Now we can write:

$$\prod_{p \in I}(1 + p^{-2s}) \prod_{p \in S_1} (1 + p^{-s})^2 \prod_{p \in S_3} (1 - p^{-s})^2 R(s) =$$
$$= \frac{\prod_{p \in I}(1 - p^{-4s}) \prod_{p \in S}(1 - p^{-2s})^2}{\prod_{p \in I}(1 - p^{-2s}) \prod_{p \in S_1}(1 - p^{-s})^2 \prod_{p \in S_3}(1 + p^{-s})^2} \times$$
$$\times \frac{\prod_{p \in R}(1 - p^{-2s})}{\prod_{p \in R_1}(1 - p^{-s}) \prod_{p \in R_3}(1 + p^{-s})} =$$
$$= \frac{B(s)/\zeta_K(2s)}{\prod_{p \in I_1}(1 - p^{-s}) \prod_{p \in I_3}(1 + p^{-s}) \prod_{p \in S_1 \cup R_1}(1 - p^{-s}) \prod_{p \in S_3 \cup R_3}(1 + p^{-s})}$$
$$\times \frac{1}{\prod_{p \in I_1}(1 + p^{-s}) \prod_{p \in I_3}(1 - p^{-s}) \prod_{p \in S_1}(1 - p^{-s}) \prod_{p \in S_3}(1 + p^{-s})} =$$
$$= \frac{L(\chi_4, s)L(\chi_4\chi_K, s)}{\zeta_K(2s)} \times B(s)$$

where $\chi_4\chi_K$ is a character on $(\mathbb{Z}/\mathrm{lcm}(4, \mathfrak{d}_K)\mathbb{Z})^\times$ and $B(s) = \prod_{\mathfrak{p} \text{ over } 2} 1/(1 - N(\mathfrak{p})^{-2s})$ is the factor of $\zeta_K(2s)$ at 2. For this character $\chi_4\chi_K(p) = 1$ if p is inert and 3 mod 4 or split and 1 mod 4 , $\chi_4\chi_K(p) = 0$ is p is ramified or 2 and $\chi_4\chi_K(p) = -1$ otherwise. We can summarize it in the following theorem.

Theorem 51. *Let K be a imaginary quadratic number field with odd class number not equal to $\mathbb{Q}[i], \mathbb{Q}[\sqrt{-3}], \mathbb{Q}[\sqrt{-2}]$. Then the function $f_-(s)$ can be written as*

$$f_-(s) = \frac{L(\chi_4, s)L(\chi_4\chi_K, s)}{\zeta_K(2s)} \times \prod_{\mathfrak{p} \text{ primes above } 2} g_-(s)_\mathfrak{p} \times B(s)$$

In particular, it is holomorphic for $\mathrm{Re}(s) \geq 1$.

Proof. The equation is clear from the preceding discussion we just added the factors for the primes above 2. The Dedekind zeta function $\zeta(2s)$ is holomorphic and nonzero on the halfplane $\mathrm{Re}(s) > 1/2$. Since the characters χ_4 and $\chi_4\chi_K$ are nontrivial if $K \neq \mathbb{Q}(i)$, the L-functions are holomorphic for all s. □

We can put everything together te get the main result

Theorem 52. *For a quadratic imaginary number field K with odd class number not equal to $\mathbb{Q}[i], \mathbb{Q}[\sqrt{-3}], \mathbb{Q}[\sqrt{-2}]$ the function $a_K(n) = \#\{L/K | \deg(L/K) = 2, \mathfrak{d}_L \leq n\}$ is asymptotically equal to*

$$a_K(n) = Cn + o(n)$$

where C is given by

$$C = \frac{1}{2\mathfrak{d}_K^2} \frac{\mathrm{Res}_{s=1}\zeta_K(s)}{\zeta_K(2)} \prod_{\mathfrak{p} \text{ over } 2} \frac{g_\mathfrak{p}(1)}{(1+N(\mathfrak{p})^{-1})} = \frac{\mathfrak{d}_K^{-5/2}\pi h_K}{2\zeta_K(2)} \prod_{\mathfrak{p} \text{ over } 2} \frac{g_\mathfrak{p}(1)}{(1+N(\mathfrak{p})^{-1})}$$

Proof. Apply the special case of Theorem 48 to the function $f_K(s) = \mathfrak{d}_K^{-2s}\frac{1}{2}(f_0(s) + f_-(s)) - \mathfrak{d}_K^{-2s}$. This function is holomorphic for $\mathrm{Re}(s) \geq 1$ except for a pole at 1. The functions $f_-(s)$ and $\mathfrak{d}_K^{-2s}$ have no pole at 1, so it doesn't affect the asymptotic growth. The number C is the residue of $f_K(s)$ at 1, which is thus $\frac{1}{2\mathfrak{d}_K^2}$ times the residue of $f_0(s)$. Then use Theorem 49 to get the formula for the residue. □

2.5 Special cases

We left the cases of $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-2})$ as last. We will show that the main Theorem 52 holds for these fields in this form:

