Galois Representations and Automorphic Forms
(MasterMath)

Peter Bruin and Arno Kret

Autumn 2016

Preliminary draft; comments and corrections are welcome
## Contents

1 Introduction 2

1.1 Quadratic reciprocity ........................................... 3
1.2 First examples of $L$-functions .............................. 5
1.3 Modular forms and elliptic curves ............................ 11
1.4 More examples of $L$-functions .............................. 14
1.5 Exercises ........................................................ 18

2 Algebraic number theory 22

2.1 Profinite groups .................................................. 23
2.2 Galois theory for infinite extensions ......................... 27
2.3 Local $p$-adic fields ........................................... 27
2.4 Algebraic number theory for infinite extensions .......... 40
2.5 Adèles and idèles ............................................... 43
2.6 Class field theory ............................................... 49
2.7 Exercises ........................................................ 50
Chapter 1

Introduction

Contents

1.1 Quadratic reciprocity ........................................... 3
1.2 First examples of \( L \)-functions ................................. 5
  1.2.1 The Riemann \( \zeta \)-function .............................. 5
  1.2.2 Dedekind \( \zeta \)-functions .................................. 8
  1.2.3 Dirichlet \( L \)-functions ..................................... 9
  1.2.4 An example of a Hecke \( L \)-function ....................... 10
1.3 Modular forms and elliptic curves ............................. 11
  1.3.1 Elliptic curves ............................................. 11
  1.3.2 Modular forms ............................................. 13
1.4 More examples of \( L \)-functions ................................ 14
  1.4.1 Artin \( L \)-functions ....................................... 14
  1.4.2 \( L \)-functions attached to elliptic curves ............... 16
  1.4.3 \( L \)-functions attached to modular forms ............... 17
1.5 Exercises ......................................................... 18

In this first chapter, our main goal will be to motivate why one would like to study the objects that this course is about, namely Galois representations and automorphic forms. We give two examples that will later turn out to be known special cases of the Langlands correspondence, namely Gauss’s quadratic reciprocity theorem and the modularity theorem of Wiles et al. We note that the general Langlands correspondence is still largely conjectural and drives much current research in number theory.

Along the way, we will encounter various number-theoretic objects, such as number fields, elliptic curves, modular forms and Galois representations, and we will associate \( L \)-functions to them. These will turn out to form the link by which one can relate objects (such as elliptic curves and modular forms) that a priori seem to be very different.
1.1 Quadratic reciprocity

Recall that if \( p \) is a prime number, then the Legendre symbol modulo \( p \) is defined, for all \( a \in \mathbb{Z} \), by

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^*, \\
-1 & \text{if } a \text{ is a non-square in } (\mathbb{Z}/p\mathbb{Z})^*, \\
0 & \text{if } a \text{ is congruent to } 0 \text{ modulo } p.
\end{cases}
\]

**Theorem 1.1** (Quadratic reciprocity law). Let \( p \) and \( q \) be two distinct odd prime numbers. Then

\[
\left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.
\]

To put this in the context of this course, we consider two different objects. The first object (a Dirichlet character) lives in the “automorphic world”, the second (a character of the Galois group of a number field) lives in the “arithmetic world”.

On the one hand, consider the quadratic Dirichlet character

\[
\chi_q: (\mathbb{Z}/q\mathbb{Z})^* \rightarrow \{\pm 1\}
\]

defined by the Legendre symbol

\[
\chi_q(a \mod q) = \left( \frac{a}{q} \right).
\]

From the fact that the subgroup of squares has index 2 in \( \mathbb{F}_q^* \), it follows that \( \chi_q \) is a surjective group homomorphism.

On the other hand, we consider the field

\[
K_q = \mathbb{Q}(\sqrt{q^*})
\]

where \( q^* = (-1)^{(q-1)/2} q \). The Galois group \( \text{Gal}(K_q/\mathbb{Q}) \) has order 2 and consists of the identity and the automorphism \( \sigma \) defined by \( \sigma(\sqrt{q^*}) = -\sqrt{q^*} \).

To any prime \( p \neq q \) we associate a Frobenius element

\[
\text{Frob}_p \in \text{Gal}(K_q/\mathbb{Q}).
\]

The general definition does not matter at this stage; it suffices to know that

\[
\text{Frob}_p = \begin{cases} 
\text{id} & \text{if } p \text{ splits in } K_q, \\
\sigma & \text{if } p \text{ is inert in } K_q.
\end{cases}
\]

Furthermore, there exists a (unique) isomorphism

\[
\epsilon_q: \text{Gal}(K_q/\mathbb{Q}) \rightarrow \{\pm 1\}.
\]

By definition, a prime \( p \in \mathbb{Z} \) splits in \( K_q \) if and only if \( q^* \) is a square modulo \( p \); in other words, we have

\[
\epsilon_q(\text{Frob}_p) = \left( \frac{q^*}{p} \right).
\]
Note that
\[
\left( \frac{q^*}{p} \right) = \left( \frac{-1}{p} \right)^{(q-1)/2} \left( \frac{q}{p} \right)
\]
and
\[
\left( \frac{-1}{p} \right) = (-1)^{(p-1)/2},
\]
so the quadratic reciprocity law is equivalent to
\[
\left( \frac{q^*}{p} \right) = \left( \frac{pq}{q} \right),
\]
which is in turn equivalent to
\[
\epsilon_q(p \mod q).
\]
Note that it is not at all obvious that the splitting behaviour of a prime \( p \) in \( K_q \) only depends on a congruence condition on \( p \).

*Sketch of proof of the quadratic reciprocity law.* The proof uses the cyclotomic field \( \mathbb{Q}(\zeta_q) \).

It is known that this is an Abelian extension of degree \( \phi(q) = q - 1 \) of \( \mathbb{Q} \), and that there exists an isomorphism
\[
\left( \frac{\mathbb{Z}/q\mathbb{Z}}{\mathbb{Z}/q\mathbb{Z}} \right)^\times \sim \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})
\]
\[a \mapsto \sigma_a,
\]
where \( \sigma_a \) is the unique automorphism of the field \( \mathbb{Q}(\zeta_q) \) with the property that \( \sigma_a(\zeta_q) = \zeta_q^a \).

There is a notion of Frobenius elements \( \text{Frob}_p \in \mathbb{Q}(\zeta_q) \) for every prime number \( p \) different from \( q \), and we have
\[
\sigma_{p \mod q} = \text{Frob}_p.
\]

In Exercise (1.6), you will prove that there exists an embedding of number fields
\[
K_q \hookrightarrow \mathbb{Q}(\zeta_q).
\]
Such an embedding (there are two of them) induces a surjective homomorphism between the Galois groups. We consider the diagram
\[
\begin{array}{ccc}
\text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) & \longrightarrow & \text{Gal}(K_q/\mathbb{Q}) \\
\sim & \downarrow & \sim \\
\left( \frac{\mathbb{Z}/q\mathbb{Z}}{\mathbb{Z}/q\mathbb{Z}} \right)^\times & \longrightarrow & \{\pm 1\} \\
\epsilon_q & & \chi_q
\end{array}
\]
Since the group \( \left( \frac{\mathbb{Z}/q\mathbb{Z}}{\mathbb{Z}/q\mathbb{Z}} \right)^\times \) is cyclic, there exists exactly one surjective group homomorphism \( \left( \frac{\mathbb{Z}/q\mathbb{Z}}{\mathbb{Z}/q\mathbb{Z}} \right)^\times \to \{\pm 1\}, \) so we see that the diagram is commutative. Furthermore, the map on Galois groups respects the Frobenius elements on both sides. Computing the image of \( p \) in \( \{\pm 1\} \) via the two possible ways in the diagram, we therefore conclude that
\[
\epsilon_q(\text{Frob}_p) = \chi_q(p \mod q),
\]
which is the identity that we had to prove. \( \square \)
1.2 First examples of \( L \)-functions

1.2.1 The Riemann \( \zeta \)-function

The prototypical example of an \( L \)-function is the **Riemann \( \zeta \)-function**. It can be defined in (at least) two ways: as a *Dirichlet series*

\[
\zeta(s) = \sum_{n \geq 1} n^{-s}
\]

or as an *Euler product*

\[
\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.
\]

Both the sum and the product converge absolutely and uniformly on subsets of \( \mathbb{C} \) of the form \( \{ s \in \mathbb{C} \mid \Re s \geq \sigma \} \) with \( \sigma > 1 \). Both expressions define the same function because of the geometric series identity

\[
\frac{1}{1 - x} = \sum_{n=0}^{\infty} x^n \quad \text{for } |x| < 1
\]

and because every positive integer has a unique prime factorisation.

We define the *completed \( \zeta \)-function* by

\[
Z(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s).
\]

Here we have used the \( \Gamma \)-function, defined by

\[
\Gamma(s) = \int_{0}^{\infty} \exp(-t)t^{s} \frac{dt}{t} \quad \text{for } \Re s > 0.
\]

By repeatedly using the functional equation

\[
\Gamma(s + 1) = s\Gamma(s),
\]

one shows that the \( \Gamma \)-function can be continued to a meromorphic function on \( \mathbb{C} \) with simple poles at the non-positive integers and no other poles.

**Theorem 1.2** (Riemann, 1859). *The function \( Z(s) \) can be continued to a meromorphic function on the whole complex plane with a simple pole at \( s = 1 \) with residue 1, a simple pole at \( s = 0 \) with residue \(-1\), and no other poles. It satisfies the functional equation

\[
Z(s) = Z(1 - s).
\]

**Proof.** (We omit some details related to convergence of sums and integrals.) The proof is based on two fundamental tools: the *Poisson summation formula* and the *Mellin transform*. The Poisson summation formula says that if \( f : \mathbb{R} \to \mathbb{C} \) is smooth and quickly decreasing, and we define the Fourier transform of \( f \) by

\[
\hat{f}(y) = \int_{-\infty}^{\infty} f(x) \exp(-2\pi i xy) \, dx,
\]
then we have
\[ \sum_{m \in \mathbb{Z}} f(x + m) = \sum_{n \in \mathbb{Z}} \hat{f}(n) \exp(2\pi inx). \]
(This can be proved by expanding the left-hand side in a Fourier series and showing that this yields the right-hand side.) In particular, putting \( x = 0 \), we get
\[ \sum_{m \in \mathbb{Z}} f(m) = \sum_{n \in \mathbb{Z}} \hat{f}(n). \]
For fixed \( t > 0 \), we now apply this to the function
\[ f_t(x) = \exp(-\pi t^2 x^2). \]
By Exercise 1.7, the Fourier transform of \( f_t \) is given by
\[ \hat{f}_t(y) = t^{-1} \exp(-\pi y^2/t^2). \]
The Poisson summation formula gives
\[ \sum_{m \in \mathbb{Z}} \exp(-\pi m^2 t^2) = t^{-1} \sum_{n \in \mathbb{Z}} \exp(-\pi n^2/t^2). \]
Hence, defining the function
\[ \phi: (0, \infty) \longrightarrow \mathbb{R} \]
\[ t \mapsto \sum_{m \in \mathbb{Z}} \exp(-\pi m^2 t^2), \]
we obtain the relation
\[ \phi(t) = t^{-1} \phi(1/t). \]
(1.1)
The definition of \( \phi(t) \) implies
\[ \phi(t) \to 1 \quad \text{as} \quad t \to \infty, \]
and combining this with the relation (1.1) between \( \phi(t) \) and \( \phi(1/t) \) gives
\[ \phi(t) \sim t^{-1} \quad \text{as} \quad t \to 0. \]
To apply the Mellin transform, we need a function that decreases at least polynomially as \( t \to \infty \). We therefore define the auxiliary function
\[ \phi_0(t) = \phi(t) - 1 \]
\[ = 2 \sum_{m=1}^{\infty} \exp(-\pi m^2 t^2). \]
Then we have
\[ \phi_0(t) \sim t^{-1} \quad \text{as} \quad t \to 0 \]
and
\[ \phi_0(t) \sim 2 \exp(-\pi t^2) \quad \text{as} \quad t \to \infty. \]
Furthermore, the equation (1.1) implies
\[ \phi_0(t) = t^{-1} \phi_0(1/t) + t^{-1} - 1. \]
Next, we consider the Mellin transform of $\phi_0$, defined by

$$(\mathcal{M}\phi_0)(s) = \int_0^\infty \phi_0(t)t^s \frac{dt}{t}.$$  

Due to the asymptotic behaviour of $\phi_0(t)$, the integral converges for $\Re s > 1$. We will now rewrite $(\mathcal{M}\phi_0)(s)$ in two different ways to prove the analytic continuation and functional equation of $Z(s)$.

On the one hand, substituting the definition of $\phi_0(t)$, we obtain

$$(\mathcal{M}\phi_0)(s) = 2 \int_0^\infty \left( \sum_{n=1}^\infty \exp(-\pi n^2 t^2) \right) t^s \frac{dt}{t}$$

Substituting $t = 1/u$ in the first integral and using (1.2), we get

$$\int_0^1 \phi_0(t)t^s \frac{dt}{t} = \int_1^\infty \phi_0(1/u)u^{-s} \frac{du}{u}$$

Using the identity $\int_1^\infty u^{-a} \frac{du}{u} = 1/a$ for $\Re a > 0$, we conclude

$$(\mathcal{M}\phi_0)(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \phi_0(1/u)u^{-s} \frac{du}{u} = \int_1^\infty \left( u\phi_0(u) + u - 1 \right) u^{-s} \frac{du}{u}.$$  

On the other hand, we can split up the integral defining $(\mathcal{M}\phi_0)(s)$ as

$$(\mathcal{M}\phi_0)(s) = \sum_{n=1}^\infty \int_0^\infty \exp(-u) \left( \frac{u}{\pi n^2} \right)^{s/2} \frac{du}{u}$$

Using the identity $\int_1^\infty u^{-a} \frac{du}{u} = 1/a$ for $\Re a > 0$, we conclude

$$(\mathcal{M}\phi_0)(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \phi_0(1/u)u^{-s} \frac{du}{u} = \int_1^\infty \left( u\phi_0(u) + u - 1 \right) u^{-s} \frac{du}{u}.$$  

Both integrals converge for all $s \in \mathbb{C}$. The right-hand side therefore gives the meromorphic continuation of $Z(s)$ with the poles described in the theorem. Furthermore, it is clear that the right-hand side is invariant under the substitution $s \mapsto 1 - s$. 

$\square$
CHAPTER 1. INTRODUCTION

Remark 1.3. Each of the above two ways of writing $\zeta(s)$ (as a Dirichlet series or as an Euler product) expresses a different aspect of $\zeta(s)$. The Dirichlet series is needed to obtain the analytic continuation, while the Euler product highlights the relationship to the prime numbers.

1.2.2 Dedekind $\zeta$-functions

The Riemann $\zeta$-function expresses information related to arithmetic in the rational field $\mathbb{Q}$. Next, we go from $\mathbb{Q}$ to general number fields (finite extensions of $\mathbb{Q}$). We will introduce Dedekind $\zeta$-functions, which are natural generalisations of the Riemann $\zeta$-function to arbitrary number fields.

Let $K$ be a number field, and let $\mathcal{O}_K$ be its ring of integers. For every non-zero ideal $a$ of $\mathcal{O}_K$, the norm of $a$ is defined as

$$N(a) = \#(\mathcal{O}_K/a).$$

Definition 1.4. Let $K$ be a number field. The Dedekind $\zeta$-function of $K$ is the function $\zeta_K : \{s \in \mathbb{C} | \Re s > 1\} \to \mathbb{C}$ defined by

$$\zeta_K(s) = \sum_{a \subseteq \mathcal{O}_K} N(a)^{-s},$$

where $a$ runs over the set of all non-zero ideals of $\mathcal{O}_K$.

