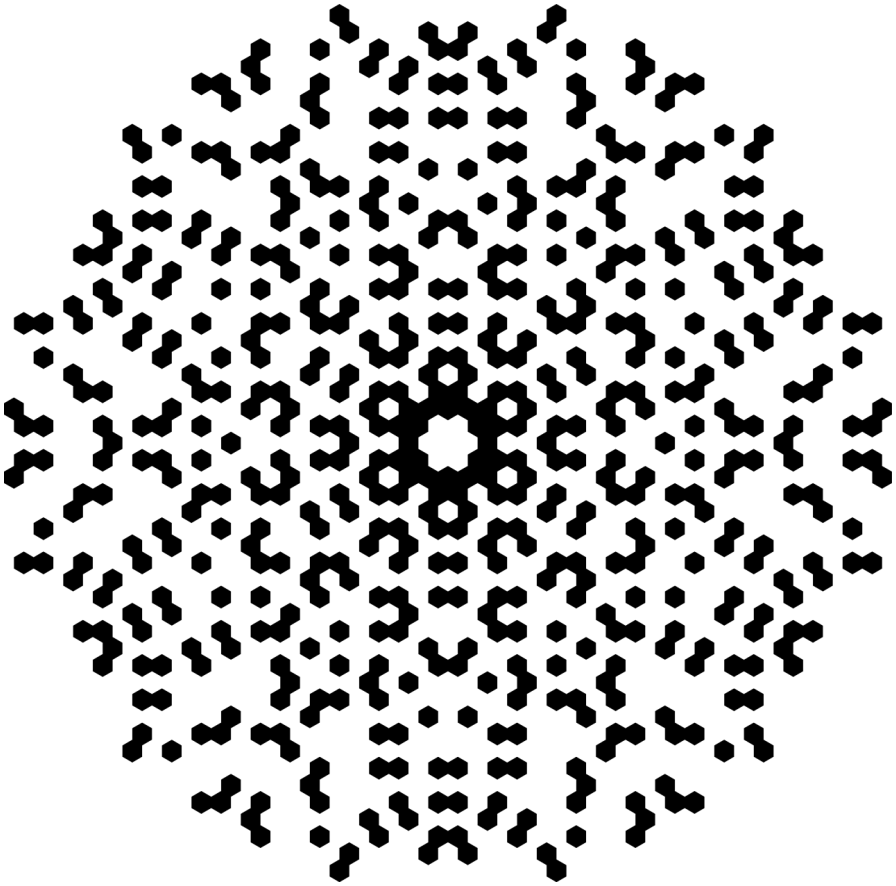
# Chebotarev's Density Theorem

Reinier Sorgdrager

June 28, 2020

Bachelor's thesis Mathematics

Supervisor: dr. Arno Kret



Korteweg-de Vries Institute for Mathematics
Faculty of Sciences
University of Amsterdam

## Abstract

After deriving the class number formula, we give a proof of Chebotarev's Density Theorem that does not invoke class field theory. We then generalize Chebotarev's Density Theorem to the setting of an infinite Galois extension $L$ of a number field $K$ that is unramified except for a set of primes of $K$ of Dirichlet density 0.
Before being able to do this we need to introduce some concepts from algebraic number theory. Most notably, we give the definition of a *cycle* $\mathfrak{c}$ of a given number field and use it to define the *generalized ideal class group* $I(\mathfrak{c})/P_{\mathfrak{c}}$. Then we give an asymptotic formula for the number of integral ideals of bounded norm in a given class of $I(\mathfrak{c})/P_{\mathfrak{c}}$. This asymptotic formula is used to prove the class number formula, after *Dirichlet series* have been introduced.

Title: Chebotarev's Density Theorem
Cover image: Eisenstein primes of norm less than 500, image by Johannes Rössel
Author: Reinier Sorgdrager, reinier@reiniersorgdrager.com, 11870397
Supervisor: dr. Arno Kret,
Second grader: prof. dr. Lenny Taelman,
End date: June 28, 2020

Korteweg-de Vries Institute for Mathematics
University of Amsterdam
Science Park 904, 1098 XH Amsterdam
`http://www.kdvi.uva.nl`

# Contents

# 1 Introduction

What is now known as Chebotarev's Density Theorem was conjectured in 1896 by Georg Frobenius [1]. Frobenius himself only succeeded in proving a weaker version and did not live to see the proof, due to Nikolai Chebotarev, appear in the *Mathematische Annalen* in 1925 [2].
The theorem can be seen as a vast generalization of Dirichlet's Theorem on Arithmetic Progressions, proven in 1837 by Gustav Lejeune Dirichlet. Dirichlet's theorem states that for coprime positive integers $m$ and $a$ the amount of prime numbers occuring in the arithmetic progression

$$a,\ a+m,\ a+2m,\ a+3m,\ a+4m,\ a+5m,\ a+6m,\ a+7m,\ a+8m,\ a+9m,\ \ldots$$

is infinite and that the prime numbers occuring in this progression even have a *density* – which one can think of as the probability for a random prime number to occur in the progression – equal to $1/\varphi(m)$. In other words, the theorem states that the prime numbers are equidistributed over the classes in $(\mathbb{Z}/m\,\mathbb{Z})^*$.
By the time Dirichlet proved this theorem, it had already been proven some decades earlier by Gauß (and conjectured by Euler in the 1770's [3, p. 5]) that whether an integer $a$ is a square in $\mathbb{F}_p$ depends only on $p \bmod 4|a|$. (This statement is essentially equivalent to the law of quadratic reciprocity.) For example, for an odd prime $p$, $-1$ is a square modulo $p$ if and only if $p = -1 \bmod 4$. Hence, knowing Dirichlet's theorem, one sees that the probability that for a random prime number $p$ there is an $x \in \mathbb{Z}$ such that $-1 = x^2 \bmod p$ is equal to $1/2$.
"What about higher powers?" one can wonder. For instance, can we compute the probability that 2 is a fifth power in $\mathbb{F}_p$?
Writing $P_n$ for the amount of prime numbers less than $n$ and $F_n$ for the amount of prime numbers $p < n$ for which 2 is a fifth power in $\mathbb{F}_p$, we see with the aid of a computer:

| $n$ | $P_n$ | $F_n$ | $F_n/P_n$ |
|---|---|---|---|
| 10 | 4 | 4 | 1 |
| 100 | 25 | 20 | 0.8 |
| 1000 | 168 | 136 | 0.80952380952... |
| 10,000 | 1229 | 983 | 0.79983726607... |
| 100,000 | 9592 | 7655 | 0.78906088407... |
| 1000,000 | 78498 | 62793 | 0.79993120843... |
| 10,000,000 | 664579 | 531706 | 0.80006440167... |
| 100,000,000 | 5761455 | 4608953 | 0.79996337731... |
| 1000,000,000 | 50847534 | 40678259 | 0.80000455872... |

The data suggest that the prime numbers $p$ for which 2 is a fifth power modulo $p$ have a density equal to $4/5$.
This does not come as a surprise: an arbitrary prime number $p$ is not congruent to 1 mod 5 with probability $3/4$ and in that case the map $\mathbb{F}_p^* \to \mathbb{F}_p^* : x \mapsto x^5$ will be surjective, because $5 \nmid \#\mathbb{F}_p^*$. With probability $1/4$ on the other hand, $p$ is congruent to 1 mod 5, in which case the group of fifth powers $\mathbb{F}_p^{*,5}$ has index 5 in $\mathbb{F}_p^*$ and one would guess that 2 "lands" with probability $1/5$ in the group $\mathbb{F}_p^{*,5}$. We would conclude that the probability that 2 is a fifth power mod $p$ is indeed

$$3/4 + 1/4 \cdot 1/5 = 4/5.$$

However, this is merely a heuristic argument. To prove it, one needs Chebotarev's Density Theorem. This is what we do in Chapter 7. More generally, we prove for a positive integer $n$ and an integer $a \in \mathbb{Z}$ that the set of prime numbers $p$ for which $a$ is an $n$'th power mod $p$ has a density equal to

$$\frac{1}{\varphi(n)} \sum_{u \in (\mathbb{Z}/n\mathbb{Z})^*} \frac{1}{\gcd(u-1, n)}, \tag{1.1}$$

under some mild assumptions on $a$ (it may not be an $n$'th power in $\mathbb{Z}$ for example). In the case $n$ is itself prime, this density equals $(n-1)/n$, which indeed gives $4/5$ in the case $n = 5$.
In order to give this proof, one should not look at the group $(\mathbb{Z}/n\mathbb{Z})^*$, but at the affine group

$$\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) = \left\{ \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} : u \in (\mathbb{Z}/n\mathbb{Z})^*, t \in \mathbb{Z}/n\mathbb{Z} \right\},$$

which is the Galois group of $\mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q}$, where $\zeta_n$ is a primitive $n$'th root of unity.
Chebotarev's theorem says that we obtain the density of prime numbers $p$ for which $a$ is an $n$'th power mod $p$, if we divide the number of so-called *Frobenius elements* in $\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z})$ that are associated to these primes $p$ by the order $n\varphi(n)$ of the affine group. This is how formula 1.1 is derived.

We prove Chebotarev's Density Theorem in Chapter 5. In the preceding chapters we develop the theory – such as that of Frobenius elements – that is required to give the proof.

# 2 Preliminaries

The reader is expected to be familiar with the groups, rings, modules, and fields. The reader should know the statements covered in a first course in Galois theory. Moreover, this thesis, being in algebraic number theory, contains many algebraic number theoretic facts. All statements from algebraic number theory are either referenced or proven, but we think the reader will benefit greatly by having taken a course in algebraic number theory covering at least the (finiteness of) the class group, the splitting behaviour of primes in an extension of number fields, and Dirichlet's Unit Theorem.
Some analysis is also needed: Chapter 3 requires knowledge of multidimensional integration and Chapter 4 requires complex analysis – in both cases a first course in the subject will suffice. Finally, in Chapter 6 the reader should be familiar with the elements of measure theory and infinite Galois theory.

## 2.1 Rings of integers and their ideals

We define a *number field* $K$ to be a field of finite degree over the rationals $\mathbb{Q}$.
Let $K$ be a number field. Then the *ring of integers* $\mathcal{O}_K$ of $K$ is defined as the integral closure of $\mathbb{Z}$ in $K$.
The ring of integers $\mathcal{O}_K$ has the nice property that every non-zero proper ideal $\mathfrak{a} \subset \mathcal{O}_K$ admits a unique factorization into non-zero prime ideals (which are maximal ideals), that is:

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$$

for certain non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and this factorization is unique up to the order of the $\mathfrak{p}_i$ [4, ch. I, thm. 3.3].
It follows that every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is of finite index in the ring of integers.
In addition to the ideals of $\mathcal{O}_K$, we also have so-called *fractional $K$-ideals* that are defined as non-zero finitely generated $\mathcal{O}_K$-submodules of $K$. For every fractional $K$-ideal $\mathfrak{a}$ there exists an $x \in \mathcal{O}_K \setminus \{0\}$ such that $\mathfrak{a} \cdot (x)$ is an ideal of $\mathcal{O}_K$.
The fractional $K$-ideals turn out to form a group under ideal multiplication, with identity element $\mathcal{O}_K$. This group is called the *group of invertible ideals* and is denoted by $I$. A subgroup of $I$ is the set $P$ of principal fractional $K$-ideals. The *class group* of $K$ is defined as the quotient $\mathrm{Cl}_K = I/P$.
The class group is finite and its order is the *class number* of $K$ [4, ch. I, thm. 6.3].

### Prime ideals in extensions of number fields

Let $L/K$ be an extension of number fields. Then we have a corresponding extension $\mathcal{O}_K \subset \mathcal{O}_L$ of the ring of integers. A non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ has an extension to

$\mathcal{O}_L$ that has a unique factorization into prime ideals:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k},$$

where the $\mathfrak{P}_i$ are distinct prime ideals and the $e_i$ are elements of $\mathbb{Z}_{>0}$. The prime ideals $\mathfrak{P}_i$ are said to *lie above* $\mathfrak{p}$. If for some $i$ we have $e_i > 1$, then $\mathfrak{p}$ is said to *ramify* in $L$ and we call $\mathfrak{P}_i$ *ramified* over $K$, if this is not the case $\mathfrak{p}$ is *unramified* in $L$ and the $\mathfrak{P}_i$ are *unramified* over $K$.
The $e_i$ are called the *ramification indices of* $\mathfrak{P}_i$ *over* $\mathfrak{p}$, and can also be denoted by $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$.
For every $i$ we have that

$$(\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})$$

is an extension of finite fields of *residue class degree* $f(\mathfrak{P}_i/\mathfrak{p}) := [(\mathcal{O}_L/\mathfrak{P}_i) : (\mathcal{O}_K/\mathfrak{p})]$.
For a non-zero prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ lying above the prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, we define the *degree* of $\mathfrak{P}$ over $K$ as $\deg_K(\mathfrak{P}) = f(\mathfrak{P}/\mathfrak{p})$. The degree $\deg_{\mathbb{Q}}(\mathfrak{P})$ is called the *absolute degree* of $\mathfrak{P}$.
We have

$$\sum_{i=1}^{k} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = [L : K],$$

see [4, ch. I, prop. 8.2]. The prime ideal $\mathfrak{p}$ is said to *split completely* if $k = [L : K]$, or equivalently, if $e(\mathfrak{P}_i/\mathfrak{p}) = f(\mathfrak{P}_i/\mathfrak{p}) = 1$ for all $i$.

## 2.2 Lattices

A lattice $L \subset \mathbb{R}^n$ is a free abelian group that is discrete as a subspace in Euclidean space. It is of the form

$$L = \mathbb{Z} \cdot x_1 + \mathbb{Z} \cdot x_2 + \cdots + \mathbb{Z} \cdot x_k,$$

where $x_1, \ldots, x_k \in \mathbb{R}^n$ are $\mathbb{R}$-linearly independent for some $k$ called the *dimension* of $L$.
If $L$ is $n$-dimensional, the parallellotope

$$P = \Big\{ \sum_i \lambda_i x_i \ : \ \lambda_i \in [0, 1) \Big\}$$

is called a *fundamental domain* of $L$ and it contains exactly one representant of each class in $\mathbb{R}^n / L$.
In the $n$-dimensional case, we define the *covolume* of $L$ as the volume of a fundamental domain and denote it by $\mathrm{Covol}(L)$. The covolume is independent of the choice of fundamental domain, because linear isomorphisms $\mathbb{Z}^n \to \mathbb{Z}^n$ have determinant $\pm 1$.
The following theorem shows that for an $n$-dimensional lattice $L \subset \mathbb{Z}^n$ one has $\mathrm{Covol}(L) = [\mathbb{Z}^n : L]$.

**Theorem 2.1.** *Let $a_1, \ldots, a_n \in \mathbb{Z}^n$ be linearly independent and let*

$$P = \Big\{ \sum_i \lambda_i a_i \ : \ \lambda_i \in [0,1) \Big\} \subset \mathbb{R}^n$$

*be the parallellotope spanned by the $a_i$. Then*

$$\mathrm{Vol}(P) = \#P \cap \mathbb{Z}^n \, .$$

*Proof.* Let $L$ be the lattice generated by the $a_i$. For $a \in P \cap \mathbb{Z}^n$ write $C_a = a + [0,1)^n$, and for $b \in L$ define $C_a^b = C_a \cap (b + P)$ (for almost all $b$ this will be the empty set). The union $\bigcup_{a \in P \cap \mathbb{Z}^n} C_a$ has volume $\#P \cap \mathbb{Z}^n$ and it has the same volume as the *disjoint* union

$$\bigcup_{\substack{a \in P \cap \mathbb{Z}^n, \\ b \in L}} (-b + C_a^b) = P.$$

■

**Corollary 2.2.** *If $\alpha : \mathbb{Z}^n \to \mathbb{Z}^n$ is a $\mathbb{Z}$-linear map and $\det(\alpha) \neq 0$, then*

$$|\det(\alpha)| = [\mathbb{Z}^n : \mathrm{Im}\, \alpha].$$

If $L \subset \mathbb{R}^n$ is an $n$-dimensional lattice and $y \in \mathbb{R}^n$, then the translated lattice $y + L$ does not necessarily have a group structure (that happens only if $y \in L$), but one can still think about it geometrically. This is why we define $\mathrm{Covol}(y + L)$ to be $\mathrm{Covol}(L)$.

## 2.3 Equivalence of norms: various definitions of the ideal norm

Let $K$ be a number field. Then one can define the norm of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ in various ways. One such definition is as follows.

**Definition** (Norm of an $\mathcal{O}_K$-ideal)**.** *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then we define its norm $\mathbf{N}\mathfrak{a}$ as*

$$\mathbf{N}\mathfrak{a} = \#\mathcal{O}_K/\mathfrak{a}.$$

The norm turns out to be related to the field norm $N_{K/\mathbb{Q}}$ on $K$, that sends an element $\alpha \in K$ to $N_{L/\mathbb{Q}}(\alpha) = \prod_\sigma \sigma(\alpha)$, where the product ranges over the embeddings $\sigma : K \to \mathbb{C}$. Note that $N_{K/\mathbb{Q}}(\alpha) = \det(- \cdot \alpha)$, where multiplication by $\alpha$ is seen as an endomorphism of the $\mathbb{Q}$-vector space $K$.