Theorem 53. *For a quadratic imaginary number field K with odd class number the function $a_K(n) = \{L/K | \deg(L/K) = 2, \mathfrak{d}_L \leq n\}$ is asymptotically equal to*

$$a_K(n) = Cn + o(n)$$

where C is given by

$$C = \frac{\mathfrak{d}_K^{-5/2}\pi h_K}{w_K\zeta_K(2)} \prod_{\mathfrak{p} \text{ primes over } 2} \frac{g_\mathfrak{p}(1)}{(1+N(\mathfrak{p})^{-1})}$$

where w_K is the number of roots of unity in K and $g_\mathfrak{p}(s)$ is

$$g_\mathfrak{p}(s) = \left\{ \begin{array}{ll} (1 + 2^{-2s} + 2\cdot 2^{-3s}), & \text{if 2 is split in } K \\ (1 + 3\cdot 4^{-2s} + 4\cdot 4^{-3s}), & \text{if 2 is inert in } K \\ (1 + 2^{-2s} + 2\cdot 2^{-4s} + 4\cdot 2^{-5s}), & \text{if 2 is ramified in } K \end{array} \right\}$$

Proof. We only need to show this for $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-2})$.
The only problem with $\mathbb{Q}(\sqrt{-3})$ is that the unit group has six elements, $\mathcal{O}_K^\times \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The $\mathbb{Z}/2\mathbb{Z}$ part is generated by -1 and the $\mathbb{Z}/3\mathbb{Z}$ is

generated by the image of $\zeta_3 = e^{2\pi i/3}$. But ζ_3 must map to $0 \in \mathbb{Z}/2\mathbb{Z}$ for every local character, since it has order 3, and so the Theorem 52 works for the number field $\mathbb{Q}(\sqrt{-3})$, except now $w_K = 6$ in the formula for the residue of the Dedekind zeta function.

For the number field $\mathbb{Q}(\sqrt{-2})$ the problem is that 2 is ramified, which means that the local factor $g_{\sqrt{-2}}(s)$ is going to be different. We can calculate it similarly as in Lemmas 35 and 39. From Theorem 10, we can see that at $\sqrt{-2}$ the local field is $\mathbb{Q}[X]/(X^2+2) \otimes_{\mathbb{Q}} \mathbb{Q}_2 \cong \mathbb{Q}_2[X]/(X^2+2)$ and its ring of integers is $\mathcal{O}_{\sqrt{-2}} \cong \mathbb{Z}_2[X]/(X^2+2)$. Using Theorem 6 we get $\mathcal{U}_{\sqrt{-2}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$, so there are also 7 non-trivial characters. The uniformizer in the local field is not 2, but $\sqrt{-2} = X$ (it is the element with the lowest nonzero valuation and $\nu_{\sqrt{-2}}(2) = 2$). Using Theorem 4, we can see that $\mathcal{U}/\mathcal{U}^{(n)} \cong (\mathbb{Z}_2[X]/(X^2+2, X^n))^\times$. By analyzing the structure of these groups, we can calculate the local factor to be $g_{\sqrt{-2}}(s) = (1 + 2^{-2s} + 2 \cdot 2^{-4s} + 4 \cdot 2^{-5s})$.

For $\mathbb{Q}(i)$ there are two problems. The prime 2 is ramified ($(2) = (1+i)^2$) and the ring of integers of the local field is $\mathbb{Z}_2[X]/(X^2+1)$ and the uniformizer is $(1+i) = (1+X)$. We can compute the local factor as in the previous case and it is also $g_{1+i}(s) = (1 + 2^{-2s} + 2 \cdot 2^{-4s} + 4 \cdot 2^{-5s})$.

The unit group has 4 elements and is generated by i. So i has to be mapped to 0 in $\mathbb{Z}/2\mathbb{Z}$ by the character, which means it has to be mapped to 1 by an even number of local characters. The number i is an element of order 4. If p is inert, that it is equal to 3 mod 4, then $8|p^2-1$ and so i gets mapped to 0. If p is split, then i is mapped to 0 iff p is 1 mod 8. The counting function is constructed similarly, only now the function $f_-(s)$ is equal to

$$f_-(s) = \prod_{p \text{ inert}} (1+p^2) \prod_{p \text{ split, } 1 \bmod 8} (1+p)^2 \prod_{p \text{ split, } 5 \bmod 8} (1-p)^2 \times g_-(s)_{1+i},$$

which can also be written as $L(\chi_8, s)L(\chi_4\chi_8, s)/\zeta_{\mathbb{Q}(i)}(2s) \times B(s)$ similarly as in Theorem 51, where the character $\chi_8(s) = -1$ for $s = 5, 7 \bmod 8$ and $\chi_8(s) = 1$ otherwise. This function is holomorphic in the region $\mathrm{Re}(s) \geq 1$ and so the Theorem 52 holds even for $\mathbb{Q}(i)$. □

Bibliography

[DF04] David S Dummit and Richard M Foote. *Abstract algebra*. J. Wiley and Sons, 2004.

[Mil13] James Milne. Class field theory, 2013. `www.jmilne.org/math/CourseNotes/CFT.pdf`.

[Mil17] James Milne. Algebraic number theory, 2017. `www.jmilne.org/math/CourseNotes/ANT.pdf`.

[Mil20] James Milne. Fields and Galois theory, 2020. `www.jmilne.org/math/CourseNotes/FT.pdf`.

[Nar83] Władysław Narkiewicz. *Number theory*. World Scientific Publishing Co., 1983.

[NS99] Jürgen Neukirch and Norbert Schappacher. *Algebraic number theory*. Springer, 1999.

[Woo14] Melanie Matchett Wood. Asymptotics for number fields and class groups. 2014. `http://swc.math.arizona.edu/aws/2014/2014WoodNotes.pdf`.

[Zag86] Don Zagier. Hyperbolic manifolds and special values of dedekind zeta-functions. 1986.