By unique prime ideal factorisation in $\mathcal{O}_K$, we can write

$$\zeta_K(s) = \prod_p \frac{1}{1 - N(p)^{-s}},$$

where $p$ runs over the set of all non-zero prime ideals of $\mathcal{O}_K$.

The same reasons why one should be interested the Riemann $\zeta$-function also apply to the Dedekind $\zeta$-function: its non-trivial zeroes encode the distribution of prime ideals in $\mathcal{O}_K$, while its special values encode interesting arithmetic data associated with $K$.

Let $\Delta_K \in \mathbb{Z}$ be the discriminant of $K$, and let $r_1$ and $r_2$ denote the number of real and complex places of $K$, respectively. Then one can show that the completed $\zeta$-function

$$Z_K(s) = |\Delta_K|^{s/2}(\pi^{-s/2}\Gamma(s/2))^r_1((2\pi)^{1-s}\Gamma(s))^{r_2}\zeta_K(s)$$

has a meromorphic continuation to $\mathbb{C}$ and satisfies

$$Z_K(s) = Z_K(1 - s).$$

Theorem 1.5 (Class number formula). Let $K$ be a number field. In addition to the above notation, let $h_K$ denote the class number, $R_K$ the regulator, and $w_K$ the number of roots of unity in $K$. Then $\zeta_K(s)$ has a simple pole in $s = 1$ with residue

$$\text{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_KR_K}{|\Delta_K|^{1/2}w_K}.$$

Furthermore, one has

$$\lim_{s \to 0} \frac{\zeta_K(s)}{s^{r_1 + r_2 - 1}} = -\frac{h_KR_K}{w_K}.$$
1.2.3 Dirichlet $L$-functions

Next, we will describe a construction of $L$-functions that is of a somewhat different nature, since it does not directly involve number fields or Galois theory. Instead, it is more representative of the $L$-functions that we will later attach to automorphic forms.

Definition 1.6. Let $n$ be a positive integer. A Dirichlet character modulo $n$ is a group homomorphism

$$\chi: (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times.$$ 

Let $n$ be a positive integer, and let $\chi$ be a Dirichlet character modulo $n$. We extend $\chi$ to a function

$$\tilde{\chi}: \mathbb{Z} \to \mathbb{C}$$

by putting

$$\tilde{\chi}(m) = \begin{cases} 
\chi(m \mod n) & \text{if } \gcd(m, n) = 1, \\
0 & \text{if } \gcd(m, n) > 1.
\end{cases}$$

By abuse of notation, we will usually write $\chi$ for $\tilde{\chi}$. Furthermore, we let $\overline{\chi}$ denote the complex conjugate of $\chi$, defined by

$$\overline{\chi}: \mathbb{Z} \to \mathbb{C},$$

$$m \mapsto \overline{\chi(m)}.$$ 

One checks immediately that $\overline{\chi}$ is a Dirichlet character satisfying

$$\chi(m)\overline{\chi}(m) = \begin{cases} 
1 & \text{if } \gcd(m, n) = 1, \\
0 & \text{if } \gcd(m, n) > 1.
\end{cases}$$

For fixed $n$, the set of Dirichlet characters modulo $n$ is a group under pointwise multiplication, with the identity element being the trivial character modulo $n$ and the inverse of $\chi$ being $\overline{\chi}$. This group can be identified with $\text{Hom}((\mathbb{Z}/n\mathbb{Z})^\times, \mathbb{C}^\times)$. It is non-canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, and its order is $\phi(n)$, where $\phi$ is Euler’s $\phi$-function.

Let $n, n'$ be positive integers with $n \mid n'$, and let $\chi$ be a Dirichlet character modulo $m$. Then $\chi$ can be lifted to a Dirichlet character $\chi^{(n')} \mod n'$ by putting

$$\chi^{(n')}(m) = \begin{cases} 
\chi(m) & \text{if } \gcd(m, n') = 1, \\
0 & \text{if } \gcd(m, n') > 1.
\end{cases}$$

The conductor of a Dirichlet character $\chi$ modulo $n$ is the smallest divisor $n_\chi$ of $n$ such that there exists a Dirichlet character $\chi_0$ modulo $n_\chi$ satisfying $\chi = \chi_0^{(n)}$. A Dirichlet character $\chi$ modulo $n$ is called primitive if $n_\chi = n$.

Remark 1.7. If you already know about the topological ring $\hat{\mathbb{Z}} = \varprojlim_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$ of profinite integers, you may alternatively view a Dirichlet character as a continuous group homomorphism

$$\chi: \hat{\mathbb{Z}}^\times \to \mathbb{C}^\times.$$ 

This is a first step towards the notion of automorphic representations. Vaguely speaking, these are representations (in general infinite-dimensional) of non-commutative groups somewhat resembling $\hat{\mathbb{Z}}^\times$. 
Note that when we view Dirichlet characters as homomorphisms $\chi: \hat{\mathbb{Z}}^\times \to \mathbb{C}^\times$, there
is no longer a notion of a modulus of $\chi$. However, we can recover the conductor of $\chi$ as
the smallest positive integer $n_\chi$ for which $\chi$ can be factored as a composition
$$\chi: \hat{\mathbb{Z}}^\times \to (\mathbb{Z}/n_\chi\mathbb{Z})^\times \to \mathbb{C}^\times.$$ 

**Definition 1.8.** Let $\chi: \mathbb{Z} \to \mathbb{C}$ be a Dirichlet character modulo $n$. The Dirichlet $L$-
function attached to $\chi$ is the function
$$L(\chi, s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$ 

In a similar way as for the Riemann $\zeta$-function, one shows that the sum converges
absolutely and uniformly on every right half-plane of the form $\{s \in \mathbb{C} \mid \Re s \geq \sigma\}$ with
$\sigma > 1$. This implies that the above Dirichlet series defines a holomorphic function $L(\chi, s)$
on the right half-plane $\{s \in \mathbb{C} \mid \Re s > 1\}$.

Furthermore, the multiplicativity of $L(\chi, s)$ implies the identity
$$L(\chi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}} \text{ for } \Re s > 1.$$ 

In Exercise 1.8 you will show that $L(\chi, s)$ admits an analytic continuation and functional
equation similar to those for $\zeta(s)$.

**Remark 1.9.** The functions $L(\chi, s)$ were introduced by P. G. Lejeune-Dirichlet in the proof
of his famous theorem on primes in arithmetic progressions:

**Theorem** (Dirichlet, 1837). Let $n$ and $a$ be coprime positive integers. Then there exist
infinitely many prime numbers $p$ with $p \equiv a \pmod{n}$.

**1.2.4 An example of a Hecke $L$-function**

Just as Dedekind $\zeta$-functions generalise the Riemann $\zeta$-function, the Dirichlet $L$-functions
$L(\chi, s)$ can be generalised to $L$-functions of Hecke characters. As the definition of Hecke
characters is slightly involved, we just give an example at this stage.

Let $I$ be the group of fractional ideals of the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers. We
define a group homomorphism
$$\chi: I \to \mathbb{Q}(\sqrt{-1})^\times$$
$$a \mapsto a^4,$$
where $a \in \mathbb{Q}(\sqrt{-1})$ is any generator of the fractional ideal $a$. Such an $a$ exists because
$\mathbb{Z}[\sqrt{-1}]$ is a principal ideal domain, and is unique up to multiplication by a unit in $\mathbb{Z}[\sqrt{-1}]$.
In particular, since all units in $\mathbb{Z}[\sqrt{-1}]$ are fourth roots of unity, $\chi(a)$ is independent of
the choice of the generator $a$. Furthermore, we have $N(a) = |a|^2$. After choosing an
embedding $\mathbb{Q}(\sqrt{-1}) \hookrightarrow \mathbb{C}$, we can view $\chi$ as a homomorphism $I \to \mathbb{C}^\times$. This is one of the
simplest examples of a Hecke character.

We define a Dirichlet series $L(\chi, s)$ by
$$L(\chi, s) = \sum_a \chi(a) N(a)^{-s},$$
CHAPTER 1. INTRODUCTION

where $a$ runs over all non-zero integral ideals of $\mathbb{Z}[\sqrt{-1}]$, and where as before $N(a)$ denotes the norm of the ideal $a$. One can check that this converges for $4 - 2s < -2$ and therefore defines a holomorphic function on $\{ s \in \mathbb{C} \mid \Re s > 3 \}$. By unique ideal factorisation in $\mathbb{Z}[\sqrt{-1}]$, this $L$-function admits an Euler product

$$L(\chi, s) = \prod_p \frac{1}{1 - \chi(p)N(p)^{-s}} = \prod_{p \text{ prime}} \prod_{p|\mathfrak{a}} \frac{1}{1 - \chi(p)N(p)^{-s}}.$$ 

where $p$ runs over the set of all non-zero prime ideals of $\mathbb{Z}[\sqrt{-1}]$.

Concretely, the ideals of smallest norm in $\mathbb{Z}[\sqrt{-1}]$ and the values of $\chi$ on them are

<table>
<thead>
<tr>
<th>$a$</th>
<th>(1)</th>
<th>(1 + $i$)</th>
<th>(2)</th>
<th>(2 + $i$)</th>
<th>(2 - $i$)</th>
<th>(2 + 2$i$)</th>
<th>(3)</th>
<th>(3 + $i$)</th>
<th>(3 - $i$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N(a)$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>$\chi(a)$</td>
<td>1</td>
<td>-4</td>
<td>16</td>
<td>-7 + 24$i$</td>
<td>-7 - 24$i$</td>
<td>-64</td>
<td>81</td>
<td>28 - 96$i$</td>
<td>28 - 96$i$</td>
</tr>
</tbody>
</table>

This gives the Dirichlet series

$$L(\chi, s) = 1^{-s} - 4 \cdot 2^{-s} + 16 \cdot 4^{-s} - 14 \cdot 5^{-s} - 64 \cdot 8^{-s} + 81 \cdot 9^{-s} + 56 \cdot 10^{-s} + \cdots$$

and the Euler product

$$L(\chi, s) = \frac{1}{1 + 2^2 \cdot 2^{-s}} \cdot \frac{1}{1 - (-7 + 24i) \cdot 5^{-s}} \cdot \frac{1}{1 - (-7 - 24i) \cdot 5^{-s}} \cdot \frac{1}{1 - 9^2 \cdot 9^{-s}} \cdots$$

1.3 Modular forms and elliptic curves

1.3.1 Elliptic curves

Let $E$ be an elliptic curve over $\mathbb{Q}$, given by a Weierstrass equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients $a_1, \ldots, a_6 \in \mathbb{Z}$. We will assume that this equation has minimal discriminant among all Weierstrass equations for $E$ with integral coefficients. For every prime power $q = p^m$, we let $\mathbb{F}_q$ denote a finite field with $q$ elements, and we consider the number of points of $E$ over $\mathbb{F}_q$. Including the point at infinity, the number of points is

$$\#E(\mathbb{F}_q) = 1 + \#\{(x, y) \in \mathbb{F}_q \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0\}.$$

For every prime number $p$, we then define a power series $\zeta_{E,p} \in \mathbb{Q}[[t]]$ by

$$\zeta_{E,p} = \exp \left( \sum_{m=1}^{\infty} \frac{\#E(\mathbb{F}_{p^m})}{m} t^m \right)$$.
Theorem 1.10 (Schmidt, 1931; Hasse, 1934). If $E$ has good reduction at $p$, then there exists an integer $a_p$ such that

$$\zeta_{E,p} = \frac{1 - a_p t + pt^2}{(1 - t)(1 - pt)} \in \mathbb{Z}[t].$$

Furthermore, $a_p$ satisfies

$$|a_p| \leq 2\sqrt{p}.$$ 

Looking at the coefficient of $t$ in $\zeta_{E,p}$, we see in particular that the number of $\mathbb{F}_p$-rational points is given in terms of $a_p$ by

$$\#E(\mathbb{F}_p) = p + 1 - a_p.$$ (1.3)

Next, suppose that $E$ has bad reduction at $p$. Then an analogue of Theorem 1.10 holds without the term $pt^2$, and the formula (1.3) remains valid. In this case, there are only three possibilities for $a_p$, namely

$$a_p = \begin{cases} 
1 & \text{if } E \text{ has split multiplicative reduction at } p, \\
-1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \\
0 & \text{if } E \text{ has additive reduction at } p.
\end{cases}$$

Remark 1.11. If $E$ has bad reduction at $p$, then the reduction of $E$ modulo $p$ has a unique singular point, and this point is $\mathbb{F}_p$-rational. The formula (1.3) for $\#E(\mathbb{F}_p)$ includes this singular point. It is not obvious at first sight whether this point should be included in $\#E(\mathbb{F}_p)$ or not; it turns out that including it is the right choice for defining the $L$-function.

We combine all the functions $\zeta_{E,p}$ by putting

$$\zeta_E(s) = \prod_{p \text{ prime}} \zeta_{E,p}(p^{-s}).$$

By Theorem 1.10, the infinite product converges absolutely and uniformly on every set of the form $\{ s \in \mathbb{C} \mid \Re s \geq \sigma \}$ with $\sigma > 3/2$.

More generally, one can try to find out what happens when we replace the elliptic curve $E$ by a more general variety $X$ (more precisely, a scheme of finite type over $\mathbb{Z}$). We can define local factors $\zeta_{X,p}$ and their product

$$\zeta_X(s) = \prod_{p \text{ prime}} \zeta_{X,p}(p^{-s}).$$

in the same way as above; some care must be taken at primes of bad reduction. However, much less is known about the properties of $\zeta_X(s)$ for general $X$. The function $\zeta_X(s)$ is known as the Hasse–Weil $\zeta$-function of $X$, and the Hasse–Weil conjecture predicts that $\zeta_X(s)$ can be extended to a meromorphic function on the whole complex plane, satisfying a certain functional equation.

For elliptic curves $E$ over $\mathbb{Q}$, the Hasse–Weil conjecture is true because of the modularity theorem, which implies that $\zeta_E(s)$ can be expressed in terms of the Riemann $\zeta$-function and the $L$-function of a modular form. More generally, for other varieties $X$, one may try to express $\zeta_X(s)$ in terms of “modular”, or more appropriately, “automorphic” objects, and use these to establish the desired analytic properties of $\zeta_X(s)$. This is one of the motivations for the Langlands conjecture.
Remark 1.12. For an interesting overview of both the mathematics and the history behind ζ-functions and the problem of counting points on varieties over finite fields, see F. Oort’s article [7].

1.3.2 Modular forms

We will denote by \( \mathcal{H} \) the upper half-plane

\[ \mathcal{H} = \{z \in \mathbb{C} \mid \Im z > 0\}. \]

This is a one-dimensional complex manifold equipped with a continuous left action of the group

\[ \text{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}. \]

A particular role will be played by the group

\[ \text{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\} \]

and the groups

\[ \Gamma(n) = \left\{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod n \right\} \]

for \( n \geq 1 \).

Definition 1.13. A congruence subgroup of \( \text{SL}_2(\mathbb{Z}) \) is a subgroup of \( \text{SL}_2(\mathbb{Z}) \) that contains \( \Gamma(n) \) for some \( n \geq 1 \).

Definition 1.14. Let \( \Gamma \) be a congruence subgroup of \( \text{SL}_2(\mathbb{Z}) \), and let \( k \) be a positive integer. A modular form of weight \( k \) is a holomorphic function

\[ f: \mathcal{H} \to \mathbb{C} \]

with the following properties:

(i) For all \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \), we have

\[ f\left( \frac{az + b}{cz + d} \right) = (cz + d)^k f(z). \]

(ii) The function \( f \) is “holomorphic at the cusps of \( \Gamma \)”. (We will not make this precise now.)