**Lemma 2.3.** *The norm is multiplicative, that is, for two non-zero $\mathcal{O}_K$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ one has $\mathbf{N}(\mathfrak{a}\mathfrak{b}) = \mathbf{N}\mathfrak{a} \cdot \mathbf{N}\mathfrak{b}$.*

*Proof.* By the Chinese Remainder Theorem it suffices to prove $\mathbf{N}(\mathfrak{p}^n) = (\mathbf{N}\mathfrak{p})^n$ when $\mathfrak{p}$ is a non-zero prime ideal. We prove this by induction on $n$. When $n = 1$ it is clearly true. For $n > 1$ we have a surjective ring morhpism

$$\mathcal{O}_K/\mathfrak{p}^n \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}^{n-1}$$

with kernel $\mathfrak{p}^{n-1}/\mathfrak{p}^n$. By the induction hypothesis we are done if we are able to show that $\#\mathfrak{p}^{n-1}/\mathfrak{p}^n = \#\mathcal{O}_K/\mathfrak{p}$. To see this, note that $\mathfrak{p}^{n-1}/\mathfrak{p}^n$ is a non-trivial vector space over $\mathcal{O}_K/\mathfrak{p}$. Its dimension cannot be greater than 1, for then we would have a proper linear subspace of $\mathfrak{p}^{n-1}/\mathfrak{p}^n$, which would, when contracted to $\mathcal{O}_K$, give rise to an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ satisfying

$$\mathfrak{p}^n \subsetneq \mathfrak{a} \subsetneq \mathfrak{p}^{n-1}.$$

In that case we would have

$$\mathfrak{p} \subsetneq \mathfrak{a}\mathfrak{p}^{1-n} \subsetneq \mathcal{O}_K,$$

contradicting the maximality of $\mathfrak{p}$. Thus $\mathfrak{p}^{n-1}/\mathfrak{p}^n$ has dimension 1 over $\mathcal{O}_K/\mathfrak{p}$. ■

**Theorem 2.4.** *The norm $\mathbf{N}\mathfrak{a}$ of a non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ is equal to the unique $n(\mathfrak{a}) := a > 0$ for which $a\mathbb{Z}$ equals the ideal generated by the image of $\mathfrak{a}$ under $N_{K/\mathbb{Q}}$.*

*Proof.* One can verify that $n$ is multiplicative. So by multiplicativity of both $\mathbf{N}$ and $n$, it suffices to verify $\mathbf{N}\mathfrak{p} = n(\mathfrak{p})$ for all non-zero prime ideals $\mathfrak{p}$ of $K$.
Let $h$ be the class number of $K$ and let $\mathfrak{p}$ be a non-zero prime of $K$. Then $\mathfrak{p}^h = \alpha\mathcal{O}_K$ is principal. We have

$$n(\mathfrak{p})^h = n(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)| = |\det(- \cdot \alpha)| = \#\mathcal{O}_K/\alpha\mathcal{O}_K = \mathbf{N}\mathfrak{p}^h,$$

where the penultimate equality follows by Corollary 2.2. Thus $n(\mathfrak{p}) = \mathbf{N}\mathfrak{p}$. ■

## 2.4 Frobenius elements

Frobenius elements play a central role in this thesis. We will state and prove a few elementary results that will allow us to give their definition (cf. [5, p. 85–86]).
Throughout this section let $L/K$ be a Galois extension of number fields with group $G$.

**Theorem 2.5.** *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a non-zero prime ideal and let $S_\mathfrak{p}$ be the set of primes $\mathfrak{P} \subset \mathcal{O}_L$ above $\mathfrak{p}$. Then the $G$-action on $S_\mathfrak{p}$, given by $\sigma\mathfrak{P} := \sigma(\mathfrak{P})$ for $\sigma \in G$, is transitive.*

*Proof.* Let $\mathfrak{P}$ be in $S_\mathfrak{p}$. By the Chinese Remainder Theorem there exists an $x \in \mathfrak{P}$ that is not an element of any $\mathfrak{P}' \in S_\mathfrak{p}$ different from $\mathfrak{P}$. Hence, for $\sigma \in G$, the only prime in $S_\mathfrak{p}$ containing $\sigma(x)$ is $\sigma\mathfrak{P}$. Because $N_{L/K}(x) = \prod_\sigma \sigma(x) \in \mathfrak{p} \subset \bigcap_{\mathfrak{P}' \in S_\mathfrak{p}} \mathfrak{P}'$ we conclude that any $\mathfrak{P}' \in S_\mathfrak{p}$ must occur as a $\sigma\mathfrak{P}$. ■

Because $G$ acts transitively on $S_\mathfrak{p}$ we see that the ramification indices $e(\mathfrak{P}/\mathfrak{p})$ and the residue class degrees $f(\mathfrak{P}/\mathfrak{p})$ are independent of $\mathfrak{P}$, we will hence denote them by $e_\mathfrak{p}$ and $f_\mathfrak{p}$ respectively. In addition, write $g_\mathfrak{p} = S_\mathfrak{p}$.

**Corollary 2.6.** *For a non-zero prime $\mathfrak{p}$ of $\mathcal{O}_K$ one has $e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = [L : K]$.*

*Proof.* On the one hand we have

$$\mathbf{N}(\mathfrak{p}\mathcal{O}_L) = \#\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = (\#\mathcal{O}_K/\mathfrak{p})^{[L:K]},$$

while on the other hand

$$\mathbf{N}(\mathfrak{p}\mathcal{O}_L) = \prod_{\mathfrak{P}\in S_\mathfrak{p}} \mathbf{N}\mathfrak{P}^{e_\mathfrak{p}} = \prod_{\mathfrak{P}\in S_\mathfrak{p}} (\#\mathcal{O}_K/\mathfrak{p})^{e_\mathfrak{p} f_\mathfrak{p}} = (\#\mathcal{O}_K/\mathfrak{p})^{e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}}.$$

■

For a prime $\mathfrak{P} \in S_\mathfrak{p}$, let $G_\mathfrak{P} \subset G$ be the stabilizer of $\mathfrak{P}$. The group $G_\mathfrak{P}$ is called the *decomposition group* of $\mathfrak{P}$.
We have $\#G_\mathfrak{P} = g_\mathfrak{p}^{-1}\#G = e_\mathfrak{p} f_\mathfrak{p}$. Moreover $G_\mathfrak{P}$ acts naturally on $\mathcal{O}_L/\mathfrak{P}$, inducing a morphism of groups $G_\mathfrak{P} \to \mathrm{Gal}\big((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\big)$.

**Lemma 2.7.** *The map $G_\mathfrak{P} \to \mathrm{Gal}\big((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\big)$ is surjective.*

*Proof.* Let $x \in \mathcal{O}_L/\mathfrak{P}$ be a primitive element for $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ with minimal polynomial $f \in (\mathcal{O}_K/\mathfrak{p})[X]$. By the Chinese Remainder Theorem there is a lift $\xi$ of $x$ that is an element of $\mathfrak{P}'$ for any $\mathfrak{P}' \in S_\mathfrak{p} \setminus \{\mathfrak{P}\}$.
Let $g = \prod_{\sigma\in G}(X - \sigma(\xi)) \in K[X]$. Its reduction modulo $\mathfrak{p}$ looks like $\overline{g} = X^{\#G - g_\mathfrak{p}} h \in (\mathcal{O}_K/\mathfrak{p})[X]$, for some polynomial $h \in (\mathcal{O}_K/\mathfrak{p})[X]$. We see that the minimal polynomial $f$ divides $h$, and hence every conjugate of $x$ over $\mathcal{O}_K/\mathfrak{p}$ is obtained by reducing $\sigma(\xi)$ modulo $\mathfrak{P}$ for some $\sigma \in G_\mathfrak{P}$. ■

In the case that $\mathfrak{p}$ does not ramify in $L$, one has $e_\mathfrak{p} = 1$, and thus $\#G_\mathfrak{P} = f_\mathfrak{p}$, which means the map is not merely a surjection, but even an isomorphism! This gives rise to the definition of the Frobenius element of an unramified prime $\mathfrak{P} \subset \mathcal{O}_L$.

**Definition** (The Frobenius element of a prime $\mathfrak{P}$)**.** *Suppose $\mathfrak{P} \subset \mathcal{O}_L$ is a non-zero prime ideal, unramified over $K$, lying above the prime $\mathfrak{p} \subset \mathcal{O}_K$. Then we define the Frobenius element $(\mathfrak{P}, L/K) \in G$ of $\mathfrak{P}$ as the unique element of $G_\mathfrak{P}$ that is sent to $(x \mapsto x^{\mathbf{N}\mathfrak{p}}) \in \mathrm{Gal}\big((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\big)$ by the map of Lemma 2.7.*

Finally, note that for any non-zero prime $\mathfrak{P} \subset \mathcal{O}_L$ and any $\sigma \in G$ one has $G_{\sigma\mathfrak{P}} = \sigma G_\mathfrak{P} \sigma^{-1}$. Moreover, in the case $\mathfrak{P} \subset \mathcal{O}_L$ is unramified over $K$ (and lies above $\mathfrak{p} \subset \mathcal{O}_K$) we have

$$(\sigma\mathfrak{P}, L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1},$$

which follows from the fact that for any $x \in \mathcal{O}_L$

$$(\sigma(\mathfrak{P}, L/K)\sigma^{-1})\Big(x + \sigma\mathfrak{P}\Big) = \sigma\Big(\big(\sigma^{-1}(x)\big)^{\mathbf{N}\mathfrak{p}} + \mathfrak{P}\Big) = x^{\mathbf{N}\mathfrak{p}} + \sigma\mathfrak{P}.$$

This means the conjugacy class of a Frobenius element of a prime $\mathfrak{P} \subset \mathcal{O}_L$ depends only on $\mathfrak{P} \cap \mathcal{O}_K$. In the case that $G$ is abelian this conjugacy class is a singleton and we can simply speak of the Frobenius element of the primes above $\mathfrak{P} \cap \mathcal{O}_K$.

# 3 Counting ideals

Throughout this chapter, let $K$ be a number field and $n = [K : \mathbb{Q}]$.

## 3.1 Some more preliminaries

In this chapter, we are interested in counting the ideals of $\mathcal{O}_K$ in a given class of a so-called "generalized ideal class group" – whose definition will be given in the next section. The counting of ideals is an essential part in calculating the densities of prime ideals which we will do in Chapter 5 where we prove Chebotarev's Density Theorem.
In order to count these ideals we will view them as part of Euclidean space, or more generally, we will view $K$ as part of Euclidean space. There is one obvious way in which we can do this: using the embeddings of $K$ into the complex numbers.
If $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding, then $\sigma$ induces an *archimedean absolute value* on $K$ by composing the absolute value of $\mathbb{C}$ with $\sigma$. Note that $\sigma$ and its complex conjugate $\overline{\sigma}$ induce the same absolute value. Conversely, one can verify that if two embeddings $\sigma, \tau : K \hookrightarrow \mathbb{C}$ induce the same absolute value, then either $\sigma = \tau$ or $\sigma = \overline{\tau}$ .
Hence, if $K$ has $r_1$ real embeddings (embeddings into $\mathbb{R}$) and $2r_2$ complex embeddings (embeddings into $\mathbb{C}$ that do not map into $\mathbb{R}$), then the number of archimedean absolute values on $K$ is $r_1 + r_2$. We will call an archimedean absolute value *real* if it is induced by a real embedding and *complex* otherwise.
To each archimedean absolute value $v$ on $K$ we associate the Euclidean space

$$K_v := \begin{cases} \mathbb{R} & \text{if } v \text{ is real,} \\ \mathbb{R}^2 & \text{if } v \text{ is complex.} \end{cases}$$

If $v$ is induced by $\sigma : K \hookrightarrow \mathbb{C}$, then in the real case we simply get the map $\sigma : K \hookrightarrow K_v$ and in the complex case we identify $\mathbb{C}$ with $\mathbb{R}^2$ (by identifying $x + iy$ with $(x, y)$) and also get a map $\sigma : K \hookrightarrow K_v$ – note that we have to *choose* an embedding to obtain a map $K \hookrightarrow K_v$ in the case $v$ is complex.
For each archimedean value $v$ we choose an embedding $\sigma_v : K \hookrightarrow K_v$ that induces $v$. This gives us a map

$$\Phi_K : K \hookrightarrow \prod_v K_v = \mathbb{R}^n : x \mapsto (\sigma_v(x))_v,$$

where $v$ runs over all archimedean absolute values of $K$. It is this map of $K$ into Euclidean $n$-space that we will use in the counting of ideals. When using this map we will always assume the $\sigma_v$ have already been chosen.

In defining the archimedean absolute value on $K$ as above, we made sure to stress that those absolute values are the *archimedean* absolute values of $K$: for there are also non-archimedean absolute values on $K$. Namely, for every non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ there is a $\mathfrak{p}$-adic absolute value on $K$ [6, ch. 2]. We will not develop or use the theory of $\mathfrak{p}$-adic absolute values here, but merely mention them as a motivation for why prime ideals $\mathfrak{p}$ and absolute values are often treated similarly (in those cases they are both referred to by "places of $K$"). We will see an instance of such similar treatment of absolute values and prime ideals in the definition of a "cycle" in the following section.
For now, we would briefly like to mention the concept of localization at a prime ideal $\mathfrak{p}$. Given a non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ we define the *localization of* $\mathcal{O}_K$ *at* $\mathfrak{p}$ as

$$(\mathcal{O}_K)_\mathfrak{p} = \{a/b \in K \colon a \in \mathcal{O}_K, b \in \mathcal{O}_K \setminus \mathfrak{p}\}.$$

The localization $(\mathcal{O}_K)_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$. We leave it to the reader to check that the natural map $\mathcal{O}_K/\mathfrak{p} \to (\mathcal{O}_K)_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ is an isomorphism.
Finally, we note that $\mathfrak{m}_\mathfrak{p}$ is a principal ideal [6, ch. I, prop. 15]. If $\pi_\mathfrak{p} \in (\mathcal{O}_K)_\mathfrak{p}$ generates $\mathfrak{m}_\mathfrak{p}$ we call $\pi_\mathfrak{p}$ a *uniformizer* of $\mathfrak{p}$.

## 3.2 Generalized ideal class groups

Now we will introduce a general kind of ideal class group that can capture information about the real embeddings of a field and about ideals coprime to some given ideal.
We define a *cycle* $\mathfrak{c}$ of $K$ as a formal product

$$\mathfrak{c} = \prod_v v^{m(v)},$$

where the $v$ run over the archimedean absolute values of $K$ and the non-zero prime ideals of $\mathcal{O}_K$, and the $m(v)$ are non-negative integers, only finitely many of which are non-zero. (In the spirit of treating absolute values and prime ideals similarly, the letter $v$ also denotes prime ideals here.) The $m(v)$ can be thought of as multiplicities and just as with ideals we write $v \mid \mathfrak{c}$ if $m(v) > 0$.
If $v$ is an archimedean absolute value, we write $v \mid \infty$, and otherwise we write $v \nmid \infty$. For each cycle $\mathfrak{c}$ we define

$$\mathfrak{c}_0 = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{m(\mathfrak{p})}.$$

This is called the finite part of $\mathfrak{c}$, and it can simply be viewed as an ideal of $\mathcal{O}_K$.

Let us denote the group of fractional $K$-ideals coprime to $\mathfrak{c}$ (by which we mean coprime to $\mathfrak{c}_0$) by $I(\mathfrak{c})$. Note that $I((1)) = I$, the group of fractional ideals. Just as we usually take the quotient $I/P$ to get the ideal class group, we will take a quotient of $I(\mathfrak{c})$ to obtain a generalized ideal class group. In order to do this, let us construct a suitable subgroup.
For an element $\alpha$ of $K^*$ we write $\alpha = 1 \bmod^* \mathfrak{c}$ if $\alpha$ satisfies the following two conditions:

(i) If $\mathfrak{p} \mid \mathfrak{c}$ is a prime ideal, then $\alpha$ lies in the localization of the ring of integers at $\mathfrak{p}$ and
$$\alpha = 1 \bmod \mathfrak{m}_{\mathfrak{p}}^{m(\mathfrak{p})},$$
where $\mathfrak{m}_{\mathfrak{p}}$ denotes the maximal ideal of $(\mathcal{O}_K)_{\mathfrak{p}}$.

(ii) If $v \mid \mathfrak{c}$ is a real absolute value induced by the embedding $\sigma : K \hookrightarrow \mathbb{R}$, then $\sigma(\alpha) > 0$.

Denote by $K_{\mathfrak{c}} \subset K^*$ the subgroup of elements satisfying these conditions. (The idea behind our notation is: given a set $X$ we will write $X_{\mathfrak{c}}$ to denote the subset of $X$ satisfying conditions (i) and (ii), while $X(\mathfrak{c})$ will denote the set of all elements of $X$ coprime to $\mathfrak{c}$.) So we write $P_{\mathfrak{c}}$ for the group of principal fractional ideals $(\alpha)$ satisfying $\alpha \in K_{\mathfrak{c}}$. We then define the *generalized ideal class group* of $\mathfrak{c}$ as $I(\mathfrak{c})/P_{\mathfrak{c}}$. If $\mathfrak{c} = (1)$ it equals the class group.
Like the class group, the generalized ideal class group $I(\mathfrak{c})/P_{\mathfrak{c}}$ turns out to be finite as well. The proof presented below can be found in [6, p. 124–126].

**Theorem 3.1.** *Let $K$ be a number field and $\mathfrak{c} = \prod_v v^{m(v)}$ a cycle of $K$. Let $K(\mathfrak{c})$ denote the subset of $K^*$ of elements coprime to $\mathfrak{c}$. Then the group $K(\mathfrak{c})/K_{\mathfrak{c}}$ is finite, and, moreover, the generalized ideal class group $I(\mathfrak{c})/P_{\mathfrak{c}}$ is finite.*

*Proof.* Note that every class in $I/P$ has a representative in $I(\mathfrak{c})$: if $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal in some class $A \in I/P$ we can solve the congruences
$$\alpha = \pi_{\mathfrak{p}}^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}} \bmod \mathfrak{p}^{1+\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}} \text{ for } \mathfrak{p} \mid \mathfrak{c}_0$$
by the Chinese Remainder Theorem – here the $\pi_{\mathfrak{p}} \in \mathcal{O}_K$ are uniformizers of $\mathfrak{p}$. Then the ideal $\mathfrak{a} \cdot (\alpha^{-1})$ is coprime to $\mathfrak{c}$ and an element of $A$.
This shows the map $I(\mathfrak{c}) \to I/P$ is surjective, giving an isomorphism
$$I(\mathfrak{c})/P(\mathfrak{c}) \cong I/P, \tag{3.1}$$
where $P(\mathfrak{c}) = I(\mathfrak{c}) \cap P$ denotes the group of non-zero principal ideals coprime to $\mathfrak{c}$.
From the definitions we have $P_{\mathfrak{c}} \subset P(\mathfrak{c})$, giving a surjective homomorphism
$$I(\mathfrak{c})/P_{\mathfrak{c}} \twoheadrightarrow I(\mathfrak{c})/P(\mathfrak{c}). \tag{3.2}$$
We will now analyze its kernel $P(\mathfrak{c})/P_{\mathfrak{c}}$.
We have a surjective group homomorphism from the elements of $K^*$ coprime to $\mathfrak{c}$ to $P(\mathfrak{c})$, namely $K(\mathfrak{c}) \to P(\mathfrak{c}) : \alpha \mapsto (\alpha)$. The inverse image of the group $P_{\mathfrak{c}}$ is precisely $UK_{\mathfrak{c}}$, where $U = \mathcal{O}_K^*$. This induces an isomorphism
$$K(\mathfrak{c})/UK_{\mathfrak{c}} \cong P(\mathfrak{c})/P_{\mathfrak{c}}. \tag{3.3}$$
If $v$ is a real absolute value induced by the embedding $\sigma : K \hookrightarrow \mathbb{R}$, let us write $K_v^+ = \mathbb{R}_{>0} \subset K_v$. Then $K_v^*/K_v^+ \cong \{\pm 1\}$ (as we can view the $K_v$ as fields). At last, let us consider the map
$$K(\mathfrak{c}) \to \prod_{\mathfrak{p} \mid \mathfrak{c}_0} \left( (\mathcal{O}_K)_{\mathfrak{p}} / \mathfrak{m}_{\mathfrak{p}}^{m(\mathfrak{p})} \right)^* \times \prod_{\substack{v \mid \mathfrak{c} \\ v \text{ real}}} K_v^*/K_v^+,$$

which maps each element of $K(\mathfrak{c})$ to its residue class in the corresponding component (where the images in the $K_v^*/K_v^+$ are determined by the natural maps $K \to K_v$ that we discussed in the previous section). The kernel of this map is precisely $K_\mathfrak{c}$. Because the codomain is finite, it follows that $K(\mathfrak{c})/K_\mathfrak{c}$ is finite. Hence $K(\mathfrak{c})/UK_\mathfrak{c}$ is finite as well. By 3.3 it then follows that $P(\mathfrak{c})/P_\mathfrak{c}$ is finite. Because $P(\mathfrak{c})/P_\mathfrak{c}$ is the kernel of the map in 3.2, it follows by 3.1 and the fact that the ideal class group is finite that $I(\mathfrak{c})/P_\mathfrak{c}$ is finite as well. ■

If $\mathfrak{c}$ is a cycle of $K$ and $A$ a class in $I(\mathfrak{c})/P_\mathfrak{c}$, then $A$ contains an $\mathcal{O}_K$-ideal: suppose the fractional $K$-ideal $\mathfrak{a}$ is contained in $A$, then for some $x \in \mathcal{O}_K \setminus \{0\}$ we have $\mathfrak{a} \cdot (x) \subset \mathcal{O}_K$. Note that we can choose $x$ coprime to $\mathfrak{c}$, so if the class of $(x)$ in $I(\mathfrak{c})/P_\mathfrak{c}$ has order $k$, we see that $A$ contains the $\mathcal{O}_K$-ideal $\mathfrak{a} \cdot (x^k)$.

## 3.3 Dirichlet's Unit Theorem and its generalization

Recall the map $\Phi_K : K \to \prod_v K_v$. Since, in constructing this map, we had to choose an embedding $\sigma_v$ for every complex embedding $v$, in a way, we threw out some information about the other embedding. To make up for this, we will write for an archimedean absolute value $v$ and an $x \in K_v$

$$\|x\| = \begin{cases} |x| & \text{if } v \text{ is real,} \\ |x|^2 & \text{if } v \text{ is complex.} \end{cases}$$

Note that for an element $\alpha \in K$ it follows that $|N_{K/\mathbb{Q}}(\alpha)| = \prod_v \|\sigma_v(\alpha)\|$.
Now recall Dirichlet's Unit Theorem.

**Theorem 3.2.** *Let $K$ be a number field that has $r_1$ real absolute values and $r_2$ complex absolute values. Then the map*

$$L : \mathcal{O}_K^* \to \prod_v \mathbb{R} = \mathbb{R}^{r_1+r_2} : x \mapsto (\log \|\sigma_v(x)\|)_v,$$

*where $v$ ranges over all archimedean absolute values, maps the unit group $\mathcal{O}_K^*$ of $K$ to an $r_1 + r_2 - 1$-dimensional lattice that lies in the hyperplane*

$$H = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \colon \sum_i x_i = 0\}.$$

*The kernel* $\ker L$ *is the set of roots of unity of $K$.*

*Proof.* See [4, ch. I, §7], [6, p. 104–108], or [5, thm. 5.14]. ■

The map $L$ of Dirichlet's Unit Theorem is often called the *log map.*
Just as with the ideal class group, the concept of the unit group $U := \mathcal{O}_K^*$ can be generalized using cycles. Let $\mathfrak{c}$ be a cycle of $K$, then this "generalized unit group" is defined as $U_\mathfrak{c} = U \cap K_\mathfrak{c}$. We see

$$U/U_\mathfrak{c} = U/(U \cap K_\mathfrak{c}) \cong UK_\mathfrak{c}/K_\mathfrak{c},$$

hence the index $[U : U_{\mathfrak{c}}] \leq [K(\mathfrak{c}) : K_{\mathfrak{c}}]$ is finite.
From this simple observation about the index of $U_{\mathfrak{c}}$ in $U$, we obtain the following generalization of Dirichlet's Unit Theorem.

**Theorem 3.3.** *Let $K$ be a number field that has $r_1$ real absolute values and $r_2$ complex absolute values and let $\mathfrak{c}$ be a cycle of $K$. Then the map*

$$L_{\mathfrak{c}} : U_{\mathfrak{c}} \to \prod_v \mathbb{R} = \mathbb{R}^{r_1+r_2} : x \mapsto (\log \|\sigma_v(x)\|)_v,$$

*where $v$ ranges over all archimedean absolute values, maps the generalized unit group $U_{\mathfrak{c}}$ to an $r_1 + r_2 - 1$-dimensional lattice that lies in the hyperplane*

$$H = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \colon \sum_i x_i = 0\}.$$

*The kernel* $\ker L_{\mathfrak{c}}$ *is the set of roots of unity that lie in $K_{\mathfrak{c}}$.*

It follows that $U_{\mathfrak{c}}$ modulo its roots of unity is a free abelian group of rank $r := r_1+r_2-1$, where $r_1$ and $r_2$ are defined as in the theorem above. Let $u_1, \ldots, u_r \in \mathcal{O}_K^*$ be units such that their images through $L_{\mathfrak{c}}$ generate the $r$-dimensional lattice. Then $u_1, \ldots, u_n$ are called *fundamental units* for $U_{\mathfrak{c}}$.
Let $v_1, \ldots, v_r$ be $r$ distinct archimedean values of all $r+1$ archimedean absolute values of $K$. Then the *regulator of* $U_{\mathfrak{c}}$, is defined as

$$R_{\mathfrak{c}} = \left| \det \begin{pmatrix} \log \|\sigma_{v_1}(u_1)\| & \cdots & \log \|\sigma_{v_1}(u_r)\| \\ \vdots & \ddots & \vdots \\ \log \|\sigma_{v_r}(u_1)\| & \cdots & \log \|\sigma_{v_r}(u_r)\| \end{pmatrix} \right|.$$

This definition is independent of the choice of absolute values $v_1, \ldots, v_r$, since $L_{\mathfrak{c}}$ maps into the hyperplane $H = \{(x_1, \ldots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \colon \sum_i x_i = 0\}$. The determinant is non-zero because of the linear independence of the $L_{\mathfrak{c}}(u_i)$. Finally, it follows from Corollary 2.2 that $R_{\mathfrak{c}}$ is independent of the choice of the $u_i$.
In the case $\mathfrak{c} = (1)$, the regulator $R_{\mathfrak{c}}$ is called the *regulator of* $K$ and is denoted by $R_K$, or simply by $R$.

## 3.4 Discriminants and covolumes of ideals

Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $K$ into $\mathbb{C}$ (both the real and complex embeddings). For $x_1, \ldots, x_n \in K$ we define the *discriminant of* $x_1, \ldots, x_n$ as

$$\Delta(x_1, \ldots, x_n) = \Big( \det(\sigma_i(x_j))_{i,j=1}^n \Big)^2.$$

Suppose $x_1, \ldots, x_n$ are linearly independent over $\mathbb{Q}$, then it follows from the Artin-Dedekind Lemma about the linear independence of characters [7, thm. 12] that $\Delta(x_1, \ldots, x_n) \neq 0$.

If $y_1, \ldots, y_n \in \mathbb{Q}$ are linear independent as well, and $T$ is the base change mapping $x_i$ to $y_i$, then it follows that

$$\Delta(y_1, \ldots, y_n) = \big(\det T\big)^2 \Delta(x_1, \ldots, x_n). \tag{3.4}$$

When $x_1, \ldots, x_n \in \mathcal{O}_K$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, we set $\Delta_K = \Delta(x_1, \ldots, x_n)$, which is independent of the choice of basis by 3.4 and Corollary 2.2. The discriminant $\Delta_K$ is called the *discriminant of* $K$.

**Lemma 3.4.** *Let $K$ be a number of field of degree $n$ over $\mathbb{Q}$ and let $\mathfrak{a}$ be a non-zero ideal of its ring of integers. The map $\Phi_K : K \to \mathbb{R}^n$ maps $\mathfrak{a}$ to an $n$-dimensional lattice that has covolume*

$$\mathrm{Covol}(\Phi_K(\mathfrak{a})) = 2^{-r_2} \mathbf{N}\mathfrak{a} \sqrt{|\Delta_K|},$$

*where $r_2$ is the number of complex absolute values of $K$.*

*Proof.* Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathfrak{a}$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of $K$ and let $\tau_1, \ldots, \tau_{r_2}$ be the complex embeddings that are used to define $\Phi_K$.
Write $\tau_k(\alpha_\ell) = x_{k\ell} + i y_{k\ell}$. Then the discriminant of $\mathfrak{a}$ equals the square of the determinant of

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ x_{11} + iy_{11} & \cdots & x_{1n} + iy_{1n} \\ \vdots & & \vdots \\ x_{11} - iy_{11} & \cdots & x_{1n} - iy_{1n} \\ \vdots & & \vdots \end{pmatrix}.$$

Adding the row corresponding to a $\tau_k$ to the row belonging to $\overline{\tau_k}$, and subsequently substracting $\frac{1}{2}$ times the new row from the row belonging to $\tau_k$ shows that this determinant equals (up to sign) that of

$$2^{r_2} \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ y_{11} & \cdots & y_{1n} \\ \vdots & & \vdots \\ x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \end{pmatrix}.$$

The absolute value of the determinant of the latter matrix (without the scalar in front) is the volume of the parallellotope spanned by the $\Phi_K(\alpha_i)$. The determinant is non-zero, therefore $\mathfrak{a}$ is indeed mapped to an $n$-dimensional lattice.
By 3.4 and 2.2 it follows that

$$\mathrm{Covol}(\Phi_K(\mathfrak{a})) = 2^{-r_2} \sqrt{|\Delta(\alpha_1, \ldots, \alpha_n)|} = 2^{-r_2} \mathbf{N}\mathfrak{a} \sqrt{|\Delta_K|}.$$

■

## 3.5 Counting ideals in ideal classes

If $\mathfrak{c}$ is a cycle of $K$ and $A$ a class in $I(\mathfrak{c})/P_{\mathfrak{c}}$, then we would like to know the number $Z(t;A)$, which is the number of $\mathcal{O}_K$-ideals in $A$ of norm $\leq t$. It turns out $Z(t;A) = \rho t + O(t^{1-1/n})$ as $t \to \infty$, for some $\rho \in \mathbb{R}$.
It is of utmost importance for Chebotarev's Density Theorem that $\rho$ is independent of the class $A$. However, the exact value of $\rho$ is not important in order to prove the density theorem. Nevertheless, we are happy to go the extra mile and compute the exact value of $\rho$, because it will enable us to derive the class number formula in Theorem 4.5.
The following theorem gives the value of $\rho$ and is due to Hecke [8, thm. 121]. We will take a slightly different approach (that of Lang [6, ch. VI, §3]) than Hecke's, because it enables us to obtain the $O$-term in $Z(t;A) = \rho t + O(t^{1-1/n})$ and it lets us deal with generalized ideal class groups rather than just the class group.

**Theorem 3.5.** *Let $K$ be a field of degree $n$ over $\mathbb{Q}$, let $\mathfrak{c}$ be a cycle of $K$, and let $A$ be a class of ideals in $I(\mathfrak{c})/P_{\mathfrak{c}}$. If $Z(t;A)$ denotes the number of (integral) ideals in $A$ of norm $\leq t$, then*

$$Z(t;A) = \frac{2^{r_1+r_2}\pi^{r_2}R_{\mathfrak{c}}}{w_{\mathfrak{c}}2^{s(\mathfrak{c})}\mathbf{N}\mathfrak{c}_0\sqrt{|\Delta_K|}}t + O(t^{1-1/n}),$$

*where $r_1$ is the number of real absolute values and $r_2$ the number complex absolute values of $K$, $s(\mathfrak{c})$ is the number of real absolute values $v \mid \mathfrak{c}$, and $w_{\mathfrak{c}}$ is the number of roots of unity in $K_{\mathfrak{c}}$.*

*Proof.* The counting of ideals can be reduced to the counting of elements of $\mathcal{O}_K$ in some domain $D \subset \mathbb{R}^n$. We should construct this $D$ with care, in order to avoid counting ideals multiple times. This is what we will do first. Afterwards it should become clear why this was the right construction.
Let

$$J_{\mathfrak{c}} = \left\{\xi \in (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \,:\, \xi_v > 0 \text{ for real } v|\mathfrak{c}\right\} \subset \prod_v K_v,$$

where we identify $\prod_v K_v$ with $\mathbb{R}^n$. Using $\Phi_K$ we will view $K_{\mathfrak{c}}$ as a subset of $J_{\mathfrak{c}}$.
Notice that the absolute value of the usual norm on $K$ can be extended to $\prod_v K_v$: send $\xi$ to $\mathbf{N}\xi := \prod_v |\xi_v|^{n_v} = \prod_v \|\xi_v\|$, where $n_v$ is 1 when $v$ is real and 2 otherwise. (The notation $\mathbf{N}\xi$ is consistent with earlier notation, for if $\xi \in \mathcal{O}_K \setminus \{0\}$ then the ideal norm $\mathbf{N}(\xi)$ equals $\prod_v \|\xi_v\|$.) We define the *homogenized log map*

$$h : J_{\mathfrak{c}} \to \mathbb{R}^{r_1+r_2} : \xi \mapsto \left(\log \frac{\|\xi_v\|}{\mathbf{N}\xi^{n_v/n}}\right)_v.$$

The image of $h$ lies in the hyperplane $H \subset \mathbb{R}^{r_1+r_2}$ of all $z$ with $\sum_{i=1}^{r_1+r_2} z_i = 0$.
Write $r = r_1 + r_2 - 1$ and let $V \subset K^*$ be the free subgroup generated by fundamental units $\eta_1, \ldots, \eta_r$ of $U_{\mathfrak{c}}$ (seen as subset of $J_{\mathfrak{c}}$). Writing $y_i = h(\eta_i)$, we see the $y_i$'s generate an $r$-dimensional lattice in $H$ by Theorem 3.3, since the homogenized log map $h$ restricted to $U_{\mathfrak{c}}$ is simply the log map. Define $F$ to be the fundamental domain of this lattice consisting of the

$$c_1y_1 + c_2y_2 + \cdots + c_ry_r, \tag{3.5}$$

with $0 \leq c_i < 1$. Finally define $D = h^{-1}(F) \subset J_{\mathfrak{c}}$.

Now we are ready to think about ideals.
Let $\mathfrak{b} \subset \mathcal{O}_K$ be an ideal in $A^{-1}$. For any ideal $\mathfrak{a} \subset \mathcal{O}_K$ in $A$ we have $\mathfrak{ab} = (\xi)$ for some $\xi = 1 \bmod^* \mathfrak{c}$ that is $0 \bmod \mathfrak{b}$. So $\mathfrak{a} \mapsto \mathfrak{ab}$ is a bijection between $A$ and the classes modulo $U_{\mathfrak{c}}$ of elements $\xi \subset \mathcal{O}_K \cap K_{\mathfrak{c}}$ satisfying $\xi = 1 \bmod^* \mathfrak{c}$ and $\xi = 0 \bmod \mathfrak{b}$.
Because $F$ is a fundamental domain for the lattice $h(V)$, there is precisely one element of the $h(V)$-orbit of $h(\xi)$ contained in $F$. Hence, adjusting for the roots of unity in $U_{\mathfrak{c}}$, for each $\mathfrak{a} \in A$ our domain $D$ contains exactly $w_{\mathfrak{c}}$ such $\xi$ representing $\mathfrak{ab}$.
Moreover, for arbitrary $\xi$ in $D$ we have the implication

$$(\xi = 1 \bmod \mathfrak{c}_0 \wedge \xi = 0 \bmod \mathfrak{b}) \implies (\xi = 1 \bmod^* \mathfrak{c} \wedge \xi = 0 \bmod \mathfrak{b}),$$

because $D$ is a subset of $J_{\mathfrak{c}}$. So it is enough to consider elements in $D$ satisfying the first condition.
Elements $\xi \in D$ satisfying $\xi = 1 \bmod \mathfrak{c}_0$ and $\xi = 0 \bmod \mathfrak{b}$ form a *translated* lattice in $\mathbb{R}^n$: every such element can be translated by an element of $\mathfrak{bc}_0$, and by the Chinese Remainder Theorem every such element is contained in $\xi' + \mathfrak{bc}_0$, for any fixed $\xi'$ satisfying $\xi' = 1 \bmod \mathfrak{c}_0$ and $\xi' = 0 \bmod \mathfrak{b}$. Thus this translated lattice, which we will call $L$, is simply the lattice of $\mathfrak{bc}_0$ translated by some $\xi$ satisfying the first condition. In particular, it has the same covolume.
Hence we find $w_{\mathfrak{c}} Z(t; A)$ is the same as the number of $\xi \in L \cap D$ satisfying $\mathbf{N}\xi \leq \mathbf{N}\mathfrak{b} \cdot t$ (because $\mathbf{N}\mathfrak{a} \leq t \iff \mathbf{N}\mathfrak{ab} \leq \mathbf{N}\mathfrak{b} \cdot t$).
Notice that $tD = D$ for $t > 0$: this follows from the fact that $h(tx) = h(x)$ for all $x \in J_{\mathfrak{c}}$, since $\frac{\|tx_v\|}{(\mathbf{N}tx)^{n_v/n}} = \frac{\|x_v\|}{\mathbf{N}x^{n_v/n}}$. So if we define

$$D_1 = \{x \in D \colon \mathbf{N}x \leq 1\},$$

then the elements $x \in D$ of norm less than or equal to $\mathbf{N}\mathfrak{b} \cdot t$ are those contained in $(\mathbf{N}\mathfrak{b} \cdot t)^{1/n} D_1$.
This means $w_{\mathfrak{c}} Z(t; A)$ equals $\#((\mathbf{N}\mathfrak{b} \cdot t)^{1/n} D_1) \cap L$, or, equivalently,

$$w_{\mathfrak{c}} Z(t; A) = \# D_1 \cap L_t,$$

where we define $L_t$ to be $\frac{1}{(\mathbf{N}\mathfrak{b} \cdot t)^{1/n}} L$.
Let $P_t$ be a fundamental domain of the lattice $\frac{1}{(\mathbf{N}\mathfrak{b} \cdot t)^{1/n}} \mathfrak{bc}_0$ and assign to every $\xi \in D_1 \cap L_t$ the parallellotope $\xi + P_t$. This way we cover $D_1$ with parallelotopes of volume $\operatorname{Covol}(L_t) = \operatorname{Vol}(P_t)$ (which tends to 0 as $t \to \infty$). By definition of the volume, we then find

$$\lim_{t \to \infty} w_{\mathfrak{c}} Z(t; A) \operatorname{Covol}(L_t) = \operatorname{Vol}(D_1). \tag{3.6}$$

Note that the volume of $D_1$ is finite, as $D_1$ is bounded: if $x \in D_1$, we have for every coordinate $|x_v| \leq \mathbf{N}x^{1/n} e^{Br} \leq e^{Br}$, where $B$ is a bound depending on the $y_1, \ldots, y_r$.
By Lemma 3.4 we have $\operatorname{Covol}(L_t) = (\mathbf{N}\mathfrak{b} \cdot t)^{-1} \operatorname{Covol}(L) = (2^{r_2} t)^{-1} \mathbf{N}\mathfrak{c}_0 \sqrt{|\Delta_K|}$. We therefore see

$$Z(t; A) = \frac{2^{r_2} \operatorname{Vol}(D_1)}{w_{\mathfrak{c}} \mathbf{N}\mathfrak{c}_0 \sqrt{|\Delta_K|}} t + \text{some error term}. \tag{3.7}$$

Although the error term is clearly $o(t)$, we still need to prove it is actually $O(t^{1-1/n})$. If we also show that $\mathrm{Vol}(D_1) = 2^{r_1-s(\mathfrak{c})}\pi^{r_2}R_{\mathfrak{c}}$, then we are done.