From now on we assume (for simplicity) that \( \Gamma \) is of the form

\[ \Gamma_1(n) = \left\{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod n \right\} \]

for some \( n \geq 1 \). Then \( \Gamma \) contains the matrix \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). Then the above definition implies that every modular form for \( \Gamma \) can be written as

\[ f(z) = \sum_{m=0}^{\infty} a_m \exp(2\pi iz) \quad \text{with} \quad a_0, a_1, \ldots \in \mathbb{C}. \]
1.4 More examples of \(L\)-functions

1.4.1 Artin \(L\)-functions

We now introduce Artin \(L\)-functions, which are among the most fundamental examples of \(L\)-functions in the “arithmetic world”. The easiest non-trivial Artin \(L\)-functions are already implicit in the quadratic reciprocity law, and are obtained as follows.

**Example 1.15.** Let \(K\) be a quadratic field of discriminant \(d\), so that \(K = \mathbb{Q}(\sqrt{d})\). Furthermore, let \(\epsilon_K\) be the unique isomorphism \(\text{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \{-1, 1\}\). Similarly to what we did in §1.1 to every prime \(p\) that is unramified in \(K\) (i.e. to every prime \(p \nmid d\)), we associate a Frobenius element \(\text{Frob}_p \in \text{Gal}(K/\mathbb{Q})\) by putting

\[
\text{Frob}_p = \begin{cases} 
\text{id} & \text{if } p \text{ splits in } K, \\
\sigma & \text{if } p \text{ is inert in } K.
\end{cases}
\]

In other words, we have

\[
\text{Frob}_p = \left(\frac{d}{p}\right).
\]

The Artin \(L\)-function attached to \(\epsilon_K\) is then defined by the Euler product

\[
L(\epsilon_K, s) = \prod_{p \text{ unramified in } K} (1 - \epsilon_K(\text{Frob}_p)p^{-s})^{-1} = \prod_{p \text{ prime}} \left(1 - \left(\frac{d}{p}\right)p^{-s}\right)^{-1}.
\]

The quadratic reciprocity law can be viewed as saying that if \(q\) is a prime number and \(K = \mathbb{Q}(\sqrt{q^*})\), where \(q^* = (−1)^{(q-1)/2}q\), and \(\chi_q\) is the quadratic Dirichlet character defined by \(\chi_q(a \mod q) = \left(\frac{a}{q}\right)\), then we have an equality of \(L\)-functions

\[
L(\epsilon_K, s) = L(\chi_q, s).
\]

As a first step towards studying non-Abelian Galois groups and their (higher-dimensional) representations, we make the following definition.

**Definition 1.16.** Let \(K\) be a finite Galois extension of \(\mathbb{Q}\), and let \(n\) be a positive integer. An Artin representation is a group homomorphism

\[
\rho: \text{Gal}(K/\mathbb{Q}) \rightarrow \text{GL}_n(\mathbb{C}).
\]

Artin representations are examples of Galois representations. More general Galois representations are obtained by looking at arbitrary Galois extensions of fields and \(\text{GL}_n\) over other rings.

**Remark 1.17.** Let \(\overline{\mathbb{Q}}\) be an algebraic closure of \(\mathbb{Q}\), and view \(K\) as a subfield of \(\overline{\mathbb{Q}}\) by choosing an embedding. Then \(\text{Gal}(K/\mathbb{Q})\) is a finite quotient of the infinite Galois group \(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\). Just as we can view a Dirichlet character as a continuous one-dimensional \(\mathbb{C}\)-linear representation of the topological group \(\mathbb{Z}^\times\), we can view an Artin representation as a continuous \(n\)-dimensional \(\mathbb{C}\)-linear representation of the topological group \(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\) factoring through the quotient map \(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(K/\mathbb{Q})\).
Next, we want to attach an $L$-function to an Artin representation. If $p$ is a prime number such that the number field $K$ is unramified at $p$, then we can define a Frobenius conjugacy class at $p$ in $\text{Gal}(K/\mathbb{Q})$. If $\sigma_p$ is any Frobenius element at $p$ (i.e. an element of the Frobenius conjugacy class), then we define the characteristic polynomial of Frobenius $F_{\rho,p} \in \mathbb{C}[t]$ by the formula

$$F_{\rho,p} = \det(1 - \rho(\sigma_p)t) \in \mathbb{C}[t].$$

(This is the determinant of an $n \times n$-matrix with coefficients in $\mathbb{C}[t]$.) More generally, if $K$ is possibly ramified at $p$, we have to modify the above definition; this gives rise to a polynomial $F_{\rho,p} \in \mathbb{C}[t]$ of degree at most $n$.

**Definition 1.18.** Let $\rho: \text{Gal}(K/\mathbb{Q}) \to \text{GL}_n(\mathbb{C})$ be an Artin representation. The Artin $L$-function of $\rho$ is the function

$$
\prod_{p \text{ prime}} \frac{1}{F_{\rho,p}(p^{-s})}.
$$

One can show that the product converges absolutely and uniformly for $s$ in sets of the form $\{s \in \mathbb{C} \mid \Re s \geq a\}$ with $a \geq 1$.

**Example 1.19.** Let $K$ be the splitting field of the irreducible polynomial $f = x^3 - x - 1 \in \mathbb{Q}[x]$. Because the discriminant of $f$ equals $-23$, which is not a square, we have

$$K = \mathbb{Q}(\alpha, \sqrt{-23}),$$

where $\alpha$ is a solution of $\alpha^3 - \alpha - 1 = 0$. The number field $K$ has discriminant $-23^3$, and the Galois group of $K$ over $\mathbb{Q}$ is isomorphic to the symmetric group $S_3$ of order 6.

The group $S_3$ has a two-dimensional representation $S_3 \to \text{GL}_2(\mathbb{C})$ defined by

$$
(1) \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (12) \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad (13) \mapsto \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix},
$$

$$
(23) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad (132) \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.
$$

Composing this with some isomorphism $\text{Gal}(K/\mathbb{Q}) \sim S_3$ gives an Artin representation

$$\rho: \text{Gal}(K/\mathbb{Q}) \to \text{GL}_2(\mathbb{C}).$$

The Frobenius conjugacy class at a prime $p$ can be read off from the splitting behaviour of $p$ in $K$, which in turn can be read off from the number of roots of the polynomial $x^3 - x - 1$ modulo $p$. (These are only equivalent because the Galois group is so small; for general Galois groups, the situation is more complicated.) It is a small exercise to show that for a prime number $p \neq 23$, there are three possibilities:

- $-23$ is a square modulo $p$, the polynomial $x^3 - x - 1$ has three roots modulo $p$, and the Frobenius conjugacy class is $\{(1)\}$;

- $-23$ is a square modulo $p$, the polynomial $x^3 - x - 1$ has no roots modulo $p$, and the Frobenius conjugacy class is $\{(123), (132)\}$;

- $-23$ is not a square modulo $p$, the polynomial $x^3 - x - 1$ has exactly one root modulo $p$, and the Frobenius conjugacy class is $\{(12), (13), (23)\}$.
Moreover, one computes the polynomial $F_{\rho,p} \in \mathbb{C}[t]$ by taking the characteristic polynomial of the matrices in the corresponding Frobenius conjugacy class. For the first few prime numbers $p$, this gives

\[
\begin{array}{cccccccc}
p & 2 & 3 & 5 & 7 & 11 & 23 & 59 & \ldots \\
[\sigma_p] & (123) & (123) & (12) & (12) & (12) & - & (1) & \ldots \\
F_{\rho,p} & 1 + t + t^2 & 1 + t + t^2 & 1 - t^2 & 1 - t^2 & 1 - t^2 & 1 - t & \ldots & 1 - 2t + t^2 & \ldots \\
\end{array}
\]

The Euler product and Dirichlet series of $L(\rho, s)$ look like

\[
L(\rho, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + \epsilon(p)p^{1-2s}}.
\]

As we saw in §1.3.1, this infinite product defines a holomorphic function $L(E, s)$ on the right half-plane $\{s \in \mathbb{C} \mid \Re s > 3/2\}$. Furthermore, the $\zeta$-function of $E$ can be expressed as

\[
\zeta_E(s) = \frac{\zeta(s)\zeta(s-1)}{L(E, s)}.
\]

**Example 1.20.** Let $E$ be the elliptic curve

\[
E: y^2 = x^3 - x^2 + x.
\]

This curve has bad reduction at the primes 2 and 3. Counting points on $E$ over the fields $\mathbb{F}_p$ for $p \in \{2, 3, 5, 7, 11\}$ gives

\[
\begin{array}{cccccccc}
p & 2 & 3 & 5 & 7 & 11 \\
\alpha_p & 0 & -1 & -2 & 0 & 4 \\
\end{array}
\]

This shows that the $L$-function of $E$ looks like

\[
L(E, s) = \frac{1}{1} \cdot \frac{1}{1 + 3^{-s}} \cdot \frac{1}{1 + 2 \cdot 5^{-s} + 5 \cdot 5^{-2s}} \cdot \frac{1}{1 + 7 \cdot 7^{-2s}} \cdot \frac{1}{1 - 4 \cdot 11^{-s} + 11 \cdot 11^{-2s}} \cdot \frac{1}{1 - 2^{-s} - 3^{-s} - 5^{-s} + 9^{-s} + 4 \cdot 11^{-s} + \ldots}
\]
We recall that by the Mordell–Weil theorem, the set \( \text{E}(\mathbb{Q}) \) of rational points on \( E \) has the structure of a finitely generated Abelian group. The rank of this Abelian group is still far from understood; it is expected to be linked to the \( L \)-function of \( E \) by the following famous conjecture.

**Conjecture 1.21** (Birch and Swinnerton-Dyer). Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Then \( L(E, s) \) can be continued to a holomorphic function on the whole complex plane, and its order of vanishing at \( s = 1 \) equals the rank of \( \text{E}(\mathbb{Q}) \).

Some partial results on this conjecture are known; in particular, it follows from work of Gross, Zagier and Kolyvagin that if the order of vanishing of \( L(E, s) \) at \( s = 1 \) is at most 1, then this order of vanishing is equal to the rank of \( \text{E}(\mathbb{Q}) \).

**Remark 1.22.** There exists a refined version of the conjecture of Birch and Swinnerton-Dyer that also predicts the leading term in the power series expansion of \( L(E, s) \) around \( s = 1 \). The predicted value involves various arithmetic invariants of \( E \); explaining these is beyond the scope of this course.

### 1.4.3 L-functions attached to modular forms

Let \( n \) and \( k \) be positive integers, and let \( f \) be a modular form of weight \( k \) for the group \( \Gamma_1(n) \), with \( q \)-expansion

\[
f(z) = \sum_{m=0}^{\infty} a_m q^m \quad (q = \exp(2\pi i z)).
\]

The \( L \)-function of \( f \) is defined as the Dirichlet series

\[
L(f, s) = \sum_{m=1}^{\infty} a_m m^{-s}
\]

for \( \Re s > (k + 1)/2 \). (Note that \( a_0 \) does not appear in the sum defining \( L(f, s) \).)

Furthermore, we define the *completed \( L \)-function* attached to \( f \) as

\[
\Lambda(f, s) = n^{s/2} \frac{\Gamma(s)}{(2\pi)^s} L(f, s).
\]

**Theorem 1.23.** Suppose \( f \) is a primitive cusp form. Then \( \Lambda(f, s) \) can be continued to a holomorphic function on all of \( \mathbb{C} \). Furthermore, there exist a primitive cusp form \( f^* \) and a complex number \( \epsilon_f \) of absolute value 1 such that \( \Lambda(f, s) \) and \( \Lambda(f^*, s) \) are related by the functional equation

\[
\Lambda(f, k - s) = \epsilon_f \Lambda(f^*, s).
\]

The proof of this theorem has some similarities to that of Theorem 1.2. The main tools are the theory of newforms, the Frické (or Atkin-Lehner) operator \( w_n \), and the Mellin transform.

The following theorem was proved by Wiles in 1993, with an important contribution by Taylor, in the case of semi-stable elliptic curves, i.e. curves having good or multiplicative reduction at every prime. The proof for general elliptic curves was finished by a sequence of papers by Breuil, Conrad, Diamond and Taylor.
Theorem 1.24 (Modularity of elliptic curves over \( \mathbb{Q} \)). Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Then there exist a positive integer \( n \) and a primitive cusp form \( f \) of weight 2 for the group \( \Gamma_0(n) \) such that
\[
L(E, s) = L(f, s).
\]

1.5 Exercises

Exercise 1.1. Let \( p \) be an odd prime number. Prove the following formulae for the Legendre symbol \( \left( \frac{\cdot}{p} \right) \):
\[
\begin{align*}
\left( \frac{-1}{p} \right) &= \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}; \end{cases} \\
\left( \frac{2}{p} \right) &= \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}; \end{cases} \\
\left( \frac{-2}{p} \right) &= \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod{8}, \\ -1 & \text{if } p \equiv 5, 7 \pmod{8}. \end{cases}
\end{align*}
\]

(Hint: embed the quadratic fields \( \mathbb{Q}(\sqrt{d}) \) for \( d \in \{-1, 2, -2\} \) into the cyclotomic field \( \mathbb{Q}(\zeta_8) \).)

Remark: Together with the quadratic reciprocity law \( \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left( \frac{p}{q} \right) \) for odd prime numbers \( q \neq p \), these formulae make it possible to express \( \left( \frac{a}{p} \right) \) in terms of congruence conditions on \( p \) for all \( a \in \mathbb{Z} \).

Exercise 1.2. Let \( K \) be a quadratic field, and let \( \epsilon_K \) be the unique injective homomorphism from \( \text{Gal}(K/\mathbb{Q}) \) to \( \mathbb{C}^\times \). Prove the identity
\[
\zeta_K(s) = \zeta(s)L(\epsilon_K, s).
\]

Exercise 1.3. Show that the character \( \chi: I \to \mathbb{C}^\times \) defined in §1.2.4, where \( I \) the group of fractional ideals of \( \mathbb{Z}[\sqrt{-1}] \), is injective.

Exercise 1.4. Let \( \chi \) be a Dirichlet character modulo \( n \). We consider the function \( \mathbb{Z} \to \mathbb{C} \) sending an integer \( m \) to the complex number
\[
\tau(\chi, m) = \sum_{j=0}^{n-1} \chi(j) \exp(2\pi ij m/n).
\]
(This can be viewed as a discrete Fourier transform of \( \chi \).) The case \( m = 1 \) deserves special mention: the complex number
\[
\tau(\chi) = \tau(\chi, 1) = \sum_{j=0}^{n-1} \chi(j) \exp(2\pi ij/n)
\]
is called the Gauss sum attached to \( \chi \).

(a) Compute \( \tau(\chi) \) for all non-trivial Dirichlet characters \( \chi \) modulo 4 and modulo 5, respectively.
(b) Suppose that \( \chi \) is primitive. Prove that for all \( m \in \mathbb{Z} \) we have

\[
\tau(\chi, m) = \overline{\chi}(m) \tau(\chi).
\]

(Hint: writing \( d = \gcd(m, n) \), distinguish the cases \( d = 1 \) and \( d > 1 \).)

(c) Deduce that if \( \chi \) is primitive, we have

\[
\tau(\chi) \tau(\overline{\chi}) = \chi(-1) n
\]

and

\[
\tau(\chi) \overline{\tau(\chi)} = n.
\]

**Exercise 1.5.** Let \( \chi \) be a primitive Dirichlet character modulo \( n \). The \textit{generalised Bernoulli numbers} attached to \( \chi \) are the complex numbers \( B_k(\chi) \) for \( k \geq 0 \) defined by the identity

\[
\sum_{k=0}^{\infty} B_k(\chi) \frac{t^k}{k!} = \frac{t}{\exp(nt) - 1} \sum_{j=1}^{n} \chi(j) \exp(jt)
\]

in the ring \( \mathbb{C}[t] \) of formal power series in \( t \).