We will compute the volume first. Let $v_1, \ldots, v_{r_1+r_2}$ be the archimedean absolute values on $K$, with the $v_1, \ldots, v_{r_1}$ being real, and consider $D_1 \subset \mathbb{R}^n$ in polar coordinates $(\rho_i, \theta_i)$ for $i \in \{1, \ldots, r_1 + r_2\}$, with $\rho_i \geq 0$ for all $i$,
$\theta_i = \begin{cases} 1 & \text{if } v_i \mid \mathfrak{c} \text{ and } i \leq r_1, \\ \pm 1 & \text{otherwise if } i \leq r_1, \end{cases}$ and, for $i > r_1$, $\theta_i \in [0, 2\pi]$.
Recalling 3.5, we see the polar coordinates of $D_1$ are those satisying

$$0 < \prod_{i=1}^{r_1+r_2} \rho_i^{n_i} \leq 1 \text{ and } \log \rho_j - \frac{1}{n} \log \prod_{i=1}^{r_1+r_2} \rho_i^{n_i} = \sum_{i=1}^{r} c_i \log |\sigma_{v_j}(\eta_i)|, \text{ for some } c_i \in [0, 1).$$

These conditions do not depend on the $\theta_i$. So consider only the space $P \subset \mathbb{R}^{r_1+r_2}$ of $(\rho_1, \ldots \rho_{r_1+r_2})$ satisfying these conditions. The Jacobian determinant of $(\rho, \theta) \mapsto \rho(\cos\theta, \sin\theta)$ equals $\rho$. Thus

$$\mathrm{Vol}(D_1) = (2\pi)^{r_2} 2^{r_1-s(\mathfrak{c})} \int_P \rho_{r_1+1} \cdots \rho_{r_1+r_2} d\rho_1 \cdots d\rho_{r_1+r_2}.$$

In order to compute this integral, we will do a change of variables. Consider in the variables $(u, c_1, \ldots, c_r)$ the cube $S = (0, 1] \times [0, 1)^r$. Then we have a bijection $f : S \to P$ given by

$$\rho_j = f_j(u, c_1, \ldots, c_r) = u^{1/n} \exp\Big( \sum_{i=1}^{r} c_i \log |\sigma_{v_j}(\eta_i)| \Big).$$

In the other direction we have $u = \prod_{i=1}^{r_1+r_2} \rho_i^{n_i}$, and the fact that the regulator $R_{\mathfrak{c}} = \Big| \det(\log \|\sigma_j(\eta_i)\|)_{i,j=1}^{r} \Big|$ is non-zero ensures there is a unique solution for the $c_i$.
Let's compute the Jacobian determinant of $f$. First note $\partial\rho_j/\partial u = \frac{1}{n}\rho_j/u$ and $\partial\rho_j/\partial c_i = \rho_j \log |\sigma_{v_j}(\eta_i)|$. So

$$\det(\mathrm{Jac}(f)) = \frac{2^{-r_2}}{n\rho_{r_1+1} \cdot \rho_{r_1+r_2}} \det \begin{pmatrix} 1 & \log |\sigma_{v_1}(\eta_1)| & \cdots & \log |\sigma_{v_1}(\eta_r)| \\ \vdots & \vdots & & \vdots \\ 1 & \log |\sigma_{v_{r_1+r_2}}(\eta_1)| & \cdots & \log |\sigma_{v_{r_1+r_2}}(\eta_r)| \end{pmatrix}.$$

Adding the first $r$ rows to the last after multiplying the $j$'th row by $n_j$ shows us $|\det(\mathrm{Jac}(f))| = \dfrac{2^{-r_2} R_{\mathfrak{c}}}{\rho_{r_1+1} \cdots \rho_{r_1+r_2}}$. Hence

$$\mathrm{Vol}(D_1) = (2\pi)^{r_2} 2^{r_1-s(\mathfrak{c})} \int_S 2^{-r_2} R_{\mathfrak{c}} = 2^{r_1-s(\mathfrak{c})} \pi^{r_2} R_{\mathfrak{c}},$$

as was to be shown.

Finally, let us consider the error term in 3.7.
First note that $f$ can be continuously extended to a map with domain $[0,1]^{r_1+r_2}$ onto the closure $\overline{P}$ of $P$, and by considering $\widetilde{f} = f(u^n, c_1, \ldots, c_r)$ we obtain a smooth map $\widetilde{f} : [0,1]^{r_1+r_2} \to \overline{P}$.
For each real absolute value $v_i$ of $K$ that does *not* divide $\mathfrak{c}$, the variable $\theta_i$ can be either 1 or $-1$. This means $D_1$ has $2^{r_1-s(\mathfrak{c})}$ connected components. Combining the maps $\widetilde{f}$ and $\theta \mapsto (\cos 2\pi\theta, \sin 2\pi\theta)$ we obtain smooth parametrizations of the components of $D_1$, denoted by $\widetilde{f}_1, \ldots, \widetilde{f}_{2^{r_1-s(\mathfrak{c})}} : [0,1]^{r_1+r_2} \times [0,1]^{r_2} = [0,1]^n \to D_1$, one for each component of $D_1$.
For the boundaries we have

$$\bigcup_j \widetilde{f}_j\big(\partial\left([0,1]^n\right)\big) \supset \partial D_1,$$

which means that the boundary $\partial D_1$ can be covered by the images of $M = 2n \cdot 2^{r_1-s(\mathfrak{c})}$ different smooth maps $g_j : [0,1]^{n-1} \to \partial D_1$.
When estimating the volume of $D_1$ as in 3.6 we can only under- or overestimate near the boundary of $D_1$. For all $t$ we can bound this error absolutely by $\mathrm{Covol}(L_t) \cdot I_t$, where $I_t$ is the number of parallellotopes intersecting the boundary:

$$I_t = \#\Big\{\xi \in L_t \colon (\xi + P_t) \cap \partial D_1 \neq \emptyset\Big\}.$$

So the error term in 3.7 can be bounded by $I_t$. We claim $I_t = O(t^{1-1/n})$ as $t \to \infty$. To see this, cut up each side of the unit $n-1$ cube $[0,1]^{n-1}$ into $\lceil t^{1/n} \rceil$ parts of equal length to obtain $\lceil t^{1/n} \rceil^{n-1}$ small cubes, that we collect in the set of small cubes $C_t$.
For a given $t$, the images of all small cubes in $C_t$ through all maps $g_j$ cover the boundary $\partial D_1$. The maps $g_j$ are smooth and hence Lipschitz, so the diameter of a set $g_j(k)$, $k \in C_t$ being a small cube, can be bounded by $ct^{-1/n}$ for some constant $c$ independent of $k$, $j$, or $t$.
Finally, there is a constant $S > 0$, only depending on the translated lattice $L_1 = \frac{1}{(\mathbf{N}\mathfrak{b})^{1/n}} L$, such that the maximal number of parallellotopes $\xi + P_1$ (for $\xi \in L_1$) that a set with diameter at most $c$ can intersect is bounded by $S$. Thus the number of parallellotopes $\xi + P_t$ (for $\xi \in L_t$) that an image of a small cube $g_j(k)$ can intersect is also bounded by $S$. Hence we see that we can bound $I_t$ by

$$M \cdot S \cdot \lceil t^{1/n} \rceil^{n-1} = O(t^{1-1/n}) \text{ as } t \to \infty,$$

proving our last claim.

■

# 4 Zeta functions of number fields

This chapter will essentially be the first part of chapter VIII (excluding §4) of Lang's *Algebraic Number Theory* [6]. All theorems found here can be found there, with more or less the same proofs.

## 4.1 Dirichlet series

Dirichlet series play a central role in Chebotarev's Density Theorem and, indeed, in number theory, as the zeta functions and $L$-series can be expressed as Dirichlet series. In order to study the latter functions, we will prove some elementary results about Dirichlet series. But first of all: what are they?

**Definition** (Dirichlet series)**.** *A Dirichlet series is a series of the form*

$$\sum_{n=1}^{\infty} a_n/n^s,$$

*where the $a_n$ are complex numbers and $s$ is a complex variable.*

If $\{a_n\}$ and $\{b_n\}$ are sequences of complex numbers and $A_n$ denotes the partial sum $a_1 + \cdots + a_n$ for $n \in \mathbb{N}$ (and $A_0 = 0$), then recall or check the following identity of summation by parts:

$$\sum_{i=m}^{n} a_i b_i = A_n b_n - A_{m-1} b_m + \sum_{i=m}^{n-1} A_i (b_i - b_{i+1}) \text{ for } m \leq n.$$

We are interested in when and where a Dirichlet series converges. The summation by parts identity will prove useful.

**Lemma 4.1.** *If the Dirichlet series $\sum a_n/n^s$ converges for $s = s_0$, then it converges for any $s$ with $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, uniformly on any compact subset of this region. In particular, it then defines an analytic function in that region.*

*Proof.* We will sum $\sum \dfrac{a_n}{n^{s_0}} \dfrac{1}{n^{s-s_0}}$ by parts. Writing $P_n(s_0) = \sum_{k=1}^{n} \dfrac{a_k}{k^{s_0}}$ this yields for $n > m$ the following:

$$\sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} = \frac{P_n(s_0)}{n^{s-s_0}} - \frac{P_m(s_0)}{(m+1)^{s-s_0}} + \sum_{k=m+1}^{n-1} P_k(s_0)\Big(\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}}\Big).$$

If $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ we have

$$\Big|\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}}\Big| = \Big|(s-s_0)\int_k^{k+1} \frac{1}{x^{s-s_0+1}}dx\Big| \leq \Big|\frac{(s-s_0)}{k}\Big|.$$

So if $\delta > 0$ and $\mathrm{Re}(s) \geq \delta + \mathrm{Re}(s_0)$, then it follows that $\sum_{k=m+1}^{n} a_k/k^s = \sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}}$ will get uniformly arbitrarily small, whenever $|s - s_0|$ is bounded.
Finally, this means the Dirichlet series defines an analytic series on $\mathrm{Re}(s) > \mathrm{Re}(s_0)$: the series is a limit of analytic functions that converges uniformly on compact sets, hence it is itself analytic by a theorem of Weierstraß [9, thm. III.1.3]. ■

The previous lemma tells us the following definition – similar to the radius of convergence of power series – makes sense.

**Definition** (Abscissa of convergence)**.** *Let $\sum a_n/n^s$ be a Dirichlet series. Then the smallest real number (or $\pm\infty$) $\sigma_0$ such that the series converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \sigma_0$ is called the abscissa of convergence.*

Now we will obtain a way to find an upper bound of the abscissa of convergence.

**Lemma 4.2.** *Assume here exists a $C \in \mathbb{R}$ and a $\sigma_1 > 0$ such that*

$$|A_n| = |a_1 + \cdots + a_n| \leq Cn^{\sigma_1}$$

*for all partial sums $A_n$. Then the abscissa of convergence of $\sum a_n/n^s$ is less than or equal to $\sigma_1$.*

*Proof.* Again writing $P_n(s) = \sum_{k=1}^{n} \frac{a_k}{k^s}$, we find for $n > m$ by summation by parts

$$\begin{aligned} P_n(s) - P_m(s) &= \frac{A_n}{n^s} - \frac{A_m}{(m+1)^s} + \sum_{k=m+1}^{n-1} A_k\Big(\frac{1}{k^s} - \frac{1}{(k+1)^s}\Big) \\ &= \frac{A_n}{n^s} - \frac{A_m}{(m+1)^s} + \sum_{k=m+1}^{n-1} A_k s \int_k^{k+1} \frac{1}{x^{s+1}}dx. \end{aligned}$$

Let $\delta > 0$ and suppose $\mathrm{Re}(s) \geq \sigma_1 + \delta$. Then for all $k$ we have

$$\Big|A_k \int_k^{k+1} \frac{1}{x^{s+1}}\Big| \leq C\int_k^{k+1} \frac{1}{x^{\mathrm{Re}(s)-\sigma_1+1}}dx,$$

hence

$$|P_n(s) - P_m(s)| \leq \frac{2C}{(m+1)^\delta} + |s|C\int_{m+1}^{n} \frac{1}{x^{1+\delta}}dx,$$

which tends to zero for $m$ and $n$ large. ■

Now consider

$$\zeta(s) = \sum \frac{1}{n^s},$$

which is analytic on $\{s \in \mathbb{C}\colon \operatorname{Re}(s) > 1\}$ by the previous lemma. This function is called the Riemann zeta function and has an analytic continuation to the right half plane $\{s \in \mathbb{C}\colon \operatorname{Re}(s) > 0\}$, *except for a single pole.*

**Lemma 4.3.** *The Riemann zeta function has an analytic continuation to* $\{s \in \mathbb{C}\colon \operatorname{Re}(s) > 0\}$*, except for a simple pole at* $s = 1$ *with residue* 1*.*

*Proof.* To find the analytic continuation let us consider "the alternating zeta function"

$$\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots.$$

By the previous lemma $\zeta_2(s)$ is analytic on $\{s \in \mathbb{C}\colon \operatorname{Re}(s) > 0\}$, since the partial sums of its coefficients alternate between 1 and 0 and are thus bounded. On the other hand, we have for $s$ with $\operatorname{Re} s > 1$

$$\frac{2}{2^s}\zeta(s) + \zeta_2(s) = \zeta(s),$$

and hence

$$\zeta(s) = (1 - \frac{2}{2^s})^{-1}\zeta_2(s),$$

which gives us an analytic continuation to $\operatorname{Re}(s) > 0$, except possibly for $s \in 1 + \frac{2\pi}{\log 2}\,\mathbb{Z}\,i$. To analyze these possible poles, consider the more general alternating zeta functions for $r \in \mathbb{N}$:

$$\zeta_r(s) = 1 + \frac{1}{2^s} + \cdots + \frac{1}{(r-1)^s} - \frac{r-1}{r^s} + \frac{1}{(r+1)^s} + \cdots.$$

For the same reason as for $r = 2$ they are analytic on $\operatorname{Re}(s) > 0$. And, like before, we get an identity $\frac{r}{r^s}\zeta(s) + \zeta_r(s) = \zeta(s)$ and hence another analytic continuation of the Riemann zeta function:

$$\zeta(s) = (1 - \frac{r}{r^s})^{-1}\zeta_r(s).$$

Taking for example $\zeta_3(s)$, we see that $\zeta(s)$ can only have poles for $s$ in $1 + \frac{2\pi}{\log 3}\,\mathbb{Z}\,i$. So for any pole $s \neq 1$ we have $s = 1 + \frac{2\pi i}{\log 2}n = 1 + \frac{2\pi i}{\log 3}m$, implying $2^n = 3^m$, which is only possible if $m = n = 0$.
Hence the only pole of $\zeta(s)$ is the one at $s = 1$. Note that for real $s > 1$ we have

$$\frac{1}{s-1} = \int_1^\infty \frac{1}{x^s}dx \leq \zeta(s) \leq 1 + \frac{1}{s-1}.$$

This implies

$$1 \leq (s-1)\zeta(s) \leq s \text{ for real } s > 1.$$

Letting $s$ go to 1 shows $\zeta(s)$ indeed has a simple pole at $s = 1$ with residue 1. ∎

The preceding lemma is the easiest case of the class number formula, that we prove in the next section in Theorem 4.5. The theorem will in fact follow quickly from the work we have done so far. Its proof uses the following theorem along with the main theorem of the previous chapter. It is no coincidence the $O$-notation is turning up again!