(a) Prove that if \( \chi \) is non-trivial (i.e. \( n > 1 \)), then we have

\[
\sum_{j=0}^{n-1} \chi(j) \frac{x + \exp(2\pi ij/n)}{x - \exp(2\pi ij/n)} = \frac{2n}{\tau(\chi)(x^n - 1)} \sum_{m=0}^{n-1} \overline{\chi}(m)x^n
\]

in the field \( \mathbb{C}(x) \) of rational functions in the variable \( x \). (Hint: compute residues.)

(b) Prove that for every integer \( k \geq 2 \) such that \((-1)^k = \chi(-1)\), the special value of the Dirichlet \( L \)-function of \( \chi \) at \( k \) is

\[
L(\chi, k) = -\frac{(2\pi i)^k B_k(\chi)}{2\tau(\chi)n^{k-1}k!}.
\]

(Hint: use the identity \( \frac{\cos z}{\sin z} = \frac{1}{z} + \sum_{m=1}^{\infty} \left( \frac{1}{z - m\pi} + \frac{1}{z + m\pi} \right) \).)

**Exercise 1.6.** Let \( q \) be an odd prime number, and let \( q^* = (-1)^{(q-1)/2}q \). Use Gauss sums to prove that there exists an inclusion of fields

\[
\mathbb{Q}(\sqrt{q^*}) \hookrightarrow \mathbb{Q}(\zeta_q).
\]

**Exercise 1.7.** The Fourier transform of a quickly decreasing function \( f : \mathbb{R} \to \mathbb{C} \) is defined by

\[
\hat{f}(y) = \int_{-\infty}^{\infty} f(x) \exp(-2\pi i xy) dx.
\]

(a) Let \( f : \mathbb{R} \to \mathbb{C} \) be a quickly decreasing function, let \( c \in \mathbb{R} \), and let \( f_c(x) = f(x + c) \). Show that \( \hat{f}_c(y) = \exp(2\pi i y) \hat{f}(y) \).

(b) Let \( f : \mathbb{R} \to \mathbb{C} \) be a quickly decreasing function, let \( c > 0 \), and let \( f^c(x) = f(cx) \). Show that \( \hat{f}^c(y) = c^{-1} \hat{f}(y/c) \).
(c) Let \( g_+(x) = \exp(-\pi x^2) \). Show that \( \hat{g}_+(y) = g_+(y) \).

(d) Let \( g_-(x) = \pi x \exp(-\pi x^2) \). Show that \( \hat{g}_-(y) = -ig_-(y) \).

(Hint for (c) and (d): shift the line of integration in the complex plane.)

Exercise 1.8. Let \( n \) be a positive integer, and let \( \chi \) be a primitive Dirichlet character modulo \( n \). Recall that the Dirichlet \( L \)-function attached to \( \chi \) is defined by

\[
L(\chi, s) = \sum_{m=1}^{\infty} \frac{\chi(m)m^{-s}}{m} \quad \text{for } \Re s > 1.
\]

Recall that \( \chi \) is called even if \( \chi(-1) = 1 \) and odd if \( \chi(-1) = -1 \). We define the completed Dirichlet \( L \)-function \( \Lambda(\chi, s) \) by

\[
\Lambda(\chi, s) = \begin{cases} 
\frac{n^{s/2} \Gamma(s/2)}{\pi^{s/2}} L(\chi, s) & \text{if } \chi \text{ is even} \\
\frac{n^{s/2} \Gamma((s+1)/2)}{\pi^{(s-1)/2}} L(\chi, s) & \text{if } \chi \text{ is odd}.
\end{cases}
\]

The goal of this exercise is to generalise the proof of Theorem 1.2 to show that \( \Lambda(\chi, s) \) admits an analytic continuation and functional equation.

We define two functions \( g_+, g_- : \mathbb{R} \to \mathbb{C} \) by

\[
g_+(x) = \exp(-\pi x^2), \\
g_-(x) = \pi x \exp(-\pi x^2).
\]

For every primitive Dirichlet character \( \chi \) modulo \( n \), we define a function

\[
\phi_\chi(t) = \begin{cases} 
\sum_{m \in \mathbb{Z}} \chi(m)g_+(mt) & \text{if } \chi \text{ is even,} \\
\sum_{m \in \mathbb{Z}} \chi(m)g_-(mt) & \text{if } \chi \text{ is odd.}
\end{cases}
\]

(a) Prove the identity

\[
\phi_\chi(t) = \begin{cases} 
\frac{\tau(\chi)}{nt} \phi_\chi(\frac{1}{nt}) & \text{if } \chi \text{ is even,} \\
\frac{\tau(\chi)}{mt} \phi_\chi(\frac{1}{mt}) & \text{if } \chi \text{ is odd.}
\end{cases}
\]

(Hint: use the Poisson summation formula and Exercises 1.4 and 1.7)

From now on, we assume that \( \chi \) is non-trivial, i.e. \( n > 1 \).

(b) Give asymptotic expressions for \( \phi_\chi(t) \) as \( t \to 0 \) and as \( t \to \infty \). (Note: the answer depends on \( \chi \).)

(c) Let \( \mathcal{M}\phi_\chi \) be the Mellin transform of \( \phi_\chi \), defined by

\[
(\mathcal{M}\phi_\chi)(s) = \int_0^\infty \phi_\chi(t)t^{s-1}dt.
\]

Prove that the integral converges for all \( s \in \mathbb{C} \), and that the completed \( L \)-function can be expressed as

\[
\Lambda(\chi, s) = n^{s/2}(\mathcal{M}\phi_\chi)(s) \quad \text{for } \Re s > 1.
\]
(d) Conclude that $\Lambda(\chi, s)$ can be continued to a holomorphic function on all of $\mathbb{C}$ (without poles), and that $\Lambda(\chi, s)$ and $\Lambda(\bar{\chi}, s)$ are related by the functional equation

$$
\Lambda(\chi, s) = \epsilon(\chi)\Lambda(\bar{\chi}, 1-s),
$$

where $\epsilon(\chi)$ is the complex number of absolute value 1 defined by

$$
\epsilon(\chi) = \begin{cases} 
\frac{\tau(\chi)}{\sqrt{n}} & \text{if } \chi \text{ is even}, \\
\frac{\tau(\chi)}{i\sqrt{n}} & \text{if } \chi \text{ is odd}.
\end{cases}
$$

**Exercise 1.9.** Let $a, b \in \mathbb{Z}$, and suppose that the integer $\Delta = -16(4a^3 + 27b^2)$ is non-zero. Let $E$ over $\mathbb{Z}[1/\Delta]$ be the elliptic curve given by the equation $y^2 = x^3 + ax + b$. Let $p$ be a prime number not dividing $\Delta$, and write

$$
N_E(\mathbb{F}_p) = 1 + \#\{(x, y) \in \mathbb{F}_p \mid y^2 = x^3 + ax + b\}.
$$

Prove that

$$
N_E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left( \left( \frac{x^3 + ax + b}{p} \right) + 1 \right)
$$

where $\left( \cdot \mid \cdot \right)$ is the Legendre symbol.

**Exercise 1.10.** Up to isogeny, there are three distinct elliptic curves of conductor 57, namely

- $E_1$: $y^2 + y = x^3 - x^2 - 2x + 2$,
- $E_2$: $y^2 + xy + y = x^3 - 2x - 1$,
- $E_3$: $y^2 + y = x^3 + x^2 + 20x - 32$.

The newforms of weight 2 for the group $\Gamma_0(57)$ are

- $f_1 = q - 2q^2 - q^3 + 2q^4 - 3q^5 + O(q^6)$,
- $f_2 = q - 2q^2 + q^3 + 2q^4 + q^5 + O(q^6)$,
- $f_3 = q + q^2 + q^3 - q^4 - 2q^5 + O(q^6)$.

Which form corresponds to which elliptic curve under Wiles’s modularity theorem?
Chapter 2

Algebraic number theory

Contents

2.1 Profinite groups .................................................. 23
2.2 Galois theory for infinite extensions ......................... 27
2.3 Local $p$-adic fields ............................................. 27
2.4 Algebraic number theory for infinite extensions ............. 40
2.5 Adèles and idèles .................................................. 43
2.6 Class field theory .................................................. 49
2.7 Exercises .......................................................... 50

In this chapter we will recall notions from algebraic number theory. Our goal is to set up the theory in sufficient generality so that we can work with it later. Unfortunately, realistically we cannot be self-contained here. Thus, we encourage the reader to also read up on algebraic number theory from Neukirch’s book, the course of Stevenhagen, and the course on $p$-adic numbers.
2.1 Profinite groups

Topological groups and algebraic groups

In this course a central role will be played by groups that are equipped with a topology. This concept will be both important for automorphic forms and Galois representations.

Definition 2.1. A group \((G, m)\) is a topological group if the underlying set \(G\) is equipped with the structure of a topological space such that the multiplication map \(m : G \times G \rightarrow G, (g, h) \mapsto gh\) and the inversion map \(G \rightarrow G, g \mapsto g^{-1}\) are continuous.

Example 2.2. The following groups are all topological groups

- \((\mathbb{R}^n, +), (\mathbb{C}^n, \times), (\mathbb{R} \times, \times), (\mathbb{R}^d, \times), (\text{GL}_n(\mathbb{R}), \cdot), (\text{GL}_n(\mathbb{C}), \cdot))\).

- \((\mathbb{R}/\mathbb{Z}) = S^1\), the circle group.

- The set of solutions \(E(\mathbb{R}) \cup \{\infty\}\) to the equation \(y^2 = x^3 + ax + b\) of an elliptic curve \(E/\mathbb{R}\) adjoined with the point ‘\(\infty\)’ at infinity, with the usual addition of points where \(\infty\) serves as the identity element for addition.

- Any finite group is a topological group for the discrete topology and also the indiscrete topology.

- An algebraic group \(G/\mathbb{C}\) is actually a topological group for (at least) two topologies: The Zariski topology, and the complex topology on \(G(\mathbb{C})\).

- \(\ldots\) and so on

Remark 2.3. A more formal way to think about topological groups is to use the concept of “group object”. Consider a category \(\mathcal{C}\) in which fibre products exist, so that in particular \(\mathcal{C}\) has a terminal object \(t\). If \(A, B \in \mathcal{C}\) are objects, we write \(A(B) = \text{Hom}_{\mathcal{C}}(B, A)\). This way \(A\) can be viewed as a covariant functor from \(\mathcal{C}\) to the category of sets (cf. the Yoneda lemma). A group object in \(\mathcal{C}\) is a triple \((G, e, m, i)\) with \(G \in \mathcal{C}\) an object, \(e : t \rightarrow G\) the ‘unit element’, \(m : G \times G \rightarrow G\) the ‘multiplication’ and \(i : G \rightarrow G\) the ‘inversion’, such that \((\ast)\) for every test object \(T \in \mathcal{C}\) the maps \(m(T)\) and \(i(T)\) on \(G(T)\) turn the set \(G(T)\) into a group with unit \(t(T)\). The condition \((\ast)\) can also be stated be requiring that a certain amount of diagrams involving \(m\) and \(i\) are commutative (expressing for instance the fact that \(m\) should be associative). In this sense, a topological group is a group object in the category of topological spaces.

Apart from topological groups, a typical example are the Lie groups. A **Lie group** is a smooth manifold equipped with \(\mathcal{C}^\infty\)-maps \(m : G \times G \rightarrow G\) and \(i : G \rightarrow G\) making \(G\) into a group. Finally, in this course, algebraic groups will play an important role as well.

Definition 2.4. Let \(k\) be a commutative ring (for instance an algebraically closed field). An algebraic group over \(k\) is an affine or projective variety \(X\) over \(k\) with a section \(e : \text{Spec}(k) \rightarrow X\), a multiplication morphism \(m : X \times X \rightarrow X\) and an inversion morphism \(i : X \rightarrow X\) satisfying the usual group axioms, i.e. \((X, e, m, i)\) is a group object in the category of \(k\)-varieties.

Example 2.5. The following are all algebraic groups,
The variety $GL_n$ defined by the polynomial equation
\[
\det \begin{pmatrix}
X_{11} & X_{21} & \ldots & X_{n1} \\
X_{21} & X_{22} & \ldots & X_{n2} \\
\vdots & \vdots & \ddots & \vdots \\
X_{1n} & X_{2n} & \ldots & X_{nn}
\end{pmatrix} \neq 0
\]
in $n^2$-dimensional affine space, with coordinates $X_{11}, \ldots, X_{nn}$. The map sending $X_{ij}$ to 1 if $i = j$ and to 0 otherwise defines the unit section $\text{Spec}(k) \to GL_n$. The usual matrix product $(X_{ij})_{i,j=1}^n \cdot (Y_{ij})_{i,j=1}^n = (\sum_{k=1}^n X_{ik}Y_{kj})_{i,j=1}^n$ is a morphism of varieties $m: GL_n \times GL_n \to GL_n$. Similarly, the inverse map $X = (X_{ij})_{i,j=1}^n \mapsto \frac{1}{\det(X)} (\det(X^{ij}))_{i,j=1}^n$ is a morphism of varieties (in the above formula $X^{ij}$ is the minor of $X$, obtained by removing the $i$-th row and $j$-th column from $X$). Thus $(G, e, m, i)$ is an algebraic group.

- The multiplicative group $G_m = \text{Spec}\mathbb{Z}[X^\pm 1]$.
- The additive group $G_a = \text{Spec}\mathbb{Z}[X]$.
- An elliptic curve $E/\mathbb{C}$ equipped with its usual addition is an algebraic group.

**Projective limits**

Let $I$ be a set, and $X_i$ for each $i \in I$ another set. We assume that $I$ is equipped with an ordering $\leq$ that is directed, i.e., for every pair $i, j \in I$ there exists a $k$ with $i \leq k$ and $j \leq k$. For every inequality $i \leq j$ we assume that we are given a map $f_{ji}: X_j \to X_i$ such that whenever $i \leq j \leq k$ we have $f_{ki} = f_{ji} \circ f_{kj}$ and $f_{ii} = \text{Id}_{X_i}$. We call the collection of all these data $(X_i, I, \leq, f_{ji})$ a projective system of sets. Viewing the ordered set $(I, \leq)$ as a category in the obvious way, one could also say that a projective system is a functor from the category $I$ to the category of sets. The projective limit (or inverse limit) of the projective system $(X_i, I, f_{ji})$ is by definition the topological space
\[
\lim_{i \in I} X_i = \left\{ x = (x_i)_{i \in I} \in \prod_{i \in I} X_i \mid \text{for all } i, j \in I \text{ with } i \leq j, f_{ji}(x_j) = x_i \right\},
\] (2.1)
equipped with the topology induced from the product topology on $\prod_{i \in I} X_i$ with the $X_i$ equipped with the discrete topology.

The projective limit $X = \lim_{i \in I} X_i$ has projections $p_i: X \to X_i$. Conversely, if any other set $Y$ has maps $q_i: Y \to X_i$ such that that for all $i \leq j$ we have $f_{ji} \circ q_j = q_i$, then there exist a unique map $u: Y \to X$, such that $q_i = p_i \circ u$ for all $i \in I$. This is the universal property of the projective limit.

**Example 2.6.** Consider a sequence of rational numbers $(x_i)_{i=1}^\infty \in \mathbb{Q}$ converging to $\pi = 3.1415\ldots$ (for instance take the decimal approximations). Put $I = \mathbb{N}$ with the usual ordering of natural numbers. Put for each $i \in \mathbb{N}$, $X_i = \{x_1, x_2, \ldots, x_i\}$ with discrete topology, and whenever $i \leq j$ define the surjection $f_{ji}: X_j \to X_i$, $x_a \mapsto x_{\min(a,i)}$. Then $\lim_{i \in I} X_i = \{x_1, x_2, \ldots, \pi\}$ with the weakest topology such that the points $x_i, i \in I$ are all open, and a system of open neighborhoods of $\pi$ is given by the subsets whose complement is finite.
Example 2.7. Take $X$ a set and let $(X_i)_{i \in I}$ be a ‘decreasing’ collection of subsets of $X$: Whenever $i \leq j$ we have $X_i \subset X_j$. Take the canonical inclusion maps $f_{ji}$. Then $(X, \leq, f_{ji})$ is a projective system. The projective limit of this system is the intersection $\bigcap_{i \in I} X_i \subset X$.

Example 2.8. Take $I$ to be the set of number fields $F$ that are contained in $C$, and which are Galois over $\mathbb{Q}$. We write $F_1 \leq F_2$ whenever $F_1 \subset F_2$. We take for each $i \in I$ with corresponding number field $F_i \subset C$, $X_i$ equal to $\text{Gal}(F_i/\mathbb{Q})$. Then $\lim_{\leftarrow i \in I} \text{Gal}(F_i/\mathbb{Q}) = \text{Aut}_{\text{field}}(\overline{\mathbb{Q}})$, where the topology on the automorphism group is the weakest topology such that for each $x \in \overline{\mathbb{Q}}$ the stabilizer is an open subgroup of $\text{Aut}_{\text{field}}(\overline{\mathbb{Q}})$. In fact, this will be one of our main examples of a projective limit.

Example 2.9. Consider the circle group $S^1 = \mathbb{R}/\mathbb{Z}$, take for each integer $N \in \mathbb{Z}$, $X_N = \mathbb{R}/N\mathbb{Z}$. If $M|N$ then we have the surjection $f_{NM} : X_N \to X_M, x \mapsto x \mod M\mathbb{Z}$. Then $\displaystyle \lim_{\leftarrow N} X_N = \lim_{\leftarrow N} \mathbb{R}/N\mathbb{Z}$ is called the solenoid.

Example 2.10. Consider for $N \in \mathbb{Z}$ the group $\Gamma(N)$ of matrices $g \in GL_2(\mathbb{Z})$ such that $g \equiv (1 \ 0) \mod N$. Consider the upper half plane $\mathcal{H}^+ = \{ z \in \mathbb{C} \mid \Im(z) \neq 0 \}$. If $M|N$ we have the canonical surjection $p_{MN} : \Gamma(N) \backslash \mathcal{H}^+ \to \Gamma(M) \backslash \mathcal{H}^+, x \mapsto \Gamma(M)x$. The projective limit $Y = \lim_{\leftarrow N} \Gamma(N) \backslash \mathcal{H}^+$ with respect to these maps $p_{MN}$ is the modular curve of infinite level. As we defined it here, $Y$ is a topological space, but, as it turns out, $Y$ is has naturally the structure of a (non-noetherian) scheme.

Besides projective limits there are also inductive limits, basically obtained by making the arrows ‘go in this other direction’. A first example is $\overline{\mathbb{Q}} = \varprojlim \mathbb{Q}$, where $F$ ranges over the number fields contained in $\overline{\mathbb{Q}}$ (in fact any set-theoretic union is an inductive limit).

We encourage the reader to read on this subject. Projective systems, inductive systems and limits of these can be defined in arbitrary categories, although they no longer need to automatically exist (just as a product objects, may, or may not exist in your favorite category $\mathcal{C}$). For instance a projective system of groups is a projective system of sets $(X_i, f_{ji})$, where the $X_i$ are groups and the $f_{ji}$ are group morphisms. This projective limit is a topological group (observe that the obvious group operations on $(\overline{\mathbb{Q}}, \lim_{\leftarrow i} \mathbb{Q})$ are indeed continuous), and thus all projective limits exist in the category of groups.

Example 2.11. The ring $R[[t]]$ of formal power series over a commutative ring $R$ is the projective limit the rings $R[t]/t^n R[t]$, ordered in the usual way, with the morphisms from $R[t]/t^{n+j} R[t]$ to $R[t]/t^n R[t]$ given by the natural projection. The topology on $R[[t]]$ coming from the projective limit is referred to as the $t$-adic topology.

Example 2.12. Let $\mathcal{O}_F$ be the ring of integers in a number field. Let $p \subset \mathcal{O}_F$ be a prime ideal. Then $\displaystyle \lim_{\leftarrow n \in \mathbb{Z}_{\geq 1}} \mathcal{O}_F/p^n$ is the completion $\mathcal{O}_{F,p}$ of $\mathcal{O}_F$ at the prime $p$. The projective limit $\mathcal{O}_{F,p}$ is a complete discrete valuation ring.

Example 2.13. Continuing with the previous example, the group $GL_d(\mathcal{O}_F)$ is profinite as well, obtained as the projective limit $\displaystyle \lim_{\leftarrow n \in \mathbb{Z}_{\geq 1}} GL_d(\mathcal{O}_F/p^n)$. In fact for any algebraic group $G$ over $\mathcal{O}_F$, $G(\mathcal{O}_F)$ is profinite, given by a similar projective limit.

Profinite groups

Proposition 2.14. Let $G$ be a topological group. The following conditions are equivalent

(i) $G$ is a projective limit of finite discrete groups
(ii) The topological space underlying to $G$ is Hausdorff, totally disconnected and compact.

(iii) The identity element $e \in G$ has a basis of open neighborhoods which are open subgroups of finite index in $G$.

These conditions are equivalent. If they are satisfied, we call the group $G$ profinite.

The first examples of profinite groups are the (additive) groups $\hat{\mathbb{Z}}_p$ of $p$-adic integers, and the group of profinite integers $\hat{\mathbb{Z}}$. We define $\hat{\mathbb{Z}} = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \mathbb{Z}/N\mathbb{Z}$, so $\hat{\mathbb{Z}}$ is a profinite group. In fact, $\hat{\mathbb{Z}}$ is even a topological ring, called the “Prüfer ring”, or the ring of “profinite integers”. Similarly, for each prime number $p$, $\mathbb{Z}_p$ is also a ring: “the ring of $p$-adic integers”. By the Chinese remainder theorem the mapping $\hat{\mathbb{Z}} \rightarrow \prod_p \mathbb{Z}_p, (x_N)_{N \in \mathbb{Z}_{\geq 1}} \mapsto \prod_{p \mathrm{prime}} (x_{p^n})_{n \in \mathbb{Z}_{\geq 1}}$ is an isomorphism of topological rings.

In fact, the group $\hat{\mathbb{Z}}$ arises as the absolute Galois group of a finite field. For a finite extension $\mathbb{F}_q^N/\mathbb{F}_q$ we have the famous Frobenius automorphism $\mathrm{Frob}: \mathbb{F}_q^N \rightarrow \mathbb{F}_q^N, x \mapsto x^q$. This Frobenius allows us to identify $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ with $\hat{\mathbb{Z}}$ via the isomorphism $\hat{\mathbb{Z}} \rightarrow \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q), x \mapsto \mathrm{Frob}_q^x$. What does raising $\mathrm{Frob}_q$ to the power of the profinite integer $x$ actually mean? Note that any $t \in \mathbb{F}_q$ actually lies in a finite extension $\mathbb{F}_q^N \subset \overline{\mathbb{F}_q}$ for $N \in \mathbb{Z}_{\geq 1}$ sufficiently large. Then for $x = (x_N) \in \hat{\mathbb{Z}}$ the power $\mathrm{Frob}_q^x$ acts on $t$ as $\mathrm{Frob}_q^{x_N}$, which by the divisibility relations does not depend on the choice of $N$. We will see that Galois theory goes through to the infinite setting and gives an inclusion reversing bijection between the closed subgroups $H$ of a Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ and the subfields $M \subset \overline{\mathbb{F}_q}$ that contain $\mathbb{F}_q$. In Exercise 2.16 we use this statement to classify all the algebraic extensions of $\mathbb{F}_q$.

Locally profinite groups

Let $G$ be a totally disconnected locally compact topological group, then $G$ is called locally profinite. Equivalently, a topological group is locally profinite if and only if there exists an open profinite subgroup $K \subset G$ (Exercise 2.5). A typical example is the group $\mathbb{Q}_p$, with open profinite subgroup $\mathbb{Z}_p \subset \mathbb{Q}_p$. Another example is $\mathrm{GL}_n(\mathbb{Q}_p)$, which is locally profinite and has $\mathrm{GL}_n(\mathbb{Z}_p)$ as profinite open subgroup. At first the study of these locally profinite groups may appear like a ‘niche’, but later in the course the groups $\mathrm{GL}_n(\mathbb{Q}_p)$ play a crucial role in describing the prime factor components of automorphic representations.

The topology on $\mathrm{GL}_n(R)$, $R$ a topological ring

Consider a topological ring $R$. Then we can make $\mathrm{GL}_n(R)$ into a topological ring by pulling back the topology via the inclusion $i_1: \mathrm{GL}_n(R) \rightarrow \mathrm{M}_n(R) \times \mathrm{M}_n(R), g \mapsto (g, g^{-1})$, where $\mathrm{M}_n(R) \times \mathrm{M}_n(R) \cong R^{2n^2}$ has the product topology. In many cases, for instance when $R = \mathbb{Q}_p, \mathbb{C}, \mathbb{R}$ it turns out that this topology is the same as pulling back the topology from the inclusion $i_2: \mathrm{GL}_n(R) \rightarrow \mathrm{M}_n(R), g \mapsto g$, with $\mathrm{M}_n(R) \cong R^{n^2}$ the product topology. However, this is not always the case. The problem if you use $i_2$ as opposed to $i_1$, the inversion mapping $\mathrm{GL}_n(R) \rightarrow \mathrm{GL}_n(R), g \mapsto g^{-1}$ is no longer guaranteed to be continuous. Hence, one should use $i_1$ to define the topology. The standard counter example is the ring of adèles, which we will encounter later in the course.
2.2 Galois theory for infinite extensions

Apart from studying Galois groups of finite Galois extensions of fields \( L/F \) it will be important for us to also consider infinite Galois extensions \( L/F \).

We call the extension \( L/F \) algebraic, if for every element \( x \in L \) there exists a polynomial \( f \in F[X] \) such that \( f(x) = 0 \). The extension is separable if, for all \( x \in L \), we can choose the polynomial \( f \) such that it has no repeated roots over \( F \). The extension is normal if the minimal polynomial of \( x \) over \( F \) splits completely in \( L \). Finally we call \( L/F \) Galois if it is normal and separable. As in the finite case, the Galois group \( \text{Gal}(L/F) \) is then the group of field automorphisms \( \sigma: L \rightarrow L \) that are the identity on \( F \). The group \( \text{Gal}(L/F) \) is given the weakest topology such that the stabilizers

\[
\text{Gal}(L/F)_x = \{ \sigma \in \text{Gal}(L/F) \mid \sigma(x) = x \} \subset \text{Gal}(L/F),
\]

are open, for all \( x \in L \). Equivalently, \( \text{Gal}(L/F) \) identifies with the projective limit

\[
\text{Gal}(L/F) = \lim_{\longleftarrow} \text{Gal}(M/F),
\]

where \( M \) ranges over all finite Galois extensions of \( F \) that are contained in \( L \). If \( M, M' \) are two such fields with \( M \subset M' \), then we have the map \( p_{M',M}: \text{Gal}(M'/F) \rightarrow \text{Gal}(M/F) \), \( \sigma \mapsto \sigma|_M \). The projective limit in (2.3) is taken with respect to the maps \( p_{M',M} \). In Exercise 2.17 you will show that the topology on \( \text{Gal}(L/F) \) defined in (2.3) is equivalent to the topology from (2.2).

**Theorem 2.15** (Galois theory for infinite extensions). Let \( L/F \) be a Galois extension of fields. The mapping

\[
\Psi: \{ M \mid F \subset M \subset L \} \rightarrow \{ \text{closed subgroups } H \subset \text{Gal}(L/F) \}, \quad M \mapsto \text{Gal}(L/M),
\]

is a bijection with inverse \( H \mapsto L^H \). Let \( H, H' \) be closed subgroups of \( \text{Gal}(L/F) \) with corresponding fields \( M, M' \). Then

(i) \( M \subset M' \) if and only if \( H \supset H' \).

(ii) Assume \( M \subset M' \). The extension \( M'/M \) is finite if and only if \( H' \) is of finite index in \( H \). Moreover, \( [M' : M] = [H : H'] \).

(iii) \( L/M \) is Galois with group \( \text{Gal}(L/M) = H \).

(iv) \( \sigma(M) \) corresponds to \( \sigma H \sigma^{-1} \) for all \( \sigma \in \text{Gal}(L/F) \).

(v) \( M/F \) is Galois if and only if the subgroup \( H \subset \text{Gal}(L/F) \) is normal, and \( \text{Gal}(M/F) = \text{Gal}(L/F)/H \).

2.3 Local \( p \)-adic fields

The \( p \)-adic numbers

Let \( p \) be a prime number. The ring of \( p \)-adic integers \( \mathbb{Z}_p \) is defined as the projective limit

\[
\lim_{\longleftarrow} \mathbb{Z}/p^n\mathbb{Z}
\]

taken with respect to the surjections \( \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z} \) whenever \( m \geq n \).
A second way to think about the \( p \)-adic integers is as infinite sequences \( x = a_0 + a_1 p^1 + a_2 p^2 + a_3 p^3 + \ldots \) with \( a_i \in \{0, 1, 2, \ldots, p-1\} \). If \( y = b_0 + b_1 p^1 + b_2 p^2 + b_3 p^3 + \ldots \) is another such \( p \)-adic integer, we have the usual formula \( x + y = (a_0 + b_0) + (a_1 + b_1) p^1 + (a_2 + b_2) p^2 + \ldots \) for addition, and the usual formula

\[
x \cdot y = a_0 b_0 + (a_1 b_0 + a_0 b_1) p^1 + (a_2 b_0 + a_1 b_1 + a_0 b_2) p^2 + \ldots
\]

for multiplication. The \( p \)-adic integer \( x \) corresponds to the element

\[
(a_0 + a_1 p^1 + a_2 p^2 + \ldots + a_n p^n)_{n \in \mathbb{Z} \geq 0} \in \lim_{n \to \infty} \mathbb{Z}_p / p^n \mathbb{Z}_p.
\]

If \( x \in \mathbb{Z}_p \), we write \( v_p(x) \) for the largest integer \( n \) such that \( x \equiv 0 \mod p^n \). Then \( v_p(x) \) is the valuation on \( \mathbb{Z}_p \). We define the norm \( | \cdot |_p \) by the formula \( |x|_p = p^{-v_p(x)} \). The \( p \)-adic valuation and \( p \)-adic norm \( |x|_p \) make sense for integers \( x \in \mathbb{Z} \) as well. In particular we can introduce a notion of \( p \)-adic Cauchy sequence of integers: Let \( (x_i)_{i \in \mathbb{Z} \geq 0} \) a sequence of integers \( x_i \in \mathbb{Z} \), then it is \( p \)-Cauchy, if for every \( \varepsilon > 0 \) there exists an integer \( M \in \mathbb{Z} \geq 1 \) such that for all \( m, n > M \) we have \( |x_m - x_n|_p < \varepsilon \). In this sense \( \mathbb{Z}_p \) is the completion of \( \mathbb{Z} \). Via the distance function \( d(x, y) = |x - y|_p \), \( \mathbb{Z}_p \) is a metric space.

**Example 2.16.** If \( N \) is an integer that is coprime to \( p \), then \( N \) has an inverse \( y_n \) modulo \( p^n \), for every \( n \). Moreover these \( y_N \) are unique, and hence form an element of the projective system \( (y_N) \in \lim_{n \to \infty} \mathbb{Z} / p^n \mathbb{Z} = \mathbb{Z}_p \).