**Theorem 4.4.** *Let $\{a_n\}$ be a sequence in $\mathbb{C}$ with partial sums $A_n$. Let $0 \leq \sigma_1 < 1$, and assume there is a $\rho \in \mathbb{C}$ such that*

$$A_n = \rho n + O(n^{\sigma_1}) \text{ as } n \to \infty.$$

*Then the function*

$$f(s) = \sum_{n=1}^{\infty} a_n/n^s,$$

*defined by the Dirichlet series on $\{s \in \mathbb{C}\colon \mathrm{Re}(s) > 1$ has an analytic continuation to the $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \sigma_1$, except for a simple pole at $s = 1$ with residue $\rho$.*

*Proof.* Apply Lemma 4.2 to the Dirichlet series $f(s) - \rho\zeta(s)$ to see it is analytic on $\mathrm{Re}(s) > \sigma_1$. Then use the previous lemma to see $f(s) = (f(s) - \rho\zeta(s)) + \rho\zeta(s)$ itself is analytic on $\mathrm{Re}(s) > \sigma_1$ except for a pole at $s = 1$ with residue equal to $\rho$. ■

## 4.2 Zeta functions and $L$-series

Throughout, let $K$ be a number field and $N = [K : \mathbb{Q}]$.

### Zeta functions

We have seen the Riemann zeta function in the previous section. One of the main reasons we are interested in it is because it allows for a vast generalization: it turns out every number field has a zeta function associated to it!
For the number field $K$, it is given by the (Dirichlet) series

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathbf{N}\mathfrak{a}^s},$$

where we sum over all non-zero ideals of the ring of integers of $K$. We call it the *Dedekind zeta function* of $K$. Note that the Dedekind zeta function of $\mathbb{Q}$ is the Riemann zeta function.
We are ready to state and prove the class number formula, which is an important result in its own right that gives an explicit formula for the residue of $\zeta_K(s)$ at $s = 1$. For the purposes of proving Chebotarev's Density Theorem, however, we note that we do not need the exact value of this residue, but only the fact that $\zeta_K(s)$ is analytic for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1 - 1/N$ with the exception of a single pole at $s = 1$ that is simple.

**Theorem 4.5** (Class number formula)**.** *The Dedekind zeta function $\zeta_K(s)$ is analytic for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1 - 1/N$, except for a single simple pole at $s = 1$ whose residue is given by*

$$\frac{2^{r_1+r_2}\pi^{r_2}hR}{w\sqrt{|\Delta_K|}},$$

*where $r_1$ is the number of real embeddings of $K$ and $r_2$ is the number of complex embeddings up to conjugation, $h$ is the class number of $K$, $R$ the regulator, and $w$ is the number of roots of unity of $K$.*

*Proof.* For some coefficients $a_1, a_2, \ldots$ we can write $\zeta_K(s) = \sum a_n/n^s$. The partial sum $A_n$ of the coefficients equals the number of non-zero ideals of $\mathcal{O}_K$ of norm less than or equal to $n$. Hence, by Theorem 3.5,

$$|A_n| = \sum_{C \in I/P} Z(n; C) = \frac{2^{r_1+r_2}\pi^{r_2}hR}{w\sqrt{|\Delta_K|}} n + O(n^{1-1/N}).$$

Theorem 4.4 finishes the proof. ∎

The Dedekind zeta function has another well-known description given as a formal product, called the *Euler product*

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathbf{N}\mathfrak{p}^s}},$$

ranging over all non-zero prime ideals.
To see it indeed describes $\zeta_K(s)$ we can take the logarithm of the formal product to obtain

$$\sum_{\mathfrak{p}} -\log(1 - \mathbf{N}\mathfrak{p}^s) = \sum_{m,\mathfrak{p}} \frac{1}{m\mathbf{N}\mathfrak{p}^{ms}},$$

using the expansion $\log(1 - x) = \sum_n -x^n/n$ for $|x| < 1$.
If $\mathrm{Re}(s) = \sigma > 1$ this sum is dominated by

$$\sum_{m,p} \frac{N}{mp^{m\sigma}} < \sum_{m,p} \frac{N}{p^{m\sigma}} < N\zeta(\sigma) < \infty,$$

where we sum over all rational prime numbers $p$.
Hence the logarithm of the product converges uniformly on $\{s \in \mathbb{C} \colon \mathrm{Re}(s) > 1\}$ by the Weierstraß M-test, and it is thus analytic on $\{s \in \mathbb{C} \colon \mathrm{Re}(s) > 1\}$ (again by [9, thm. III.1.3]). So when we exponentiate it again we get the product expression back, which apparently converges. Multiplying out yields

$$\prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathbf{N}\mathfrak{p}^s}} = \prod_{\mathfrak{p}} \left(1 + 1/\mathbf{N}\mathfrak{p}^s + 1/\mathbf{N}\mathfrak{p}^{2s} + \cdots\right) = \sum_{\mathfrak{a}} \frac{1}{\mathbf{N}\mathfrak{a}^s} = \zeta_K(s),$$

which follows from multiplicativity of the norm map and the unique prime factorization of ideals in $\mathcal{O}_K$.

The logarithm of the Dedekind zeta function is of utmost importance in defining the density of sets of prime ideals in the next chapter. Especially the fact that it has a pole in $s = 1$ is crucial. We have

$$\sum_{m\geq 2,\mathfrak{p}} \frac{1}{m\mathbf{N}\mathfrak{p}^m} < \sum_{p,m} \frac{N}{p^{2m}} + \sum_{p,m} \frac{N}{p^{2m+1}} < \infty.$$

Hence only

$$\sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s}$$

contributes to the pole of $\log \zeta_K$ at $s = 1$. In fact, using a similar argument, only the primes $\mathfrak{p}$ of absolute degree 1 contribute to the pole: the other primes have norm equal to a perfect power of a rational prime, so the reciprocals of those norms do not contribute to the pole.
Let us write $f \sim g$ if $f$ and $g$ differ (additively) by a function that is analytic at $s = 1$. From the discussion above it then follows that

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s} \sim \sum_{\deg_{\mathbb{Q}} \mathfrak{p}=1} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Because $\zeta_K(s)$ has a simple pole at $s = 1$ we have that $\log\big((s-1)\zeta_K\big)$ is analytic around $s = 1$ and thus

$$\log \frac{1}{s-1} \sim \log \zeta_K(s).$$

Later we will gratefully use the fact that all logarithms of Dedekind zeta functions differ from each other by functions that are analytic around 1.

### $L$-series

Another interesting class of functions are the so-called *$L$-series*. They are similar to the Dedekind zeta functions, but now we plug in some character of the ideal class group, or more generally, of $I(\mathfrak{c})/P_{\mathfrak{c}}$ for some cycle $\mathfrak{c}$ of $K$. Let $\chi : I(\mathfrak{c})/P_{\mathfrak{c}} \to \mathbb{C}^*$ be such a character. Then we define

$$L_{\mathfrak{c}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{c}} \Big(1 - \frac{\chi(\mathfrak{p})}{\mathbf{N}\mathfrak{p}^s}\Big)^{-1},$$

where by $\chi(\mathfrak{p})$ we mean $\chi(\overline{\mathfrak{p}})$, $\overline{\mathfrak{p}}$ being the class of $\mathfrak{p}$ in $I(\mathfrak{c})/P_{\mathfrak{c}}$.
Just as with the zeta functions, we also have

$$L_{\mathfrak{c}}(s,\chi) = \sum_{\mathfrak{a}\nmid\mathfrak{c}} \frac{\chi(\mathfrak{a})}{\mathbf{N}\mathfrak{a}^s},$$

using the multiplicativity of $\chi$.
If $\chi$ and $\mathfrak{c}$ are trivial we obtain the Dedekind zeta function $\zeta_K(s)$. However, when $\chi$ is non-trivial $L_{\mathfrak{c}}(s,\chi)$ has no pole at $s=1$, contrary to the Dedekind zeta functions.

**Theorem 4.6.** *If $\chi \neq 1$ is a character of $I(\mathfrak{c})/P_{\mathfrak{c}}$, the Dirichlet series representation for $L_{\mathfrak{c}}(s,\chi)$ is convergent for $\mathrm{Re}(s) > 1 - 1/N$.*

*Proof.* Let $B \in I(\mathfrak{c})/P_{\mathfrak{c}}$ be such that $\chi(B) \neq 1$, then

$$\chi(B) \sum_{A \in I(\mathfrak{c})/P_{\mathfrak{c}}} \chi(A) = \chi(B) \sum_{A \in I(\mathfrak{c})/P_{\mathfrak{c}}} \chi(B^{-1}A) = \sum_{A \in I(\mathfrak{c})/P_{\mathfrak{c}}} \chi(A),$$

from which we conclude that $\sum_{A \in I(\mathfrak{c})/P_{\mathfrak{c}}} \chi(A) = 0$.
Theorem 3.5 tells us all classes in $A \in I(\mathfrak{c})/P_{\mathfrak{c}}$ contain, for some $\rho$ independent of $A$, $\rho n + O(n^{1-1/N})$ ideals of norm less than $n$ as $n \to \infty$. So if we write $L_{\mathfrak{c}}(s,\chi) = \sum a_n/n^s$, with partial sums of the coefficients $A_n$, we obtain

$$A_n = \rho \sum_{A \in I(\mathfrak{c})/P_{\mathfrak{c}}} \chi(A) + O(n^{1-1/N}) = O(n^{1-1/N}) \text{ as } n \to \infty.$$

The theorem follows by an application of Theorem 4.4. ■

# 5 Density of ideals

## 5.1 The Dirichlet density

From the preceding chapter we collect the following result:

**Lemma 5.1.** *For every number field $K$ we have*

$$\log \frac{1}{s-1} \sim \log \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s} \sim \sum_{\deg_{\mathbb{Q}} \mathfrak{p}=1} \frac{1}{\mathbf{N}\mathfrak{p}^s} \quad \text{as } s \downarrow 1.$$

It leads to a natural definition of the density of a subset of prime ideals: the *Dirichlet density*.

**Definition** (Dirichlet density)**.** *Let $K$ be a number field and $A$ a subset of the set of all non-zero prime ideals of $\mathcal{O}_K$. Then we define the (Dirichlet) density of $A$ as*

$$\lim_{s \downarrow 1} \frac{\displaystyle\sum_{\mathfrak{p} \in A} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \dfrac{1}{s-1}},$$

*if this limit exists.*

A more intuitive notion of density is called "natural density" and is defined by

$$\lim_{n \to \infty} \frac{\#\{\mathfrak{p} \in A : \mathbf{N}\mathfrak{p} \leq n\}}{\#\{\mathfrak{p} : \mathbf{N}\mathfrak{p} \leq n\}}.$$

It turns out that if the natural density exists, then the Dirichlet density exists as well and must be equal to it [10, p. 118–120]. However, the converse does not necessarily hold: there are (pathological) cases of sets of primes that have a Dirichlet density, but not a natural density [11, p. 76].
We will only work with the Dirichlet density, and shall therefore often omit the "Dirichlet" part when refering to the Dirichlet density.
Finally, we will adopt a convention common in other parts of mathematics: when all prime ideals of the ring of integers of some number field satisfy a certain property, except for those in a set of density 0, we will say that *almost all* prime ideals satisfy said property.

## 5.2 Arithmetic progressions and cyclotomic extensions

When $a$ and $m$ are coprime rational integers, Dirichlet's Theorem on Arithmetic Progressions states that there are infinitely many primes in the arithmetic progression

$$a,\ a+m,\ a+2m,\ a+3m,\ a+4m,\ a+5m,\ \ldots\ .$$

An even stronger result says the density of these primes exists and equals $1/\varphi(m)$. This result follows from taking $K=\mathbb{Q}$ in the following theorem (cf. the "Universal Norm Index Inequality" and the corollary to Theorem 8 of Chapter VIII of [6]).

**Theorem 5.2.** *Let $K(\zeta_m)/K$ be a cyclotomic extension of number fields, where $\zeta_m$ is an $m$'th primitive root of unity. Let $b\in G=\mathrm{Gal}(K(\zeta_m)/K)\subset(\mathbb{Z}/m\,\mathbb{Z})^*$ and let $S_b$ be the set of unramified prime ideals $\mathfrak{p}$ of $K$ above which there is prime $\mathfrak{P}\subset\mathcal{O}_{K(\zeta_m)}$ with Frobenius element $(\mathfrak{P},K(\zeta_m)/K)=b$. Then*

$$S_b=\{\mathfrak{p}\subset\mathcal{O}_K\colon \mathfrak{p}\ \textit{is unramified in}\ K(\zeta_m)\ \textit{and}\ \mathbf{N}\mathfrak{p}=b \bmod m\}.$$

*Moreover, $S_b$ has a density, equal to*

$$\lim_{s\downarrow 1}\ \frac{\displaystyle\sum_{\mathbf{N}\mathfrak{p}=b \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log\dfrac{1}{s-1}}=\frac{1}{[K(\zeta_m):K]}.$$

*Proof.* Let $\mathfrak{c}$ be a cycle of $K$ containing all real valuations, the ideal $(m)$, and all primes of $K$ that ramify in $K(\zeta_m)$ (and no other ideals). This means the prime ideals of $K$ that are coprime to $\mathfrak{c}$ are unramified in $K(\zeta_m)$.
Let $\mathfrak{p}$ be a prime of $K$ that is unramified in $K(\zeta_m)$ and let $\mathfrak{P}\subset\mathcal{O}_{K(\zeta_m)}$ be a prime above it. Looking at the residue class fields, we see the Frobenius element $(\mathfrak{P},K(\zeta_m)/K)$ (acting on $\mathcal{O}_{K(\zeta_m)}/\mathfrak{P}$) sends $\zeta_m\in\mathcal{O}_{K(\zeta_m)}/\mathfrak{P}$ to $\zeta_m^{\mathbf{N}\mathfrak{p}}$, which means $(\mathfrak{P},K(\zeta_m)/K)=\mathbf{N}\mathfrak{p}\in(\mathbb{Z}/m\,\mathbb{Z})^*$. This proves the first statement that

$$S_b=\{\mathfrak{p}\subset\mathcal{O}_K\colon \mathfrak{p}\ \text{is unramified in}\ K(\zeta_m)\ \text{and}\ \mathbf{N}\mathfrak{p}=b \bmod m\}.$$

The ideals in $P_{\mathfrak{c}}$ are of the form $(a)$ with $a=1 \bmod^* \mathfrak{c}$, which implies $a=1 \bmod m$ and $\sigma(a)>0$ for every real embedding $\sigma$. We have $N_{K/\mathbb{Q}}(a)>0$, as the norm of $a$ is the product of its Galois conjugates and in this product, by construction, every real conjugate is positive and of course the non-real conjugates can be paired with their complex conjugates. The congruence $a'=1 \bmod m$ also holds for the Galois conjugates $a'$ of $a$, and hence $N_{K/\mathbb{Q}}(a)=1 \bmod m$. Thus $\mathbf{N}(a)=|N_{K/\mathbb{Q}}(a)|=1 \bmod m$.
As a result, the morphism $I(\mathfrak{c})\to G:\mathfrak{a}\mapsto(\mathbf{N}\mathfrak{a} \bmod m)$ factors through $I(\mathfrak{c})/P_{\mathfrak{c}}$. In this way we can view characters of $G$ as characters of $I(\mathfrak{c})/P_{\mathfrak{c}}$. We will denote the set of such characters of $I(\mathfrak{c})/P_{\mathfrak{c}}$ by $X$.
Let $\chi\in X$ be a non-trivial character. By Theorem 4.6 $L_{\mathfrak{c}}(s,\chi)$ is analytic around 1. We shall see in a moment that $L_{\mathfrak{c}}(1,\chi)\neq 0$.

Write $m(\chi)$ for the order of the zero of $L_{\mathfrak{c}}(s,\chi)$ in $s=1$. So $m(\chi)\geq 0$. Then for some $g$ analytic around 1 we have $L_{\mathfrak{c}}(s,\chi)=(s-1)^{m(\chi)}g(s)$, hence

$$\log L_{\mathfrak{c}}(s,\chi)\sim m(\chi)\log(s-1)\sim -m(\chi)\log\frac{1}{s-1}.$$

For $s\in\mathbb{C}$ with $\mathrm{Re}(s)>1$ and any character $\chi$ of $G$, we can view $\chi$ as an element of $X$ and write

$$\log L_{\mathfrak{c}}(s,\chi)\sim\sum_{a\in G}\chi(a)\sum_{\mathbf{N}\mathfrak{p}=a \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s}. \tag{5.1}$$

(Note that 5.1 holds even if the sum on the right hand side would range over some $\mathfrak{p}\mid\mathfrak{c}$, as there are only finitely many $\mathfrak{p}$ dividing $\mathfrak{c}$.)
Summing over all characters of $G$, we obtain

$$\big(1-\sum_{\chi\neq 1}m(\chi)\big)\log\frac{1}{s-1}\sim\log\zeta_K(s)+\sum_{\chi\neq 1}\log L_{\mathfrak{c}}(s,\chi)\sim\sum_{\chi}\sum_{a\in G}\chi(a)\sum_{\mathbf{N}\mathfrak{p}=a \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Recall that the characters of $G$ form a group (the dual group) of the same order as $G$, and that the elements of $G$ can be viewed as characters of the dual group [12, ex. 5.13]. Thus

$$\sum_{\chi}\sum_{a\in G}\chi(a)\sum_{\mathbf{N}\mathfrak{p}=a \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s}=\#G\sum_{\mathbf{N}\mathfrak{p}=1 \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s},$$

as $\sum_\chi\chi(a)=0$, unless $a$ is the identity element of $G$.
A prime ideal $\mathfrak{p}$ of $K$ splits completely in $K(\zeta_m)$ if and only if $\mathbf{N}\mathfrak{p}=1 \bmod m$, and in that case it has precisely $\#G=[K(\zeta_m):K]$ primes $\mathfrak{P}$ of $K(\zeta_m)$ above it. Recall only primes $\mathfrak{P}$ of absolute degree 1 contribute to the poles (and for these primes $\mathfrak{P}\cap K$ splits completely in $K(\zeta_m)$). Taking all this in consideration, we find

$$\big(1-\sum_{\chi\neq 1}m(\chi)\big)\log\frac{1}{s-1}\sim\#G\sum_{\mathbf{N}\mathfrak{p}=1 \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s}\gtrsim\sum_{\deg_{\mathbb{Q}}\mathfrak{P}=1}\frac{1}{\mathbf{N}\mathfrak{P}^s}\sim\log\frac{1}{s-1},$$

where we consider only real values $s>1$, let $s\to 1$, and use the sign $\gtrsim$ to mean that the right-hand side is less than or equal to the left-hand side plus some constant in a neighbourhood of 1.
This shows $m(\chi)=0$ for all non-trivial $\chi$.