By the example, \( \mathbb{Z}_p \) contains the localization \( \mathbb{Z}_{(p)} \) of \( \mathbb{Z} \) at the prime ideal \( (p) \). Just as \( \mathbb{Z}_{(p)} \), the ring \( \mathbb{Z}_p \) is a discrete valuation ring with prime ideals \( (0) \) and \( (p) \). So \( \mathbb{Z}_p \) is a completion of \( \mathbb{Z}_{(p)} \). In fact any local ring \( (R, \mathfrak{m}) \) can be completed for its \( \mathfrak{m} \)-adic topology, by taking the projective limit over the quotients \( R / \mathfrak{m}^n \). For example, we will often consider completions at the various prime ideals of the ring of integers of a number field.

We define the field of \( p \)-adic numbers \( \mathbb{Q}_p \) to be the fraction field of \( \mathbb{Z}_p \). Similar to \( \mathbb{Z}_p \), the elements of \( x = \mathbb{Q}_p \) can be expressed as series \( x = \sum_{i \in \mathbb{Z}} a_i p^i \), where \( a_i \in \{0, 1, 2, \ldots, p-1\} \) and such that for some \( M \in \mathbb{Z} \) we have \( a_i = 0 \) for all \( i < M \). The topology on \( \mathbb{Q}_p \) is the weakest such that \( \mathbb{Z}_p \subset \mathbb{Q}_p \) is an open subring. The valuation \( v \) on \( \mathbb{Z}_p \) extends to \( \mathbb{Q}_p \) by setting \( v(x) = v(a) - v(b) \) if \( x = a/b \in \mathbb{Q}_p \) with \( a, b \in \mathbb{Z}_p \) and \( b \neq 0 \). One checks easily that \( v(x) \) does not depend on the choice of \( a \) and \( b \).

**Norms**

Let \( F \) be a field. A norm on \( F \) is a function \( | \cdot |: F \to \mathbb{R} \geq 0 \) satisfying

\begin{align*}
(N1) \quad & \text{for all } x \in F, \ |x| = 0 \text{ if and only if } x = 0, \\
(N2) \quad & \text{for all } x, y \in F, \ |xy| = |x||y|, \\
(N3) \quad & \text{for all } x, y \in F, \ |x + y| \leq |x| + |y|.
\end{align*}

**Example 2.17.** The trivial norm: \( |x| = 1 \) if and only if \( x \neq 0 \) is a norm on any field. Other than this one we have \( | \cdot |_p \) and the absolute value on \( \mathbb{Q} \), which are both norms.
Let $F$ be a normed field. A sequence $(x_i)_{i=1}^{\infty}$ of elements $x_i \in F$ is a Cauchy sequence if for all $\varepsilon > 0$, there exists $N > 0$ such that for all $n, m \geq N$ we have $|x_n - x_m| < \varepsilon$. The space $F$ is complete if every Cauchy sequence converges. We say that two norms $|\cdot|_1, |\cdot|_2$ on a field are equivalent if a sequence of elements $x_i$ is Cauchy for the one norm, if and only if it is Cauchy for the other norm. It turns out that $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if $|\cdot|_2^\alpha = |\cdot|_1$ for some $\alpha > 0$.

**Theorem 2.18** (Ostrowski’s theorem). Any non-trivial norm $|\cdot|$ on $\mathbb{Q}$ is equivalent to either the usual norm or a $p$-adic norm for some prime number $p$.

We call a norm $|\cdot|$ non-Archimedean, if it satisfies the stronger condition

\[(N3+) \ |x + y| \leq \max(|x|, |y|).\]

When working with number fields and $p$-adic fields, all the non-Archimedean norms are discrete. We call $|\cdot|$ discrete if for every positive real number $x$ there exists an open neighborhood $U \subset \mathbb{R}_{>0}$ of $x$ such that $|F| \cap U = \{x\}$.

**Places of a number field**

If $F$ is a number field, we write $\Sigma_F$ for the set of non-trivial norms on $F$, taken modulo equivalence. We call the elements of $\Sigma_F$ the places or $F$-places if the field $F$ is not clear from the context. We have seen that $\Sigma_\mathbb{Q} = \{\infty, 2, 3, 5, \ldots\}$ so the elements of $\Sigma_F$ can be thought of as an extension of the set of primes, in the following sense

**Lemma 2.19.** Write $\Sigma_F^\infty$ for the finite $F$-places. The mapping

$$\Sigma_F^\infty \to \{\text{non-zero prime ideals } \mathfrak{p} \subset \mathcal{O}_F\}, \quad v \mapsto \{x \in \mathcal{O}_F \mid |x|_v < 1\}$$

is a bijection.

In general if $L/F$ is an extension of number fields, we have the mapping $\Sigma_L \to \Sigma_F$, $w \mapsto v$ given by restricting a norm $|\cdot|_w$ on $L$ to the subfield $F \subset L$, which yields a norm $|\cdot|_v$ on $F$ that corresponds to a place $v \in \Sigma_F$. The fibres of this map are finite, and we say that the place $w$ lies above $v$, and that $v$ lies under $w$.

**Completion**

Recall that $\mathbb{R}$ is constructed from $\mathbb{Q}$ using Cauchy sequences. In fact, we may carry out this construction in much greater generality. Let $F$ be a number field and $v \in \Sigma_F$ be a place with corresponding norm $|\cdot|_v$. Then $(F, |\cdot|_v)$ is not complete, but, we can form its completion $F_v$. This completion is a map $i_v: F \to F_v$, with the following universal property. For any morphism $f: F \to M$ of $F$ into a normed field $M$, such that $|x|_F = |f(x)|_M$ and for any Cauchy sequence $(x_i)_{i=1}^{\infty}$ in $F$ the sequence $(f(x_i))_{i=1}^{\infty}$ in $F$ has a limit point in $M$, there exists a unique map from $u: F_v \to M$ such that $u \circ i_v = f$. The field $F_v$ can be constructed from $F$ by considering the ring $\mathcal{R}$ of all Cauchy sequences and taking the quotient by the ideal $\mathcal{I}$ in $\mathcal{R}$ of sequences that converge to 0.

**Example 2.20.** The field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ for the $p$-adic norm $|\cdot|_p$. 
Norms on a vector space

If $V$ is a finite dimensional vector space over a normed field $(F, |\cdot|)$, a norm on $V$ is a function $|\cdot|: V \to \mathbb{R}_{\geq 0}$ satisfying

(NV1) for all $v \in V$, $|v| = 0$ if and only if $v = 0$,

(NV2) for all $v, w \in V$ and $\lambda \in F$, $|\lambda v| = |\lambda||v|$,

(NV3) for all $v, w \in V$, $|v + w| \leq |v| + |w|$.

Example 2.21. If $V = F^n$, then $v = \sum_{i=1}^{n} v_i e_i \mapsto ||v||_{\text{max}} := \max_{i=1}^{n} |v_i|$ is a norm on $V$.

Proposition 2.22. Let $F$ be a normed field which is complete. Let $V$ be a finite dimensional vector space over $F$. Let $||\cdot||_1, ||\cdot||_2$ be two norms on $V$. Then there exist constants $c, C \in \mathbb{R}_{>0}$ such that for all $v \in V$ we have $c||v||_1 \leq ||v||_2 \leq C||v||_2$, i.e. all norms on $V$ are equivalent.

Valuations

To any non-Archimedean norm we may attach a valuation by taking the logarithm. Even though the one can be deduced by a simple formula from the other, it is often more convenient and intuitive to use both concepts. A valuation $v$ on a field $F$ is a mapping $F \to \mathbb{R}_{\geq 0}$ such that

(V1) $v_F(x) = \infty$ if and only if $x = 0$,

(V2) $v_F(xy) = v_F(x) + v_F(y)$,

(V3) $v_F(x + y) \geq \min(v_F(x), v_F(y))$,

for all $x, y \in F$.

$p$-Adic fields

Let $F$ be a non-Archimedean local field. With this we mean a field $F$ that is equipped with a discrete norm $|\cdot|_F$ which induces a locally compact topology on $F$. It turns out that these fields $F$ are precisely those fields that are obtained as a finite extensions of $\mathbb{Q}_p$ for some prime number $p$.

Proposition 2.23. (i) The topology on $F$ is totally disconnected and $|\cdot|_F$ is non-Archimedean. In particular the topology on $F$ is induced from a discrete valuation $v_F: F \to \mathbb{Z} \cup \{\infty\}$.

(ii) The subset $\mathcal{O}_F = \{x \in F \mid |x|_F \leq 1\} \subset F$ is a subring (the ring of integers).

(iii) The subset $\mathfrak{p} = \{x \in F \mid |x|_F < 1\} \subset \mathcal{O}_F$ is a maximal ideal.

(iv) $\mathcal{O}_F \subset F$ is profinite and equal to the projective limit $\projlim_{n \in \mathbb{Z}_{\geq 0}} \mathcal{O}_F/\mathfrak{p}^n$.

(v) $\mathcal{O}_F$ is local.

(vi) $\mathcal{O}_F$ is a discrete valuation ring.
(vii) \( \mathcal{O}_F \) is of finite type over \( \mathbb{Z}_p \) (and hence the integral closure of \( \mathbb{Z}_p \) in \( F \)).

Proof. (i) If \( |\cdot|_F \) were Archimedean, then \( F \) would be \( \mathbb{R} \) or \( \mathbb{C} \), which do not have a discrete norm. Thus (N3+) must hold, and then (N3+) implies that the topology on \( F \) is totally disconnected. Since the norm is non-Archimedean, it induces a valuation \( v_F \) on \( F \), which we may normalize so that it has value group \( \mathbb{Z} \).

(ii) By (N2), \( \mathcal{O}_F \) is stable under multiplication, and by (N3+), \( \mathcal{O}_F \) is stable under addition, since also \( 0, 1 \in \mathcal{O}_F \) it is indeed an open subring of \( F \).

For (iii) it is easy to see that \( p \) is an ideal. It is also prime, since if \( |xy| < 1 \) for \( |x|, |y| \leq 1 \) we must have \( |x| < 1 \) or \( |y| < 1 \). In (iv) we will see that the index of \( p \) in \( \mathcal{O}_F \) is finite. Thus \( \mathcal{O}_F/p \) is a finite domain and therefore a field.

(iv) Note that \( p \) and \( \mathcal{O}_F \) are open subsets of \( F \). Moreover, since we assumed \( F \) to be locally compact, \( \mathcal{O}_F \) must contain an open neighborhood \( U \) of \( 1 \) with compact closure \( \overline{U} \) in \( F \). Since the topology on \( F \) is induced from the norm, we have \( s \in \mathbb{Z} \) large enough such that \( p^s \subseteq U \). Thus \( p^s \) is compact, hence profinite. The cosets of \( p^{s+1} \) form a disjoint open covering of \( p^s \), which must be finite. By multiplying with a uniformizer we get bijections \( p^t/p^{t-1} \cong p^{t-1}/p^{t-2} \). Thus all the \( p^t/p^{t-1} \) are finite. Hence \( \mathcal{O}_F \) is profinite.

(v) If \( x \in \mathcal{O}_F \setminus p \), then \( |x|_F = 1 \), hence \( |x^{-1}|_F = 1 \) as well and thus \( x \in \mathcal{O}_F^\times \). Hence any element not in \( p \) is a unit, and therefore \( \mathcal{O}_F \) is local.

(vi) Exercise.

(vii) One way to see this is to use a topological version of Nakayama’s lemma, which states that if you have a pro-\( p \) profinite ring \( \Lambda \), a \( \Lambda \)-module \( X \), also pro-\( p \) profinite, and \( I \subset \Lambda \) a closed ideal. Then \( X \) is of finite type over \( \Lambda \) if and only if \( X/I \) is of finite type over \( \Lambda/I \) (see page 89 of Serre’s Bourbaki paper on Iwasawa theory\(^1\)). By this lemma, it suffices to show that \( \mathcal{O}_F/p\mathcal{O}_F \) is finite, which is true. \( \square \)

Convention on normalizations

Both the valuation and norm on a \( p \)-adic \( F \) can be normalized in several ways. For now in, these notes we will work with the convention that \( |\cdot|_F \) has no preferred normalization, so strictly speaking, we work with \( |\cdot|_F \) well-defined only up to positive powers. However, we will normalize the valuation \( v_F \) in such a way that its value group is \( \mathbb{Z} \). In particular \( v_F(\varpi_F) = 1 \), where \( \varpi_F \in F \) is a uniformizer, i.e. a generator of the non-zero prime ideal \( p \subset \mathcal{O}_F \).

Hensel’s lemma

Arguably the most important basic result in the theory of \( p \)-adic integers is Hensel’s lemma. Let us first illustrate the lemma with an example.

Example 2.24. The number 7 is a square modulo 3, since \( 7 \equiv 1^2 \mod 3 \). Even though 7 is not congruent to \( 1^2 \) modulo 25, we can replace \( x_1 = 1 \) with \( x_2 = 1 + a \cdot 3 \), and find the equation \((1 + a_1 \cdot 3)^2 \equiv 1 + 6a \mod 3^2 \) which is satisfied for \( a = 1 \), so \( x_2 = 1 + 3^1 \) is a root of 7 modulo \( 3^2 \). Similarly, if \( x_3 = (1 + a_1 \cdot 3 + a_2 \cdot 3^2) \) for some \( a_2 \in \{0, 1, 2\} \). Then

\[
7 \equiv x_3^2 \equiv (x_2 + a_2 \cdot 3^2) \equiv x_2^2 + 2x_2a_23^2 \equiv 16 + 8a_23^2 \mod 3^3
\]

Hence $a_2 = 1$. Inductively, if we have
\[ x_{n-1}^2 = (a_0 + a_1 3^1 + a_2 3^2 + \ldots + a_{n-1} 3^{n-1})^2 \equiv 7 \pmod{3^n} \]
with $a_i \in \{0, 1, 2\}$, then we can solve for $a_n$ the equation $(x_{n-1} + a_n 3^n)^2 \equiv 7 \pmod{3^{n+1}}$
which rewrites to (noting that $2x_{n-1} \not\equiv 0 \pmod{3}$, so $2x_{n-1} \in (\mathbb{Z}/3^{n+1}\mathbb{Z})^\times$)
\[ a_n 3^n \equiv \frac{7 - x_{n-1}^2}{2x_{n-1}} \pmod{3^{n+1}}. \]
Since $7 \equiv x_{n-1}^2 \pmod{3^n}$, there is a unique choice for $a_n \in \{0, 1, 2\}$ satisfying this congruence.
Hence we have inductively defined a sequence of approximations $x_n$ of $\sqrt{7}$ in $\mathbb{Z}_3$.
Since these approximations $x_n$ are ‘correct’ modulo $3^n$, the sequence $x_n$ is Cauchy for $| \cdot |_3$
and hence converges to a 3-adic integer which we denote by the symbol $\sqrt{7} \in \mathbb{Z}_3$. Note for $a_0$
we had two choices, we chose $a_0 = 1$ for no good reason as we could also have taken $a_0 = 2$. After $a_0$
have been fixed, the $a_i$ for $i > 0$ are uniquely determined by the above inductive procedure. This reflects
the fact that, as in any domain of characteristic $\neq 2, 7$, we have two (or zero!) choices for the square root $\pm \sqrt{7}$
of $7$.

**Proposition 2.25** (Hensel’s lemma). Let $f \in \mathbb{Z}_p[X]$ be a monic polynomial such that $f(x) \equiv 0 \pmod{p}$
for some $x \in \mathbb{Z}_p$ and $f'(x) \not\equiv 0 \pmod{p}$. Then $f$ has a root $\alpha$ in $\mathbb{Z}_p$ such
that $\alpha \equiv x \pmod{p}$.