Now let $b\in G$ and multiply both sides of (5.1) by $\chi(b^{-1})$. Sum over all $\chi$ and use the fact that $\log L_{\mathfrak{c}}(s,\chi)$ is analytic around 1 for non-trivial $\chi$ to get

$$\log\frac{1}{s-1}\sim\log\zeta_K(s)\sim\sum_{a\in G}\sum_{\chi}\chi(ab^{-1})\sum_{\mathbf{N}\mathfrak{p}=a \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

The sum over the $\chi$ yields 0 unless $a=b \bmod m$, and hence

$$\log\frac{1}{s-1}\sim\#G\sum_{\mathbf{N}\mathfrak{p}=b \bmod m}\frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

This finishes the proof, as

$$\lim_{s\downarrow 1} \frac{\sum_{\mathbf{N}\mathfrak{p}=b \bmod m} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}} = \frac{1}{\#G} = \frac{1}{[K(\zeta_m):K]}.$$

■

**Corollary 5.3** (Dirichlet's Theorem on Arithmetic Progressions)**.** *Let $m$ be an integer and $a \in (\mathbb{Z}/m\mathbb{Z})^*$. Then the set $S_a$ of prime numbers $p \in \mathbb{Z}$ for which $a = p \bmod m$ has a density, equal to*

$$\frac{1}{\varphi(m)}.$$

.

*Proof.* We have

$$\lim_{s\downarrow 1} \frac{\sum_{p=a \bmod m} \frac{1}{p^s}}{\log \frac{1}{s-1}} = \lim_{s\downarrow 1} \frac{\sum_{\mathbf{N}(p)=a \bmod m} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}} = \frac{1}{[K(\zeta_m):K]},$$

by Theorem 5.2, where the first equality holds because $\mathbf{N}(p) = p$ and only finitely many $p$ ramify in $\mathbb{Q}(\zeta_m)$. ■

## 5.3 Chebotarev's Density Theorem

Let $L/K$ be a Galois extension of number fields and $\sigma \in \mathrm{Gal}(L/K)$. Write

$$S_\sigma = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ is unramified in } L \text{ and } \exists \mathfrak{P} \subset \mathcal{O}_L \text{ above } \mathfrak{p} \text{ with } (\mathfrak{P}, L/K) = \sigma\}.$$

In the case $L/K$ cyclotomic we know from Theorem 5.2 that $S_\sigma$ has a density equal to $1/[L:K]$. For the general case it is Chebotarev's Density Theorem that states that $S_\sigma$ has a density, and the theorem also gives its value, which might be different from $1/[L:K]$.
Suppose $\mathfrak{p} \in S_\sigma$ and that $\mathfrak{P} \subset \mathcal{O}_L$ lies above $\mathfrak{p}$ and $(\mathfrak{P}, L/K) = \sigma$. Then for any $\tau \in \mathrm{Gal}(L/K)$ we have $(\tau\mathfrak{P}, L/K) = \tau\sigma\tau^{-1}$. So we see that

$$S_\sigma = S_{\tau\sigma\tau^{-1}}.$$

Hence, supposing $C \subset \mathrm{Gal}(L/K)$ is the conjugacy class of $\sigma$, it is not be ambiguous to write $S_C := S_\sigma$. We will introduce some convenient notation for the densities we are interested in.

**Definition** (The (upper and lower) density of $S_C$)**.** *For a Galois extension of number fields $L/K$, a conjugacy class $C \subset \mathrm{Gal}(L/K)$, and*

$$S_C = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ is unramified in } L \text{ and } \exists \mathfrak{P} \subset \mathcal{O}_L \text{ above } \mathfrak{p} \text{ with } (\mathfrak{P}, L/K) \in C\},$$

*we define, respectively, the upper and lower density of $S_C$ as*

$$d_{\sup}(L/K, C) = \limsup_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in S_C} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}} \text{ and } d_{\inf}(L/K, C) = \liminf_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in S_C} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}},$$

*and in the case those values are equal we let*

$$d(L/K, C) := \lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in S_C} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}}$$

*denote the density of $S_C$.*

Now we state Chebotarev's Density Theorem.

**Theorem 5.4** (Chebotarev)**.** *Let $L/K$ be Galois extension of number fields with group $G$, and let $C$ be a conjugacy class of $G$. Then the density $d(L/K, C)$ exists and equals $\#C/\#G$.*

If $\sigma$ is an element of $C \subset G := \mathrm{Gal}(L/K)$, then $L$ is an abelian extension of the field of invariants $Z := \{x \in L : \sigma x = x\}$ with group $\mathrm{Gal}(L/Z) = \langle \sigma \rangle$. The following counting argument due to Deuring [13] shows we can reduce Chebotarev's Density Theorem to the case of an abelian extension.

**Lemma 5.5** (Deuring)**.** *If $d(L/Z, \{\sigma\}) = 1/[L : Z]$, then $d(L/K, C) = \#C/\#G$.*

*Proof.* Let $S_{L,\sigma}$ be the set of primes $\mathfrak{P}$ of $L$ (unramified over $K$) with $(\mathfrak{P}, L/K) = \sigma$. Next, denote by $S$ the set of primes $\mathfrak{p}$ of $K$ for which there is a $\mathfrak{P} \in S_{L,\sigma}$ dividing it (i.e. the set whose density we want to know).
Finally, let $S_Z$ be the set of primes $\mathfrak{q}$ of $Z$ for which there is a $\mathfrak{P} \mid \mathfrak{q}$ of $L$ with $(\mathfrak{P}, L/Z) = \sigma$ and $\deg_K(\mathfrak{q}) = 1$.
We claim

$$\lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in S} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\sum_{\mathfrak{q} \in S_Z} \frac{1}{\mathbf{N}\mathfrak{q}^s}} = \frac{\#C[L : Z]}{\#G}. \tag{5.2}$$

To see this, note that above every $\mathfrak{q} \in S_Z$ there lies exactly one $\mathfrak{P} \in S_{L,\sigma}$: the Galois group $\langle \sigma \rangle$ acts transitively on the primes above $\mathfrak{q}$, but also $\sigma(\mathfrak{P}) = \mathfrak{P}$ for such $\mathfrak{q}$. Conversely, if $\mathfrak{P} \in S_{L,\sigma}$ it divides some non-zero prime $\mathfrak{q}$ of $Z$, and as the Frobenius element

$\sigma$ of $\mathfrak{P}$ is the identity on $Z$, it follows that $\deg_Z(\mathfrak{P}) = \#\langle\sigma\rangle = \deg_K(\mathfrak{P})$, which implies $\deg_K(\mathfrak{q}) = 1$, and hence $\mathfrak{q} \in S_Z$. This gives a bijection between $S_Z$ and $S_{L,\sigma}$.
For a fixed $\mathfrak{p} \in S$ the number of $\mathfrak{P}$ above $\mathfrak{p}$ such that $\sigma = (\mathfrak{P}, L/K)$ equals $\#C_\sigma/\#G_\mathfrak{P}$, where $C_\sigma$ is the subgroup of $G$ of elements commuting with $\sigma$ and $G_\mathfrak{P}$ is the decomposition group of $\mathfrak{P}$. As $\#C_\sigma = \#G/\#C$ and $\#G_\mathfrak{P} = \#\langle\sigma\rangle = [L : Z]$, this number is equal to

$$\frac{\#G}{\#C[L : Z]}.$$

For every $\mathfrak{P} \mid \mathfrak{p}$ with $\sigma = (\mathfrak{P}, L/K)$ there is a unique $\mathfrak{q} \in S_Z$ with $\mathfrak{P} \mid \mathfrak{q} \mid \mathfrak{p}$, moreover $\mathbf{N}\mathfrak{p} = \mathbf{N}\mathfrak{q}$. Hence it follows from the observations above that for any $s > 1$

$$\frac{\#G}{\#C[L : Z]} \sum_{\mathfrak{p} \in S} \frac{1}{\mathbf{N}\mathfrak{p}^s} = \sum_{\mathfrak{q} \in S_Z} \frac{1}{\mathbf{N}\mathfrak{q}^s},$$

and thus 5.2 is true.
Now, because only primes of $Z$ of degree 1 over $K$ contribute to the poles (as in fact only those of absolute degree 1 contribute to the poles), we see

$$\frac{1}{[L : Z]} = d(L/Z, \{\sigma\}) = \lim_{s \downarrow 1} \frac{\displaystyle\sum_{\mathfrak{q} \in S_Z} \frac{1}{\mathbf{N}\mathfrak{q}^s}}{\log \dfrac{1}{s-1}}.$$

This concludes the proof, as

$$d(L/K, C) = \lim_{s \downarrow 1} \frac{\displaystyle\sum_{\mathfrak{p} \in S} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \dfrac{1}{s-1}} = \lim_{s \downarrow 1} \frac{\displaystyle\sum_{\mathfrak{p} \in S} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\displaystyle\sum_{\mathfrak{q} \in S_Z} \frac{1}{\mathbf{N}\mathfrak{q}^s}} \cdot \frac{\displaystyle\sum_{\mathfrak{q} \in S_Z} \frac{1}{\mathbf{N}\mathfrak{q}^s}}{\log \dfrac{1}{s-1}} = \frac{\#C}{\#G}.$$

■

While the original proof by Chebotarev did not, most modern proofs of his density theorem rely on class field theory. Stevenhagen and Lenstra, however, discuss a proof that does not [14]. It is this proof that is presented below.

**Theorem 5.4** (Chebotarev)**.** *Let $L/K$ be Galois extension of number fields with group $G$, and let $C$ be a conjugacy class of $G$. Then the density $d(L/K, C)$ exists and equals $\#C/\#G$.*

*Proof.* Assume $L \neq K$, otherwise we are done. By the preceding lemma we can also assume $L/K$ is abelian. So $C = \{\sigma\}$ for some $\sigma \in G$.
For a rational prime $p$, let $\zeta_p$ be some $p$'th root of unity. Choose an $M$ such that for all $p > M$ we have $L \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$.
Let $p > M$ and denote the Galois group of $K(\zeta_p)/K$ by $H \cong (\mathbb{Z}/p\mathbb{Z})^*$. Then the Galois

group of $L(\zeta_p)/K$ can be identified with $G \times H$.
Now, if a prime $\mathfrak{p}$ of $K$ has a prime $\mathfrak{P}$ of $L(\zeta_p)$ above it with Frobenius element $(\sigma, \tau) \in G \times H$, then $\mathfrak{P} \cap L$ has Frobenius element $\sigma \in G$. Hence

$$d_{\inf}(L/K, \{\sigma\}) \geq \sum_{\tau \in H} d_{\inf}(L(\zeta_p)/K, \{(\sigma, \tau)\}).$$

Write $n := [L : K]$ and fix $(\sigma, \tau) \in G \times H$. When $n$ divides the order of $\tau$, the subgroups $\langle(\sigma, \tau)\rangle$ and $G \times \{1\}$ of $G \times H$ intersect trivially. It follows that the field of invariants $F = \{x \in L(\zeta_p) : (\sigma, \tau)(x) = x\}$ satisfies $F(\zeta_p) = L(\zeta_p)$, such that $L(\zeta_p)/F$ is cyclotomic. Still supposing $n$ divides the order of $\tau$, by Theorem 5.2 we have

$$d(L(\zeta_p)/F, \{(\sigma, \tau)\}) = \frac{1}{[L(\zeta_p) : F]},$$

and thus by Lemma 5.5

$$d(L(\zeta_p)/K, \{(\sigma, \tau)\}) = \frac{1}{[L(\zeta_p) : F][F : K]} = \frac{1}{\#G\#H}.$$

Writing $H_n$ for the set of $\tau \in H$ whose order is divisible by $n$, the above considerations yield

$$d_{\inf}(L/K, \{\sigma\}) \geq \frac{\#H_n}{\#G\#H}.$$

Suppose $k > 0$ and $p = 1 \bmod n^k$. Then $H \cong \mathbb{Z}/n^k r\,\mathbb{Z}$ for some $r \in \mathbb{Z}_{>0}$. Suppose $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$ with the $p_i$ distinct prime numbers and $e_i > 0$. Then, if we consider for each $i$ the map

$$\varphi_i : H \to H : h \mapsto \frac{n^k r}{p_i^{(k-1)e_i}} \cdot h$$

of multiplication by $n^k r p_i^{(1-k)e_i}$, we see that $\#\ker\varphi_i = n^k r p_i^{(1-k)e_i}$ and that every element of $H$ whose order is not divisible by $p_i^{e_i}$ lies in $\ker\varphi_i$. It follows that

$$\frac{\#H_n}{\#H} \geq \frac{n^k r - \sum_i \#\ker\varphi_i}{n^k r} = \frac{n^k r - \sum_i n^k r p_i^{(1-k)e_i}}{n^k r} = 1 - \sum_i \frac{1}{p_i^{(k-1)e_i}},$$

which comes arbitrarily close to 1 for large $k$. Dirichlet's Theorem on Arithmetic Progressions tells us there are (infinitely many) primes $p > M$ satisfying the congruence $p = 1 \bmod n^k$, for every $k$.
So we obtain

$$d_{\inf}(L/K, \{\sigma\}) \geq 1/\#G.$$

This is true for every $\sigma \in G$. We claim that $d_{\sup}(L/K, \{\sigma\}) \leq 1/\#G$ for every $\sigma$: for suppose this is not true for, say, $\sigma_1 \in G$, then

$$1 = \limsup_{s \downarrow 1} \frac{\displaystyle\sum_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \dfrac{1}{s-1}} \geq d_{\sup}(L/K, \{\sigma_1\}) + \sum_{\sigma \in G \setminus \{\sigma_1\}} d_{\inf}(L/K, \{\sigma\}) > 1,$$

which is a contradiction.
So the upper and lower densities $d_{\sup}$ and $d_{\inf}$ coincide and hence the Dirichlet densities exist for all $\sigma \in G$ and equal

$$d(L/K, \{\sigma\}) = 1/\#G.$$

■

# 6 Chebotarev's Density Theorem for infinite Galois extensions

Let $K$ be a number field and $L/K$ a Galois extension of $K$ with group $G$. Even if the extension $L/K$ is infinite we still turn out to have a notion of Frobenius elements in $G$, as we will see in Section 6.2. This allows us to formulate an analogon of Chebotarev's Density Theorem.
However, suppose that $G$ is infinite and $X \subset G$ is closed under conjugation, then the density of the primes $\mathfrak{p} \subset \mathcal{O}_K$ above which there is a prime in $\mathcal{O}_L$ with Frobenius element in $X$ cannot possibly be $\#X/\#G$ – as in the finite case of Chebotarev's Density Theorem – as this expression has no meaning, because $G$ (and possibly $X$) is infinite.
So in order to formulate Chebotarev's Density Theorem in the infinite setting we need something else. Here the Haar measure comes into play: we wil be able to construct a measure $h$ on the Galois group $G$ with $h(G) = 1$, called the Haar measure. When we have this measure, we wil see that the density of the primes in $\mathcal{O}_K$ above which there is a prime with Frobenius in $X$ is equal to $h(X)$.
The following section deals with the construction of the Haar measure.

## 6.1 The Haar measure

We start by introducing some measure theoretic definitions which will allow us to state the rather technical result from Carathéodory about when certain maps (pre-measures) can be extended to measures.

**Definition** (Semi-ring on a set)**.** *Let $X$ be a set. Then $S \subset \mathcal{P}(X)$ is said to be a semi-ring on $X$ if $S$ contains the empty set, is closed under intersection, and if it holds that if $S, T \in \mathcal{S}$, then there are finitely many disjoint $S_1, \ldots, S_n \in \mathcal{S}$ such that $S \setminus T = \bigcup_i S_i$.*

**Definition** (Pre-measure on a semi-ring)**.** *Let $X$ be a set and $S$ a semi-ring on $X$. Then $\mu : \mathcal{S} \to [0, \infty)$ is called a pre-measure (on $S$) if $\mu(\emptyset) = 0$ and*

$$\mu\Big(\bigcup_{i \in \mathbb{N}} S_i\Big) = \sum_{i \in \mathbb{N}} \mu(S_i),$$

*whenever $S_1, S_2, \ldots$ is a countable sequence of disjoint sets in $\mathcal{S}$ whose union is also in $\mathcal{S}$.*

Carathéodory's Extension Theorem shows that any pre-measure on a semi-ring $S$ on some set $X$ can be extended to a measure on the $\sigma$-algebra generated by $S$ (i.e. the smallest $\sigma$-algebra containing $S$).

**Theorem 6.1** (Carathéodory's Extension Theorem)**.** *Let $X$ be a set and $S$ a semi-ring on $X$. If $\mu : S \to [0, \infty)$ is a pre-measure, then $\mu$ can be extended to a measure on the $\sigma$-algebra generated by $\mathcal{S}$. This extension is unique if $\mu$ is defined on $X$ and $\mu(X) < \infty$.*

*Proof.* See [15, thm. 6.1]. ■

In a profinite group $G$ there is a fundamental system of neighbourhoods of the identity consisting of open subgroups $G_i$ of finite index in $G$, we will call such a system of $G_i$ *a fundamental system of* $G$. Because a profinite group is a topological group, the set of all $a + G_i$ with $a \in G$ forms a basis for the topology on $G$. Carathéodory's theorem allows us to construct a Haar measure on profinite groups that have a fundamental system that is *countable*.

**Theorem 6.2.** *Let $G$ be a profinite group with countable fundamental system $\{G_i\}_{i\in I}$, indexed by a directed poset $I$. Then the map*

$$h : \mathcal{T}(G) \to [0, 1] : U \mapsto \sup_{i\in I} \sum_{aG_i \subset U} \frac{1}{[G : G_i]},$$

*where $\mathcal{T}(G)$ is the set of opens of $G$, can be uniquely extended to a left-translation invariant measure on the Borel $\sigma$-algebra of $G$ (i.e. the $\sigma$-algebra generated by the open sets).*

*Proof.* Consider the set

$$\mathcal{S} = \{\bigcup_{j=1}^{n} a_j G_i \ : a_1, \ldots, a_n \in G, i \in I\} \cup \{\emptyset\}$$

of finite unions of left-cosets of subgroups in $\{G_i\}_{i\in I}$, containing in addition the empty set. Note that the elements of $\mathcal{S}$ are compact and open, and that they form a basis for the topology of $G$.
Define $\widetilde{h} : \mathcal{S} \to [0, 1]$ by

$$\widetilde{h} : \bigsqcup_{j=1}^{n} a_j G_i \mapsto \frac{n}{[G : G_i]} \text{ and } \emptyset \mapsto 0.$$

This is well-defined: if $A = \bigsqcup_{j=1}^{n} a_j G_i = \bigsqcup_{k=1}^{m} b_k G_\ell$ we can suppose without loss of generality that $G_\ell \subset G_j$ (because the system is directed), and we find

$$\frac{n}{[G : G_i]} = \sum_{aG_i \subset A} \frac{1}{[G : G_i]} = \sum_{aG_i \subset A} \sum_{bG_\ell \subset aG_i} \frac{1}{[G : G_\ell]} = \frac{m}{[G : G_\ell]}.$$

This shows $\widetilde{h}$ is well-defined. One can show in a similar way that $\widetilde{h}(A \sqcup B) = \widetilde{h}(A) + \widetilde{h}(B)$, which means $\widetilde{h}$ respects finite disjoint unions.
Suppose that $\bigsqcup_{i\in\mathbb{N}} A_i \in \mathcal{S}$ for certain $A_1, A_2, \cdots \in \mathcal{S}$ is non-empty, then by compactness only finitely many of the $A_i$ are non-empty. Thus it follows that $\widetilde{h}(\bigsqcup_{i\in\mathbb{N}} A_i) =$

$\sum_{i\in\mathbb{N}} \widetilde{h}(A_i)$, as it is in fact a finite union. By Theorem 6.1 the map $\widetilde{h}$ can be uniquely extended to a measure $h$ on the $\sigma$-algebra generated by $\mathcal{S}$. As $I$ is countable, it follows that every open subset $G$ is a countable union of elements of $\mathcal{S}$, hence the $\sigma$-algebra generated by $\mathcal{S}$ is in fact the Borel $\sigma$-algebra of $G$.
From the definition of $\widetilde{h}$ it follows immediately that $\widetilde{h}$ is left-translation invariant. The uniqueness of the extension $h$ then implies that the two measures $h(-)$ and $h(g\cdot -)$ are actually the same, for any $g \in G$. This shows $h$ is left-translation invariant.
It remains to prove $h$ is given by

$$U \mapsto \sup_{i\in I} \sum_{aG_i\subset U} \frac{1}{[G:G_i]}$$

on the opens $U$ of $G$.
The fact that $h$ is a measure implies $h(U) \geq \sup_{i\in I} \sum_{aG_i\subset U} \frac{1}{[G:G_i]}$. Now, because $I$ is countable we can find a chain $C \subset I$ that is order isomorphic to (a subset of) $\mathbb{N}$ such that for all $i \in I$ there is a $c \in C$ with $i \leq c$ (this property is called cofinality). Viewing $C$ as a suborder of $\mathbb{N}$ we can define for each $n \in \mathbb{N}$ the measurable sets

$$A_0 = \emptyset \text{ and } A_{n+1} = \begin{cases} \Big( \bigcup\limits_{aG_n\subset U} aG_n \Big) \setminus A_n, & \text{if } n \in C, \\ A_n, & \text{otherwise.} \end{cases}$$

Then

$$h(U) = h(\bigsqcup_{i\in\mathbb{N}} A_i) = \sum_{i\in\mathbb{N}} h(A_i) = \sup_{n\in C} \sum_{i=1}^{n+1} h(A_i) = \sup_{n\in C} h\Big( \bigcup_{aG_n\subset U} aG_n \Big) \leq \sup_{i\in I} \sum_{aG_i\subset U} \frac{1}{[G:G_i]}.$$

■

**Corollary 6.3.** *Let $K$ be a number field and suppose $L/K$ is a Galois extension with profinite group $G$. Then there exists a unique left-translation invariant measure $h$ satisfying*

$$h : \mathcal{T}(G) \to [0,1] : U \mapsto \sup_N \sum_{aN\subset U} \frac{1}{[G:N]},$$

*where $\mathcal{T}(G)$ is the set of opens of $G$ and the supremum is taken over the closed normal subgroups $N$ of finite index (i.e. those corresponding to finite subextensions $E/K$ of $L/K$).*

*Proof.* The Galois group $G$ is the projective limit of the Galois groups of finite Galois subextensions $F/K$ [16, thm. 2.2]. There are countably many polynomials in $K[X]$, so there are at most countably many finite Galois subextensions $F/K$.
This means $G$ is a profinite group with a countable fundamental system. The statement then follows from Theorem 6.2. ■

## 6.2 The infinite case of Chebotarev's Density Theorem

Let $K$ be a number field and let $L/K$ be Galois with profinite group $G$. Suppose $L_1 \subset L_2 \subset \dots$ is an ascending chain of subextensions of $L/K$ that are finite and Galois over $K$ with $L = \bigcup_i L_i$.
We call the integral closure of $\mathbb{Z}$ in $L$ the *ring of integers of* $L$ and denote it by $\mathcal{O}_L$. Note that in the case $L/K$ is infinite $\mathcal{O}_L$ might not have unique factorization into prime ideals: for example, if $L$ is the normal closure of $\mathbb{Q}(\sqrt[n]{2}\colon n \in \mathbb{Z}_{>0})$ we have $\mathfrak{t}^2 = \mathfrak{t}$ for the non-zero $\mathcal{O}_L$-ideal $\mathfrak{t} = (\sqrt[n]{2}\colon n \in \mathbb{Z}_{>0})$ generated by all roots of 2.
Let $\mathfrak{P}$ be a non-zero prime ideal of the ring of integers $\mathcal{O}_L$ of $L$. Then one can verify that $\mathfrak{P}$ is a maximal ideal, and writing $\mathfrak{p} = K \cap \mathfrak{P}$ and $\mathfrak{p}_i = L_i \cap \mathfrak{P}$ we obtain an ascending chain of prime ideals that lie in $\mathcal{O}_K$ and $\mathcal{O}_{L_i}$, respectively.
We will say that $\mathfrak{p}$ *does not ramify in* $L$ if $\mathfrak{p}$ does not ramify in any $L_i$ – note that this definition does not depend on the choice of $L_i$. Equivalently, $\mathfrak{p}$ does not ramify in $L$ if and only if the only nilpotent element of $\mathcal{O}_L/\mathfrak{P}$ is 0.
Suppose $\mathfrak{p}$ does not ramify in $L$. For each $i$ we will then get embeddings

$$\mathrm{Gal}\left((\mathcal{O}_{L_i}/\mathfrak{p}_i)/(\mathcal{O}_K/\mathfrak{p})\right) \hookrightarrow \mathrm{Gal}(L_i/K)$$

sending the Frobenius automorphism $\overline{x} \mapsto \overline{x}^{\mathbf{N}\mathfrak{p}}$ to the Frobenius element $(\mathfrak{p}_i, L_i/K)$. We have commutative diagrams

$$\begin{array}{ccc} \mathrm{Gal}\left((\mathcal{O}_{L_{i+1}}/\mathfrak{p}_{i+1})/(\mathcal{O}_K/\mathfrak{p})\right) & \longhookrightarrow & \mathrm{Gal}(L_{i+1}/K) \\ \downarrow & & \downarrow \\ \mathrm{Gal}\left((\mathcal{O}_{L_i}/\mathfrak{p}_i)/(\mathcal{O}_K/\mathfrak{p})\right) & \longhookrightarrow & \mathrm{Gal}(L_i/K) \end{array}$$

for each $i \in \mathbb{N}$, where the downward arrows are the quotient maps. This induces an embedding [17, prop. 10.2]

$$\mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right) \cong \varprojlim_i \mathrm{Gal}\left((\mathcal{O}_{L_i}/\mathfrak{p}_i)/(\mathcal{O}_K/\mathfrak{p})\right) \hookrightarrow \varprojlim_i \mathrm{Gal}(L_i/K) \cong G.$$

(Note that the hence defined embedding $\mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right) \hookrightarrow G$ is independent of the choice of the $L_i$.) Thus we can define *the Frobenius element* $(\mathfrak{P}, L/K)$ *of* $\mathfrak{P}$ as the image of $\overline{x} \mapsto \overline{x}^{\mathbf{N}\mathfrak{p}}$ in $\mathrm{Gal}(L/K)$ through the embedding $\mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right) \hookrightarrow G$ described above. Note that this definition of the Frobenius element agrees with the definition we earlier gave in the case $L/K$ is finite.
We could have defined the Frobenius element $(\mathfrak{P}, L/K)$ in a similar way as when we defined them in the case of an extension of number fields. Namely, the fact that $G$ acts transitively on the primes in $\mathcal{O}_{L_i}$ above $\mathfrak{p}$, means $G$ also acts transitively on the primes in $\mathcal{O}_L$ above $\mathfrak{p}$. Moreover, we can again define the decomposition group $G_{\mathfrak{P}}$ as the stabilizer of $\mathfrak{P}$ to find out $G_{\mathfrak{P}} \cong \mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right)$ (since we assumed that $\mathfrak{p}$ does not ramify in $L$). Then the Frobenius element would be the element in $G_{\mathfrak{P}}$ corresponding to the Frobenius automorphism in $\mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right)$. We leave it to the reader to verify

that this definition of the Frobenius element is equivalent to the one we gave.
Given a subset $X \subset G$ that is closed under conjugation, we can again define, respectively, the upper and lower densities

$$d_{\sup}(L/K, X) = \limsup_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in S_X} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}} \text{ and } d_{\inf}(L/K, X) = \liminf_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in S_X} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}},$$

where

$$S_X = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ is unramified in } L \text{ and } \exists \mathfrak{P} \subset \mathcal{O}_L \text{ above } \mathfrak{p} \text{ with } (\mathfrak{P}, L/K) \in X\}.$$

If the upper and lower densities are equal, we denote their value by $d(L/K, C)$.
Now we are ready to formulate the version of Chebotarev's Density Theorem that also covers the infinite case (cf. [18, I-8, cor. 2]). The theorem requires one additional condition on $L/K$ to those considered above: the primes of the base field $K$ that ramify in $L$ should have density 0.

**Theorem 6.4** (Chebotarev's Density Theorem for infinite extensions)**.** *Let $K$ be a number field. Suppose $L/K$ is Galois with group $G$ and let $X \subset G$ be closed under conjugation. Suppose the set of primes $\mathfrak{p}$ of $K$ that ramify in $L$ has a density, equal to 0. If $h$ is the Haar measure as obtained in Corollary 6.3, then*

$$h\big(\overline{X}\big) \geq d_{\sup}(L/K, X) \geq d_{\inf}(L/K, X) \geq h(X^\circ),$$

*where $\overline{X}$ denotes the closure and $X^\circ$ the interior of $X$. In particular, if the boundary $\partial X$ of $X$ has measure 0, then $S_X$ has a density, equal to $d(L/K, X) = h(X)$.*

*Proof.* Let $L_i \subset L$ for $i \in \mathbb{N}$ be finite Galois over $K$ as in the discussion above. Define, for each $i$, $X_i^+ \subset \mathrm{Gal}(L_i/K)$ as the image of $X$ through the quotient map

$$\mathrm{Gal}(L/K) \twoheadrightarrow G/\mathrm{Gal}(L/L_i) \cong \mathrm{Gal}(L_i/K).$$

(The inclusion $\mathrm{Gal}(L/L_i) \subset G$ and the isomorphism $G/\mathrm{Gal}(L/L_i) \cong \mathrm{Gal}(L_i/K)$ follow from the Main Theorem of Galois Theory, which also holds in the infinite case [16, thm. 2.3].)
For each $i$ define the set of primes of $\mathcal{O}_K$

$$S_i^+ = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ is unramified in } L_i \text{ and } \exists \mathfrak{p}_i \subset \mathcal{O}_{L_i} \text{ with } \mathfrak{p}_i \mid \mathfrak{p} \text{ and } (\mathfrak{p}_i, L_i/K) \in X_i^+\}.$$

Note that $S_i^+ \supset S_{i+1}^+ \supset S_X$ for all $i$. So for all $i$ and all $s \in (1, 2)$ we have

$$\frac{\sum_{\mathfrak{p} \in S_i^+} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}} \geq \frac{\sum_{\mathfrak{p} \in S_X} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\log \frac{1}{s-1}}.$$

Taking the limit $s \to 1$ first and then letting $i \to \infty$ we see

$$\liminf_{i\to\infty} d(L_i/K, X_i^+) \geq d_{\sup}(L/K, X).$$

By Chebotarev's Density Theorem and the way $h$ behaves on opens we have

$$\liminf_{i\to\infty} d(L_i/K, X_i^+) = \liminf_{i\to\infty} \frac{\#X_i^+}{[L_i:K]} = 1 - \limsup_{i\to\infty} \frac{[L_i:K] - \#X_i^+}{[L_i:K]} = 1 - h\big((G\setminus X)^\circ\big),$$

which is equal to $h\big(\overline{X}\big)$. So $h\big(\overline{X}\big) \geq d_{\sup}(L/K, X)$.
In order to bound the lower density from below, define, for each $i$, $X_i^- \subset \mathrm{Gal}(L_i/K)$ as the image of

$$\bigcup_{\substack{\sigma\in G:\\ \sigma\,\mathrm{Gal}(L/L_i)\subset X}} \sigma\,\mathrm{Gal}(L/L_i)$$

through the quotient map $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(L_i/K)$.
Now define

$$S_i^- = \{\mathfrak{p} \subset \mathcal{O}_K \colon \mathfrak{p} \text{ is unramified in } L_i \text{ and } \exists \mathfrak{p}_i \subset \mathcal{O}_{L_i} \text{ with } \mathfrak{p}_i \mid \mathfrak{p} \text{ and } (\mathfrak{p}_i, L_i/K) \in X_i^-\}$$

and note that

$$\frac{\displaystyle\sum_{\mathfrak{p}\in S_X} \frac{1}{\mathbf{N}\mathfrak{p}^s} + \sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ \text{ramified in } L}} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\displaystyle\log\frac{1}{s-1}} \geq \frac{\displaystyle\sum_{\mathfrak{p}\in S_i^-} \frac{1}{\mathbf{N}\mathfrak{p}^s}}{\displaystyle\log\frac{1}{s-1}}$$

for all $i$ and $s \in (1,2)$. Because the primes that ramify in $L$ have density 0, when taking the limit of $s$ to 1 we see

$$d_{\inf}(L/K, X) \geq d(L_i/K, S_i^-) = \frac{\#X_i^-}{[L_i:K]}.$$

Taking the limit $i \to \infty$ it follows from Chebotarev's Density Theorem and properties of $h$ that

$$d_{\inf}(L/K, X) \geq \limsup_{i\to\infty} \frac{\#X_i^-}{[L_i:K]} = h(X^\circ).$$

We see

$$h\big(\overline{X}\big) \geq d_{\sup}(L/K, X) \geq d_{\inf}(L/K, X) \geq h(X^\circ).$$

If $h(\overline{X}) - h(X^\circ) = h(\partial X) = 0$, we see $d(L/K, X)$ is defined and equals $h(X)$. ■

**Corollary 6.5.** *Let $K$ be a number field and suppose $L/K$ is Galois with group $G$. Suppose the set of primes $\mathfrak{p}$ of $K$ that ramify in $L$ has a density, equal to 0. Then the set of elements in $G$ that are Frobenius elements of some prime $\mathfrak{P} \subset \mathcal{O}_L$ lies dense in $G$.*

# 7 Some applications

In the previous chapter we have seen that the finite Chebotarev's Density Theorem can be used to prove an infinite version. Here we will present some elementary applications of the finite version. The first application was mentioned in the introductory chapter. We start with a lemma.

**Lemma 7.1.** *Let $L = K(\alpha_1, \ldots, \alpha_n)/K$ be an extension of number fields with $\alpha_1, \ldots, \alpha_n$ integral over $\mathcal{O}_K$. Then for all but finitely many primes $\mathfrak{P} \subset \mathcal{O}_L$ one has that the natural map*

$$\psi : \mathcal{O}_K[\alpha_1, \ldots, \alpha_n]/\big(\mathfrak{P} \cap \mathcal{O}_K[\alpha_1, \ldots, \alpha_n]\big) \to \mathcal{O}_L/\mathfrak{P}$$

*is an isomorphism.*

*Proof.* The ring $\mathcal{O}_K[\alpha_1, \ldots, \alpha_n]$, being a free abelian group of the same rank as $\mathcal{O}_L$, has finite index in $\mathcal{O}_L$. If $\psi$ is not surjective, its image has non-trivial index in $\mathcal{O}_L/\mathfrak{P}$ and this index must divide $[\mathcal{O}_L : \mathcal{O}_K[\alpha_1, \ldots, \alpha_n]]$. At the same time, the index of the image should be divisible by $\mathfrak{P}$ in that case, because $\mathfrak{P} \mid [\mathcal{O}_L/\mathfrak{P} : \operatorname{Im}\psi]$.
This shows it is only possible for the map not to be an isomorphism in the case

$$\mathfrak{P} \mid [\mathcal{O}_L : \mathcal{O}_K[\alpha_1, \ldots, \alpha_n]].$$

■

## 7.1 On the density of rational primes $p$ for which $a$ is an $n$'th power mod $p$

In Chapter 4 we saw that Dirichlet's Theorem on Arithmetic Progressions is a special case of Chebotarev's Density Theorem. Given an integer $a \in \mathbb{Z}$ we can ask for the density of prime numbers $p \in \mathbb{Z}$ with the property that $a = \square \bmod p$. Using the law of quadratic reciprocity one sees that $a$ being a square mod $p$ happens if and only if $p$ satisfies certain congruences mod $4|a|$. One can then use Dirichlet's theorem to compute the density of the primes $p$ for which $a = \square \bmod p$.
Chebotarev's Density Theorem allows us to do this for arbitrary $n$'th powers, instead of merely for $n = 2$. In order to do this, one needs to compute the Galois group of $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)/\mathbb{Q}$. With a few conditions on $a$ we know what this group looks like.

**Theorem 7.2.** *Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$ and suppose $a$ is not a $d$'th power in $\mathbb{Z}$ for all $d \mid n$ with $d \neq 1$. Suppose as well that $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\sqrt[n]{a}) = \mathbb{Q}$, where $\zeta_n$ is a primitive $n$'th root of unity. Then the set of rational primes $p$ for which $a$ is an $n$'th power* $\bmod p$ *has a density that is equal to*

$$\frac{1}{\varphi(n)} \sum_{u \in (\mathbb{Z}/n\mathbb{Z})^*} \frac{1}{\gcd(u-1, n)}.$$

*In particular, when $n$ is a prime number, this density is* $\dfrac{n-1}{n}$.