**Sketch.** Define $a_n$ inductively by $a_0 = x$, $a_{n+1} = a_n - f(a_n)y$, where $y \in \mathbb{Z}$ is a lift of the
inverse of $f'(x)$ modulo $p$. Now show that $\lim_{n \to \infty} a_n = \alpha$. \qed

**Example 2.26.** For any prime number $p$ the $p - 1$-th roots of unity lie in $\mathbb{Z}_p$. To see this, consider
the cyclotomic polynomial $\Phi_{p-1} \in \mathbb{Z}_p[X]$. For $\zeta \in \mathbb{F}_p$ a generator of $\mathbb{F}_p^\times \cong
\mathbb{Z}/(p-1)\mathbb{Z}$, we have $\Phi_{p-1}(\zeta) = 0$. Moreover, $\Phi_{p-1}$ divides the polynomial $X^{p-1}$
which is separable modulo $p$. If the derivative $\Phi'_{p-1}(\zeta)$ were 0 then $\zeta$ would be a repeated zero
of $\Phi_{p-1}|X^{p-1} - 1$. Hence $\Phi'_{p-1}(\zeta) \neq 0$. By Hensel’s lemma $\zeta$ lifts to a root in $\mathbb{Z}_p$.

Hensel’s lemma has many more forms. The first obvious generalizations are from $\mathbb{Q}_p$
to $p$-adic fields $F$, and instead of linear factors modulo $p$, look at lifting a factorization of
a polynomial that exists modulo $p$ to a factorization in $\mathcal{O}_F[x]$.

**Proposition 2.27.** Assume that $f \in \mathcal{O}_F[X]$ is a monic polynomial, and that $\overline{f} \in \kappa_F[X]$
factors into a product $\overline{f} = h \cdot g$ of two monic, relatively prime polynomials $h, g \in \kappa_F[X]$.
Then there exists polynomials $H, G \in \mathcal{O}_F[X]$ such that $H \cdot G = f$ and $\overline{H} = h, \overline{G} = g$.

Another, very general form of Hensel’s lemma is given in EGA IV [?, 18.5.17].

**Theorem 2.28.** Let $R$ be an Henselian local ring with maximal ideal $\mathfrak{m}$, and let $X$ be a
smooth $R$-scheme. Then $X(R) \to X(R/\mathfrak{m})$ is surjective.

In this theorem a local ring $(R, \mathfrak{m})$ is ‘Henselian’ if $R$ satisfies the conclusion of Proposition
2.25 stating that a mod $\mathfrak{m}$ root $\alpha$ of a polynomial $f$ lifts if $f'(\alpha) \not\equiv 0 \pmod{\mathfrak{m}}$. There
are many equivalent ways to characterize henselian rings [Tag 04GE]. In particular the ring $\mathcal{O}_F$
for $F$ a $p$-adic field is Henselian. Another example of an Henselian ring is $\mathbb{Z}_p^{\text{h}}(p)$, by
which we mean the ring of all $\alpha \in \mathbb{Z}_p$ that are algebraic over $\mathbb{Q}$. Since $\mathbb{Z}_p^{\text{h}}(p)$ is countable
while $\mathbb{Z}_p$ is uncountable, the subring $\mathbb{Z}_p^{\text{h}}(p) \subset \mathbb{Z}_p$ is strict with a ‘huge’ index.
For readers which are not familiar with schemes, we spell out explicitly what Theorem 2.28 translates to in terms of a system of polynomials (affine $R$-schemes). Suppose that we are given a collection of polynomials $f_1, f_2, \ldots, f_n \in R[X_1, X_2, \ldots, X_d]$ and elements $\alpha_1, \alpha_2, \ldots, \alpha_d \in R/m$ such that $\overline{f}_i(\alpha_1, \alpha_2, \ldots, \alpha_d) = 0 \in R/m$ for $i = 1, 2, \ldots, n$ and the Jacobian matrix

$$
\text{Jac}(\alpha_1, \alpha_2, \ldots, \alpha_d) = \begin{pmatrix}
\frac{\partial f_1(\alpha_1)}{\partial X_1} & \frac{\partial f_1(\alpha_1)}{\partial X_2} & \cdots & \frac{\partial f_1(\alpha_1)}{\partial X_d} \\
\frac{\partial f_2(\alpha_1)}{\partial X_1} & \frac{\partial f_2(\alpha_1)}{\partial X_2} & \cdots & \frac{\partial f_2(\alpha_1)}{\partial X_d} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{\partial f_n(\alpha_1)}{\partial X_1} & \frac{\partial f_n(\alpha_1)}{\partial X_2} & \cdots & \frac{\partial f_n(\alpha_1)}{\partial X_d}
\end{pmatrix} \in \text{Mat}_{d \times n}(R/m)
$$

has maximal rank $d - n$ (in general the rank of $\text{Jac}(\alpha_1, \alpha_2, \ldots, \alpha_d)$ is at most $d - n$). Then Theorem 2.28 states that $\alpha_1, \alpha_2, \ldots, \alpha_d$ lift to elements $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_d \in R$ such that $f_i(\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_d) = 0 \in R$ for $i = 1, 2, \ldots, n$.

Example 2.29. Consider the (affine part of the) elliptic curve $E$ over $\mathbb{Z}_p$ given by the equation $Y^2 = X^3 + aX + b$, so with discriminant $\Delta = -16(4a^3 + 27b^2)$ not divisible by $p$. The Jacobian matrix $J$ is given by $\left(3x^2 + a, -2y\right)$. If the rank of $J_{\mathbb{F}_p}$ were $0 < 1$ at some point $(x, y) \in \mathbb{F}_p^2$, then both entries of $J(x, y)$ had to be zero modulo $p$, and then the polynomial $f = X^3 + aX + b$ has a root in common with its derivative $3X^2 + a$, contradicting $\Delta \not\equiv 0 \mod p$. Thus the mapping $E(\mathbb{Z}_p) \rightarrow E(\mathbb{F}_p)$ is surjective. More abstractly, any elliptic curve is smooth, so Theorem 2.28 applies.

Finite extensions of $p$-adic fields

Let $L/F$ be a finite extension of $p$-adic fields. Let $N_{L/F} : L \rightarrow F$, be the norm mapping from Galois theory, i.e. if $x \in L$, let $x$ act on $L \cong F^n$ by multiplication, which gives a matrix $M_x \in M_n(F)$, well-defined up to conjugacy. We put $N_{L/F}(x) := \det(M_x)$, which does not depend on the choice of basis. Recall that $N_{L/F}$ is compatible in towers, and if $\alpha \in L$ is a primitive element, then $N_{L/F}(\alpha)$ is (up to sign) the constant term of the minimal polynomial of $\alpha$ over $F$.

Proposition 2.30. The mapping $x \mapsto |N_{L/F}(x)|$ defines a norm on $L$.

Proof. The properties (N1) and (N2) being easy; let us focus on showing (N3+). We have to show that for all $x, y \in L$

$$
|N_{L/F}(x + y)|_F \leq \max(|N_{L/F}(x)|_F, |N_{L/F}(y)|_F).
$$

We may assume that $x/y \in O_L$ (otherwise $y/x \in O_L$, and we can re-label). Dividing by $y$, it is equivalent to show that for all $x \in O_L$ we have

$$
|N_{L/F}(x + 1)|_F \leq \max(|N_{L/F}(x)|_F, 1).
$$

Since $x \in O_L$, we have $x + 1 \in O_L$ as well. The statement thus reduces to $N_{L/F}O_L \subset O_F$, which is clear. $\square$
Eisenstein polynomials

When studying extensions of local fields a crucial role is played by the Eisenstein polynomials. Later we will see that these polynomials give precisely the totally ramified extensions.

**Proposition 2.31.** Let \( f = a_0 + a_1 X^1 + a_2 X^2 + \ldots + X^n \in \mathcal{O}_F[X] \) be a monic polynomial of degree \( n \) whose constant term \( a_0 \) has \( v_F(a_0) = 1 \). Then \( f \) is irreducible if and only if \( a_i \in \mathfrak{p} \) for all \( i \). In this case we call \( f \) an Eisenstein polynomial.

**Proof.** Assume \( f \) is Eisenstein and \( f = g \cdot h \) is a factorization of \( f \) in \( F[X] \) where we may assume \( g \) and \( h \) are monic. Any algebraic number that is a root of \( g \) is also a root of \( f \) and hence is integral. Modulo \( \mathfrak{p} \) we have \( \overline{g} \cdot \overline{h} \equiv X^n \), hence every non-leading coefficient of \( g \) and \( h \) lies in \( \mathfrak{p} \). Let \( g_0 \) (resp. \( h_0 \)) be the constant coefficient of \( g \) (resp. \( v \)). Then \( g_0 h_0 = a_0 \), the constant coefficient of \( f \). Since \( a_0 \in \mathfrak{p} \)\( \mathfrak{p}^2 \) exactly one of the two coefficients \( \{g_0, h_0\} \) lies in \( \mathfrak{p} \). Say it is \( g_0 \). Then \( h_0 \) is a unit, and hence must be the leading coefficient of \( h \) (because we established that all other coefficients lie in \( \mathfrak{p} \)). Thus \( \deg(h) = 0 \) and \( f \) is irreducible. Conversely, assume that \( f \) is irreducible and \( v_F(a_0) = 1 \). Modulo \( \mathfrak{p} \) we may factor \( \overline{f} = X^i \cdot \overline{g} \) where \( \overline{g} \in \kappa_F[X] \) is some polynomial with non-zero constant term. By Hensel’s lemma this factorization lifts to a factorization \( f = h \cdot g \) with \( \overline{h} = X^i \). Since \( \deg(h) > 1 \), we must have \( \deg(h) = \deg(f) \) and \( \deg(g) = 0 \) by irreducibility of \( f \). Thus \( \overline{f} = X^{\deg(f)} \) and \( f \) is an Eisenstein polynomial. \( \square \)

**Example 2.32.** For an odd prime number \( p \) there are by Exercise ?? exactly \( 3 = \# \mathbb{Q}_p^\times/\mathbb{Q}_p^\times 2 - 1 \) quadratic extensions. They are easily written down: \( \mathbb{Q}_p(\sqrt{\zeta}), \mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{-p}) \), where \( \zeta \in \mathbb{Q}_p \) is a primitive root of unity of order \( p - 1 \) (cf. Example 2.26). The quadratic extension \( \mathbb{Q}_p(\sqrt{\zeta}) \) is ‘unramified’ and hence cannot be given by an Eisenstein polynomial (this will be explained in the next section). The other two minimal polynomials are \( X^2 + p \) and \( X^2 + \zeta p \in \mathbb{Z}_p[X] \), which are clearly Eisenstein. As we will see later, studying quadratic extensions is in fact most interesting over \( \mathbb{Q}_2 \), due to the presence of ‘wild ramification’.

For \( p = 2 \), the following \( 7 = \#((\mathbb{Q}_2/\mathbb{Q}_2^\times) - 1 \) extensions are all the quadratic extensions of \( \mathbb{Q}_2 \):

\[
\begin{align*}
\mathbb{Q}_2(\sqrt{2}), & \quad \mathbb{Q}_2(\sqrt{6}), & \quad \mathbb{Q}_2(\sqrt{3}), & \quad \mathbb{Q}_2(i) \\
\mathbb{Q}_2(\sqrt{-2}), & \quad \mathbb{Q}_2(\sqrt{-6}), & \quad \mathbb{Q}_2(\sqrt{-3})
\end{align*}
\]

Precisely 1 of these 7 extensions is ‘unramified’, and hence cannot be given by an Eisenstein polynomial (see next section). From the above list, this is the extension \( \mathbb{Q}_2(\sqrt{-3}) \), since \( \sqrt{-3} = 2 \zeta_3 + 1 \). For all these extensions, except \( \mathbb{Q}_2(i) \) and \( \mathbb{Q}_2(\sqrt{3}) \), the minimal polynomial of the given generator is Eisenstein. For the other two fields we can ‘shift’ the primitive element to obtain an Eisenstein polynomial

\[
\begin{align*}
\mathbb{Q}_2[X]/(X^2 + 2X + 2) \xrightarrow{\sim} \mathbb{Q}_2(i), & \quad X \mapsto 1 - i, \\
\mathbb{Q}_2[X]/(X^2 + 2X - 2) \xrightarrow{\sim} \mathbb{Q}_2(\sqrt{3}), & \quad X \mapsto \sqrt{3} - 1.
\end{align*}
\]

**Ramification of local extensions**

Let \( L/F \) be a finite extension of \( p \)-adic fields. We write \( v_L, v_F \) for the valuations on \( L \) and \( F \) whose value group is \( \mathbb{Z} \subset \mathbb{R} \), so they are normalized in such a way that they take uniformizing elements to 1. Let \( \mathfrak{P} \) be the maximal ideal of \( \mathcal{O}_L \) and \( \mathfrak{p} \) the maximal ideal
of $\mathcal{O}_F$. Then we have $\mathcal{O}_F/(\mathfrak{p} \cap \mathcal{O}_F) \subset \mathcal{O}_L/\mathfrak{p}$. Consequently, $\mathcal{O}_F/(\mathfrak{p} \cap \mathcal{O}_F)$ is a finite domain, and hence a field. Thus $\mathfrak{p} \cap \mathcal{O}_F$ equals the maximal ideal $\mathfrak{p}$ of $\mathcal{O}_F$. In the other direction for the $\mathcal{O}_L$-ideal generated by $\mathfrak{p}$ we have $\mathfrak{p} \mathcal{O}_L = \mathfrak{p}^{e_L/F}$, where $e_{L/F} \in \mathbb{Z}$ is called the ramification index. We write $f_{L/F} = [\kappa_L : \kappa_F]$ for the inertial degree. The unramified extensions are those $L/F$ with $e_{L/F} = 1$, and the totally ramified extensions are those with $e_{L/F} = [L : F]$.

**Proposition 2.33.** We have $[L : F] = f_{L/F} \cdot e_{L/F}$.

**Sketch.** Since $\mathcal{O}_L$ is torsion-free, it is projective over $\mathcal{O}_F$ and hence free as $\mathcal{O}_F$ is local (see, e.g. [5, Exercise 11.10, Theorem 2.5], [5, Theorem 2.5]). Thus, $\mathcal{O}_L \cong \mathcal{O}_F^d$ as $\mathcal{O}_F$-module, and hence also $L \cong F^d$ which implies $d = [L : F]$. Similarly, the $\kappa_F$-dimension of $\mathcal{O}_L \otimes \kappa_F \cong \mathcal{O}_F^d \otimes \kappa_F$ is $d$. On the other hand the successive quotients of the filtration $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ of $\mathcal{O}_L \otimes \kappa_F = \mathcal{O}_L/\mathfrak{p}^{e_L/F}$ are all $\kappa_F$-isomorphic to $\kappa_L$. Since the filtration is of length $e_{L/F}$, we obtain $[L : F] = \dim_{\kappa_F}(\mathcal{O}_L \otimes \kappa_F) = e_{L/F} \cdot f_{L/F}$. \qed

**Corollary 2.34.** If $L/M/F$ is a tower of finite extensions of $p$-adic fields, then $e_{L/F} = e_{L/M} \cdot e_{M/F}$ and $f_{L/F} = f_{L/M} \cdot f_{M/F}$.

**Theorem 2.35.** Let $L/F$ be an extension of $p$-adic fields of degree $n$.

(i) The valuation $v_L$ is given by the formula $v_L(x) = f_{L/F}^{-1} \cdot v_F(N_{L/F}(x))$.

(ii) The extension $L/F$ is unramified if and only if it is of the form $L = F(\zeta)$ where $\zeta$ is root of unity whose order is prime to $p$.