*Proof.* We begin by computing the Galois group $G$ of $\mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q}$. By our assumptions $X^n - a$ is irreducible in $\mathbb{Q}(\zeta_n)[X]$. Hence $G$ has order $n\varphi(n)$.
Every $\sigma \in G$ is determined by where it sends $\zeta_n$ and $\sqrt[n]{a}$ to. So it is not ambiguous to write $\sigma_{b,c}$ for the element of $G$ that sends $\zeta_n$ to $\zeta_n^b$ and $\sqrt[n]{a}$ to $\zeta_n^c \sqrt[n]{a}$. Because for any $\sigma_{b,c} \in G$ we must have $b \in (\mathbb{Z}/n\mathbb{Z})^*$ and $c \in \mathbb{Z}/n\mathbb{Z}$ it follows from $\#G = n\varphi(n)$ that we have a bijective map to the affine group over $\mathbb{Z}/n\mathbb{Z}$

$$\psi : G \to \mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) = \left\{ \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} : u \in (\mathbb{Z}/n\mathbb{Z})^*, t \in \mathbb{Z}/n\mathbb{Z} \right\} : \sigma_{b,c} \mapsto \begin{pmatrix} b & c \\ 0 & 1 \end{pmatrix}.$$

Note that $\sigma_{u,t}\sigma_{b,c}(\zeta_n) = \zeta_n^{ub}$ and $\sigma_{u,t}\sigma_{b,c}(\sqrt[n]{a}) = \zeta_n^{uc+t}\sqrt[n]{a}$, so $\sigma_{u,t}\sigma_{b,c} = \sigma_{ub,uc+t}$, from which it follows that $\psi$ is an isomorphism of groups. Hence we can identify $G$ and $\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z})$.
By Lemma 7.1 for all but finitely many prime numbers $p$ we have that the residue class field extensions $(\mathcal{O}_{\mathbb{Q}(\zeta_n, \sqrt[n]{a})}/\mathfrak{p})/\mathbb{F}_p$, for primes $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(\zeta_n, \sqrt[n]{a})}$ above $p$, are the same as the extension $Z[\zeta_n, \sqrt[n]{a}]/\big(\mathfrak{p} \cap \mathbb{Z}[\zeta_n, \sqrt[n]{a}]\big)$ of $\mathbb{F}_p$.
So assume this is true for $p$, then we have that $a$ is an $n$'th power mod $p$ if and only if there is some $k \in \mathbb{Z}$ such that the Frobenius automorphism fixes $\zeta_n^k \sqrt[n]{a} \in \mathbb{Z}[\zeta_n, \sqrt[n]{a}]/\big(\mathfrak{p} \cap \mathbb{Z}[\zeta_n, \sqrt[n]{a}]\big)$. If $\mathfrak{p}$ lies above $p$ and has Frobenius element

$$(\mathfrak{p}, \mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q}) = \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix},$$

then $\zeta_n^k \sqrt[n]{a} \in \mathbb{F}_p(\zeta_n, \sqrt[n]{a})$ is fixed if

$$\zeta_n^k \sqrt[n]{a} = \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} \zeta_n^k \sqrt[n]{a} = \zeta_n^{uk+t} \sqrt[n]{a},$$

which happens precisely if $(u-1)k + t = 0 \bmod n$. In that case one has

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix},$$

and one has that the conjugacy class of $(\mathfrak{p}, \mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q})$, which is that of $\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$, equals

$$C_u := \left\{ \begin{pmatrix} 1 & -\ell \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix} : \ell \in \mathbb{Z}/n\mathbb{Z} \right\} = \left\{ \begin{pmatrix} u & (u-1)\ell \\ 0 & 1 \end{pmatrix} : \ell \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

So

$$\#C_u = \#(u-1)(\mathbb{Z}/n\mathbb{Z}) = \frac{n}{\gcd(n, u-1)}.$$

We conlude that for all but finitely many rational primes $p$ we have that $a$ is an $n$'th power mod $p$ if and only if the Frobenius elements of the primes above $p$ belong to a $C_u$ for some $u \in (\mathbb{Z}/n\mathbb{Z})^*$, and thus the density of those rational primes $p$ is equal to

$$\frac{1}{n\varphi(n)} \sum_{u \in (\mathbb{Z}/n\mathbb{Z})^*} \frac{n}{\gcd(n, u-1)} = \frac{1}{\varphi(n)} \sum_{u \in (\mathbb{Z}/n\mathbb{Z})^*} \frac{1}{\gcd(u-1, n)}.$$

In case $n$ is prime, this density is equal to

$$\begin{aligned} \frac{1}{n-1} \sum_{u \in (\mathbb{Z}/n\mathbb{Z})^*} \frac{1}{\gcd(u-1, n)} &= \frac{1}{n-1} \left( \frac{1}{\gcd(0, n)} + \sum_{u=2}^{n-1} \frac{1}{\gcd(u-1, n)} \right) \\ &= \frac{1}{n-1} \Big( \frac{1}{n} + n - 2 \Big) = \frac{n-1}{n}. \end{aligned}$$

■

## 7.2 What the splitting behaviour of primes says about the extension

Given an extension of number fields $L/K$ let $\mathrm{Spl}(L/K)$ denote the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ that split completely in $\mathcal{O}_L$.
The following theorem can be found in the *second* edition of Lang's *Algebraic Number Theory* as a corollary to Chebotarev's Density Theorem [19, p. 170].

**Theorem 7.3.** *Let $K$ be a number field and $f \in \mathcal{O}_K[X]$ an irreducible polynomial. If $f$ has roots in $\mathcal{O}_K/\mathfrak{p}$ for all primes $\mathfrak{p}$, except for those in a set of Dirichlet density 0, then $f$ has a root in $K$.*

*Proof.* Let $L$ be the splitting field of $f$ over $K$ and let $G$ be its Galois group. Let $\alpha \in L$ be a root of $f$ and let $H = \mathrm{Gal}(L/K(\alpha)) \subset G$. Conjugates $\sigma H \sigma^{-1}$ have invariant field $K(\sigma(\alpha))$, so by assumption almost every prime $\mathfrak{P} \subset \mathcal{O}_L$ has a Frobenius element in some conjugate of $H$ (only the primes $\mathfrak{P}$ above $\mathfrak{p} \subset \mathcal{O}_K$ for which $f$ has no roots mod $\mathfrak{p}$ and those for which $\mathfrak{p} \mid \Delta(f)$ are excluded – in the latter case $\alpha$ and some conjugate $\alpha' \neq \alpha$ of $\alpha$ might be the same mod $\mathfrak{P}$).
It follows that every element of $G$ lies in some conjugate of $H$. Hence $G = \bigcup_{\sigma \in G} \sigma H \sigma^{-1}$. If $f$ would have degree 1, $K(\alpha)$ would be a proper field extension of $K$, and hence $H$ would be a proper subgroup of $G$. However, the number of conjugates of $H$ is less than or equal to $[G : H]$ and each conjugate has $\#H$ elements, while in the union $G = \bigcup_{\sigma \in G} \sigma H \sigma^{-1}$ the identity element occurs in each conjugate, which yields the contradiction

$$\#G < [G : H]\#H = \#G.$$

This shows $f$ has degree 1 and a root in $K$. ■

We obtain the following corollary that could also have been proven by noting that the density of the primes of $K$ that split completely in a Galois extension of number fields $L/K$ is equal to $1/[L:K]$.

**Corollary 7.4.** *Let $L/K$ be a Galois extension of number fields and suppose all primes of $K$ split completely in $L$ except for a set of density 0. Then $L = K$.*

In Theorem 7.3 the assumption that $f$ is irreducible is crucial: for example, the polynomial $(X^2+1)(X^2+5)(X^2-5) \in \mathbb{Q}[X]$ has no roots in $\mathbb{Q}$, but it does have roots in $\mathbb{F}_p$ for every rational prime $p$.
Furthermore, it is not true that if $f$ is not irreducible modulo every prime $\mathfrak{p}$, that it is not irreducible in $K[X]$: for this we have the counter example $X^4+1 \in \mathbb{Q}[X]$, as it is clearly not irreducible in $\mathbb{F}_2[X]$ and for odd primes $p$ it has a root in $\mathbb{F}_{p^2}$, since then $8 \mid p^2-1$. (Alternatively, one can argue that since the Galois group of $X^4+1$ over $\mathbb{Q}$ does not have an element of order 4, there can be no Frobenius elements of order 4.)

**Theorem 7.5.** *Let $K$ be a number field and $L_1, L_2$ finite field extensions of $K$ that are contained in the same algebraic closure. If $\mathrm{Spl}(L_1/K)$ and $\mathrm{Spl}(L_2/K)$ differ by a set that has density 0, then $L_1$ and $L_2$ have the same normal closure over $K$.*

*Proof.* Let $\Omega_1$ and $\Omega_2$ be the normal closures of $L_1$ and $L_2$ in $\overline{K}$, respectively. For $i \in \{1,2\}$ we have $\mathrm{Spl}(\Omega_i/K) \subset \mathrm{Spl}(\Omega_i/K)$ and for all but finitely many $\mathfrak{p} \in \mathrm{Spl}(L_i/K)$ we have $\mathfrak{p} \in \mathrm{Spl}(\Omega_i/K)$:[1] let $f \in \mathcal{O}_K[X]$ be the minimal polynomial over $K$ of some integral primitive element for $L_i/K$ and let $\alpha_1, \ldots, \alpha_n$ be its roots. If $\mathfrak{p} \in \mathrm{Spl}(L_i/K)$ and $\mathfrak{P} \subset \mathcal{O}_{\Omega_i}$ is a prime above $\mathfrak{p}$, then we have

$$\big[\mathcal{O}_K[\alpha_1, \cdots, \alpha_n]/\big(\mathfrak{P} \cap \mathcal{O}_K[\alpha_1, \cdots, \alpha_n]\big) : \mathcal{O}_K/\mathfrak{p}\big] = 1.$$

So by Lemma 7.1, as $\Omega_i = K(\alpha_1, \ldots, \alpha_n)$, it indeed follows that all but finitely many $\mathfrak{p} \in \mathrm{Spl}(L_i/K)$ are elements of $\mathrm{Spl}(\Omega_i/K)$.
Hence $\mathrm{Spl}(\Omega_1/K)$ and $\mathrm{Spl}(\Omega_2)$ also differ by a set that has Dirichlet density 0. Thus almost all primes $\mathfrak{p} \in \mathrm{Spl}(\Omega_1/K)$ split completely in the compositum $\Omega_1\Omega_2$, because, by Lemma 7.1, for all but finitely many $\mathfrak{p} \in \mathrm{Spl}\,\Omega_1/K)$ we have that $\mathfrak{p}$ splits completely in $\Omega_1\Omega_2$ if some minimal polynomial $f \in \mathcal{O}_K[X]$ of an (integral) primitive element for $\Omega_2/K$ splits into linear factors modulo $\mathfrak{p}$, and the latter is true for almost all $\mathfrak{p} \in \mathrm{Spl}\,\Omega_1/K)$.
In particular the primes $\mathfrak{P} \subset \mathcal{O}_{\Omega_1}$ of absolute degree 1 (almost all primes of $\mathcal{O}_{\Omega_1}$ have this property!) lie above primes in $\mathrm{Spl}(\Omega_1/K)$, so almost all of them split completely in $\Omega_1\Omega_2$. Hence it follows by Corollary 7.4 that $\Omega_1 = \Omega_1\Omega_2$.
Similarly, we find $\Omega_2 = \Omega_1\Omega_2$. ∎

[1] In fact one has $\mathrm{Spl}(\Omega_i/K) = \mathrm{Spl}(L_i/K)$, see [4, ch. 4, §9, ex. 4].

# 8 Concluding remarks

We would like to begin by pointing out that, although introducing the generalized ideal class groups in this thesis was very technically motivated, the generalized ideal class groups (also known as "ray class groups") occupy a central position within class field theory. Therefore the reader should not worry about having learned an obsolete definition only to never think about it again after having finished the proof of Chebotarev's Density Theorem.

Furthermore, we mention that we have only touched upon the surface in the discussion of the applications of the theorem. We considered including a chapter on the application of the infinite version of Chebotarev's theorem to the study of the Tate module of an elliptic curve (the author intented to study [18] to this end). However, this was deemed to shift the focus of the thesis too much away from Chebotarev's theorem.

Regarding more elementary applications of (the finite version of) Chebotarev's Density Theorem, there seem to be many others as well: for one thing, the theorem could also have been applied to more difficult polynomials than $X^n - a$.

A more spectacular kind of result that follows from the density theorem is that the rational primes $p$ for which the decimal expansion of $1/p$ has odd period length has a density equal to $1/3$. The proof can be found in [20]. Although the statement itself is quite elementary, the proof in fact relies on a so-called "effective" form of Chebotarev's Density Theorem: an asymptotic formula à la Theorem 3.5 that gives the number of prime ideals of bounded norm of a number field $K$ for which the primes above have a given Frobenius element (the primes above thus lying in some number field $L$ that is Galois over $K$). These effective forms are far from elementary and some even rely on the Generalized Riemann Hypothesis [21, §2]. We did not touch upon effective forms of the density theorem in this thesis, but we would like to point them out to the reader as a domain worth further exploration.

Finally, on a more personal note, many thanks are due to Arno Kret: for his helpful and pleasant guidance and for his excellent suggestion of writing a thesis on Chebotarev's Density Theorem.

# Bibliography


[1] F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. *Sitz. Akad. Wiss. Berlin*, 689–703, 1896.

[2] N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math. Ann.* **95**, 191–228, 1925.

[3] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer, 2000.

[4] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[5] P. Stevenhagen, *Number Rings*, http://websites.math.leidenuniv.nl/algebra/ant.pdf.

[6] S. Lang, *Algebraic Number Theory*, Addison-Wesley, 1970.

[7] E. Artin, *Galois Theory*, second edition, sixth printing, Notre Dame, 1971.

[8] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981.

[9] E. Freitag, R. Busam, *Complex Analysis*, Springer, 2005.

[10] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, erster Band, B. G. Teubner, 1909.

[11] J.-P. Serre, *A Course in Arithmetic*, corrected fifth printing, Springer, 1996.

[12] B. Steinberg, *Representation Theory of Finite Groups*, Springer, 2012.

[13] M. Deuring, Über den Tschebotareffschen Dichtigkeitssatz. *Math. Ann.* **110**, 414–415, 1935.

[14] P. Stevenhagen, H. W. Lenstra, Chebotarëv and his Density Theorem. *Math. Intelligencer* **18**, 26–37, 1996.

[15] R. L. Schilling, *Measures, Integrals and Martingales*, second edition, Cambridge University Press, 2017.

[16] H. W. Lenstra, *Galois theory for schemes*, electronic third edition, 2008.

[17] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[18] J.-P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, Addison-Wesley, 1989.

[19] S. Lang, *Algebraic Number Theory*, second edition, Springer, 1994.

[20] R. W. K. Odoni, A Conjecture of Krishnamurty on Decimal Periods and Some Allied Problems. *J. Number Theory* **13**, 303–319, 1981.

[21] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I.H.E.S.* **54**, 123–201, 1981.

# Populaire samenvatting

Vaak wordt van priemgetallen gedacht dat er totaal geen patronen in te ontdekken vallen. We willen niet bestrijden dat hier mogelijk enige vorm van waarheid in schuilt, maar zonder te specificeren wat er met "patronen" wordt bedoeld kan men er al gauw tegen inbrengen dat er wel degelijk patronen te ontdekken zijn: zo is ieder priemgetal groter dan 2 bijvoorbeeld oneven.
Afgezien van dit soort flauwe observaties, zijn er ook subtielere patronen: zo kan men de "kans" bepalen dat een willekeurig priemgetal eindigt op een 1. Met wat rekenen ziet men bijvoorbeeld al:

| $n$ | aantal priemgetallen $< n$ | aantal priemgetallen $< n$ eindigend op 1 | percentage $< n$ eindigend op 1 |
|---|---|---|---|
| 10 | 4 | 0 | $00,0000\ldots\%$ |
| 100 | 25 | 5 | $20,0000\ldots\%$ |
| 1000 | 168 | 40 | $23,8095\ldots\%$ |
| 10.000 | 1229 | 306 | $24,8982\ldots\%$ |
| 100.000 | 9592 | 2387 | $24,8853\ldots\%$ |
| 1000.000 | 78498 | 19617 | $24,9904\ldots\%$ |
| 10.000.000 | 664579 | 166104 | $24,9938\ldots\%$ |
| 100.000.000 | 5761455 | 1440298 | $24,9988\ldots\%$ |
| 1000.000.000 | 50847534 | 12711386 | $24,9990\ldots\%$ |

Dit suggereert dat de kans dat een priemgetal op een 1 eindigt 25% is. Dit wordt natuurlijk uitgrekend met de computer, maar dan nog weet men het nooit: wie weet komen er na de miljard wel helemaal geen priemgetallen meer die eindigen op een 1!
Het blijkt toch wel zo te zijn, en hoe meer priemgetallen men zelfs afgaat, hoe dichter het percentage bij de 25% zal komen te liggen: dit is een gevolg van Dirichlets Stelling over Rekenkundige Rijen.
Chebotarevs Dichtheidsstelling – het onderwerp van deze scriptie – is een generalisatie van Dirichlets stelling. De dichtheidsstelling maakt het mogelijk een heel spectrum aan kansen te berekenen. Zo kan men de "kans" berekenen dat voor een willekeurig priemgetal $p$ het getal 2 met een $p$-voud verschilt van een vijfde macht: deze kans blijkt 80% te zijn. Ook blijkt uit de dichtheidsstelling – al behandelen we dat niet in deze scriptie – dat voor een derde van de priemgetallen $p$ de decimale ontwikkeling van $1/p$ een periode van oneven lengte heeft [20].
Onder enig voorbehoud spraken we net van "kans", want eigenlijk gaat de stelling niet over *kansen* maar over *dichtheden*. Om die dichtheden te kunnen definiëren heeft men

de beroemde Riemann-zetafunctie

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

nodig – beroemd van de tot op heden onopgehelderde Riemannhypothese. Naast de Riemann-zetafunctie moet men wat meetkunde en algebraïsche getaltheorie doen, en dan kan men de mouwen opstropen om Chebotarevs Dichtheidsstelling te bewijzen!