(iii) The subfield $F(\varpi_L) \subset L$ is a (in general non-unique) maximal totally ramified extension of $F$ in $L$.

(iv) The minimal polynomial $f \in \mathcal{O}_F[X]$ of $\varpi_L$ over $F$ is an Eisenstein polynomial.

(v) Let $f \in \mathcal{O}_F[X]$ be an Eisenstein polynomial. Then $L = F[X]/(f)$ is a totally ramified extension of $F$ with uniformizer $X$.

**Proof.** (i) We know that $|N_{L/F}(\cdot)|_F$ defines a norm on $L$. Since all these norms are equivalent, it follows that $|\cdot|_L$ and $|N_{L/F}(\cdot)|_L$ differ by a power of a positive real number. Thus also $v_L(\cdot) = \alpha v_F(N_{L/F}(\cdot))$ for some $\alpha \in \mathbb{R}_{>0}$. Filling in an $F$-uniformizer, we obtain $v_L(\varpi_F) = \alpha v_F(N_{L/F}(\varpi_F))$, and hence $e_{L/F} = \alpha v_F(\varpi_F^{[L:F]}) = \alpha [L : F]$. By Proposition 2.33 we have $f_{L/F} = \alpha^{-1}$. \qed

(ii) Let $\zeta \in L$ be a root of unity of prime to $p$ order. We check that $F(\zeta)/F$ is unramified. The minimal polynomial $f$ of $\zeta$ over $F$ divides the polynomial $X^m - 1 \in \mathcal{O}_F[X]$, with $m$ coprime to $p$. Hence $\bar{f}$ is separable modulo $p$. By Hensel’s lemma any factorization of $\bar{f}$ lifts, and hence $\bar{f}$ must be irreducible. Consequently, the degree of $\kappa_{F(\zeta)}$ over $\kappa_F$ is equal to $\deg(f) = [F(\zeta) : F]$. By Proposition 2.33 the extension $F(\zeta)/F$ is unramified. The converse statement is similar: If $M/F$ is an unramified subfield of $L$, then $\kappa_M$ is generated by a root of unity $\zeta$ over $\kappa_F$, whose order is prime to $p$. By Hensel’s lemma this root of unity lifts to a root of unity $\zeta \in M$. It is then easy to see that $M = F(\zeta)$.

(iii) Exercise 2.21.

(iv) By Proposition 2.33 we have $\kappa_F = \kappa_L$ in the totally ramified case. Let $\varpi_L \in \mathcal{O}_L$ be a primitive element and $f \in \mathcal{O}_F[X]$ its minimal polynomial over $F$. We have
\(v_F(N_{L/F}(\varpi_L)) = v_L(\varpi_L) = 1\). Write \(f = \sum_{i=0}^{[L:F]} a_i X^i\), then \(a_0 = \pm N_{L/F}(\varpi_L)\). Hence \(v_F(a_0) = 1\), thus the constant term of \(f\) has valuation 1. On the other hand, assume \(f \equiv \prod_{i=1}^{k} \phi_i^{e_i} \in \kappa_F[X]\), with the \(\phi_i \in \kappa_F[X]\) irreducible and coprime. By Hensel’s lemma this factorization lifts to a factorization \(f = \prod_{i=1}^{k} f_i \in \mathcal{O}_F[X]\), where \(f_i\) lifts \(\phi_i^{e_i}\). Since \(f\) is irreducible, we must have \(k = 1\). Now \(\varpi_L \equiv 0 \mod \mathfrak{p}\) is a root of the irreducible polynomial \(\phi_1\). Hence \(\phi_1 = X\) and \(f = X^{[L:F]}\).

**(v)** Put \(L = F[X]/(f)\). The norm of \(X\) acting on \(L\) is equal to the constant term \(a_0\) of \(f\), which has the property that \(a_0 \in \mathfrak{p} \mathfrak{p}^2\). Hence \(v_L(X) = f_{L/K}^{-1} v_F(a_0) = f_{L/F}^{-1}\), which is only possible if \(f_{L/F} = 1\).

**Primitive element theorem for \(p\)-adic rings**

A basic theorem for finite extensions \(L/F\) of number fields is that any such extension has a primitive element \(\alpha\) such that \(L = F(\alpha)\). However, on the level of rings of integers there are many examples where \(\mathcal{O}_L\) can not be generated by a single element over \(\mathcal{O}_F\). In case of finite extensions of \(p\)-adic number rings the situation is better, in this case we can find a fairly explicit generator.

Let \(L/F\) be a finite extension of \(p\)-adic fields. The first basic observation is that if \(S \subset \mathcal{O}_L\) is a system of representatives for the quotient \(\mathcal{O}_L/\mathfrak{p}\), then any element \(x \in \mathcal{O}_L\) can be written as an infinite sum \(x = \sum_{i=0}^{\infty} s_i \varpi_L^i\) for \(s_i \in S\). In particular, we may take \(\mu \subset \mathcal{O}_L\) the set of roots of unity of prime to \(p\)-order contained in \(\mathcal{O}_L^\times\). Then \(\mu\) is a system of representatives for \(\mathcal{O}_L/\mathfrak{p}\), and hence \(\mathcal{O}_L = \mathbb{Z}_p[\varpi_L, \zeta]\), if \(\zeta \in \mu\) is of maximal order. Thus, in case \(L/F\) is totally ramified, \(\mathcal{O}_L\) equals \(\mathcal{O}_F[\varpi_L]\), and if \(L/F\) is unramified, \(\mathcal{O}_L\) equals \(\mathcal{O}_F[\zeta]\). In general we have

**Proposition 2.36.** We have \(\mathcal{O}_L = \mathcal{O}_F[\varpi_L + \zeta]\).

**Proof.** Let \(\Phi\) be the minimal polynomial of \(\zeta\) over \(F\). Then \(\Phi(\zeta + \varpi_L) = \frac{d}{dX} \Phi'(\zeta) \varpi_L + \varepsilon\) for some \(\varepsilon \in \mathcal{O}_L\) with \(v_L(\varepsilon) \geq 2\). Since \(\Phi\) is separable modulo \(\mathfrak{p}\) we have \(\Phi'(\zeta) \in \mathcal{O}_L^\times\). Hence \(v_L(\Phi(\varpi_L + \zeta)) = 1\) and \(\Phi(\varpi_L + \zeta)\) is a uniformizing element of \(\mathcal{O}_L\). For each integer \(a \in \mathbb{Z}_{\geq 0}\) we have \((\zeta + \varpi_L)^a = \zeta^a + \varpi_L \varepsilon\) for some \(\varepsilon \in \mathcal{O}_L\). Consider the set \(S\) consisting of 0 and the elements \((\zeta + \varpi_L)^a\) for \(a = 0, 1, 2, \ldots, p^{[F:L]} - 1\). Then \(S\) is a system of representatives \(S\) for the quotient \(\mathcal{O}_L/\mathfrak{p}\). The result now follows by applying the remark above the proposition to the uniformizer \(\Phi(\zeta + \varpi_L)\) and the set of representatives \(S\).

**Ramification groups, the lower numbering filtration**

Let \(L/F\) be a finite Galois extension of \(p\)-adic fields with Galois group \(G = \text{Gal}(L/F)\). Write \(n\) for the degree \(|L:F|\), \(\mathfrak{p}\) for the maximal ideal of \(\mathcal{O}_F\) and \(\mathfrak{p}\) for the maximal ideal of \(L\). The group \(\text{Gal}(L/F)\) preserves the valuation \(v_L(x)\) of elements \(x \in L\). In particular \(G\) acts on \(\mathcal{O}_L\), which is easily seen to be faithful (choose a primitive element \(\alpha\) of \(L/F\) that is also integral, \(\alpha \in \mathcal{O}_L\)). From this action we obtain \(G \rightarrow \text{Aut}_{\mathcal{O}_F}(\mathcal{O}_L)\). The \(i\)-th ramification subgroup \(G_i \subset G\) is defined to be the kernel of the composition

\[G \rightarrow \text{Aut}_{\mathcal{O}_F}(\mathcal{O}_L) \rightarrow \text{Aut}_{\mathcal{O}_F}(\mathcal{O}_L/\mathfrak{p}^{i+1}).\]

Equivalently, \(G_i = \{\sigma \in G \mid \forall x \in \mathcal{O}_L\ v_L(\sigma(x) - x) \geq i + 1\}\). The first 3 groups of this sequence have a special name:
CHAPTER 2. ALGEBRAIC NUMBER THEORY

- $G_{-1} = G$ is the total Galois group,
- $G_0 = I(L/F)$ is the inertia subgroup,
- $G_1 = I(L/F)^{\text{wild}}$ is the wild inertia subgroup.

Let’s first analyze the case $i = -1$. Then we are looking at the mapping

$$G/G_0 = \text{Gal}(L/F)/I(L/F) \to \text{Aut}_{\mathcal{O}_F}(\mathcal{O}_L/\mathfrak{P}) = \text{Aut}_{\mathcal{O}_F}(\kappa_L) = \langle \text{Frob} \rangle, \quad \text{Frob}: x \mapsto x^q.$$  

The subgroup $I(L/F)$ corresponds via Galois theory to the maximal extension $L^{ur} \subset L$ of $F$ that is unramified. We have seen that $L^{ur} = F(\zeta)$, where $\zeta$ is a primitive root of unity, whose order is prime to $p$. Hence Frob lifts to an automorphism of $F(\zeta)$: Send $\zeta$ to $\zeta^q$. This gives the Frobenius element $\text{Frob} \in \text{Gal}(L/F)/I(L/F)$. Abusing language, one sometimes speaks of Frobenius elements $\text{Frob} \in \text{Gal}(L/F)$, with the understanding that only their $I(L/F)$ coset is well-defined.

Let’s now look at the higher ramification groups. Let $i \geq 0$, and define the subgroups

$$U_L^{(i)} = \{ x \in \mathcal{O}^\times_L \mid x \equiv 1 \mod \varpi_L^i \}.$$  

Choose a uniformizing element $\varpi_L \in \mathcal{O}_L$, so that $\mathcal{O}_L = \mathcal{O}_F[a]$, then we obtain the injection

$$G_i/G_{i+1} \hookrightarrow U_L^{(i)}/U_L^{(i+1)}, \quad \sigma \mapsto \sigma(\varpi_L)/\varpi_L.$$  

We have

$$U_L^{(i)}/U_L^{(i+1)} \subset \left\{ \begin{array}{ll} (\kappa_L^\times, -), & i = 0 \\ (\kappa_L^\times, +), & i > 0 \end{array} \right.$$  

Observe that $\kappa_L^\times$ is a finite group of order prime to $p$, while $\kappa_L$ is a $p$-group. In particular the wild inertia $I(L/F)^{\text{wild}}$ is a $p$-Sylow subgroup of $\text{Gal}(L/F)$, and this Sylow $p$-subgroup is normal.

Example: Ramification groups of the cyclotomic extension

Let us look at the example $\mathbb{Q}_p(\zeta_{p^n})$ over $\mathbb{Q}_p$, where $\zeta_{p^n}$ is a primitive $p^n$-th root of unity. We claim that $\mathbb{Q}_p(\zeta_{p^n})$ is a totally ramified extension of $\mathbb{Q}_p$. We have

$$\text{Gal}(\mathbb{Q}_p(\zeta_{p^n})|n \in \mathbb{Z}_{\geq 1}/\mathbb{Q}_p) \subset \mathbb{Z}_p^\times.$$  

in particular by the computation below it will follow that the degree of $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is $(p-1)p^{n-1} = \text{deg}(\Phi_{p^n})$, hence the inclusion above is actually equality.

The minimal polynomial of $\zeta_{p^n}$ over $\mathbb{Q}$ is given by the polynomial

$$\Phi_{p^n}(X) = \frac{X^{p^n} - 1}{X^{p^n-1} - 1} = 1 + X^{p^n-1} + X^{2p^n-1} + \ldots + X^{p^n-p^n-1} \in \mathbb{Q}[X].$$  

By Theorem 2.35 we should be able to find a primitive element in the extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ whose minimal polynomial is Eisenstein. Clearly $\Phi_{p^n}(X)$ is not such a polynomial. In fact, since $\zeta_{p^n} \in \mathbb{Z}[\zeta_{p^n}]$ is a unit, it has no chance of being a uniformizer. The element $1 - \zeta_{p^n} \in \mathbb{Z}[\zeta_{p^n}]$ seems to be a better choice, since $\mathbb{Z}_p[\zeta_{p^n}]/(1 - \zeta_{p^n}) \cong \mathbb{F}_p$, $\zeta_{p^n} \mapsto 1$ and hence $1 - \zeta_{p^n} \in \mathbb{Z}_p[\zeta_{p^n}]$ can’t be a unit.
We check with induction that indeed \( \Phi_{p^n}(X + 1) \) is an Eisenstein polynomial. Clearly, \( \Phi_{p^n}(1) = p \) by the above formula, so we need only to check that the coefficients are divisible by \( p \). For \( n = 1 \) we have
\[
\Phi_p(X + 1) = \frac{(X + 1)^p - 1}{X} \equiv \frac{(X^p + 1) - 1}{X} = X^{p-1} \in \mathbb{F}_p[X],
\]
hence all its coefficients are divisible by \( p \). Assume that the desired divisibility is true for \( m < n \), then compute
\[
\Phi_{p^m}(X + 1) = \frac{(X + 1)^{p^m} - 1}{(X + 1)^{p^{m-1}} - 1} = \frac{(X + 1)^{p^n} - 1}{X \Phi_p(X + 1) \cdots \Phi_{p^{n-1}}(X + 1)} = X^{p^n - p^{n-1}} \in \mathbb{F}_p[X].
\]
Hence \( \Phi_{p^m}(X + 1) \) is indeed Eisenstein. Consequently, \( \mathbb{Q}_p(\zeta_{p^m}) / \mathbb{Q}_p \) is totally ramified.

We compute the ramification subgroups \( \text{Gal}(\mathbb{Q}_p(\zeta_{p^m}) / \mathbb{Q}_p)_i \subset \text{Gal}(\mathbb{Q}_p(\zeta_{p^n}) / \mathbb{Q}_p)_i \). By definition, \( \text{Gal}(\mathbb{Q}_p(\zeta_{p^m}) / \mathbb{Q}_p)_i \) consists of those \( \sigma \in \text{Gal}(\mathbb{Q}_p(\zeta_{p^n}) / \mathbb{Q}_p) \) such that \( v(\sigma(\zeta_{p^m}) - \zeta_{p^n}) \geq i \). Let \( x \in (\mathbb{Z}/p^n \mathbb{Z})^\times \) be such that \( \sigma(\zeta_{p^n}) = \zeta_{p^n}^x \), then
\[
v(\sigma(\zeta_{p^n}) - \zeta_{p^n}) = v(\zeta_{p^n}^x - \zeta_{p^n}) = v(\zeta_{p^n}^{x-1} - 1) = v_p(N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}(\zeta_{p^n}^{x-1} - 1))
\]
Observe that \( \zeta_{p^n}^{x-1} - 1 \) generates the intermediate extension \( \mathbb{Q}_p / \mathbb{Q}_p(\zeta_{p^n}^{x-1}) \subset \mathbb{Q}_p(\zeta_{p^n}) \) where each step is totally ramified. Hence \( v(\zeta_{p^n}^{x-1} - 1) \) equals \( [\mathbb{Q}_p(\zeta_{p^n}) : \mathbb{Q}_p(\zeta_{p^n}^{x-1})] = v_p(x - 1) \), and \( \text{Gal}(\mathbb{Q}_p(\zeta_{p^n}) / \mathbb{Q}_p)_i \) identifies with the subgroup
\[
\{ x \in (\mathbb{Z}/p^n \mathbb{Z})^\times \mid x \equiv 1 \mod p^{i+1} \} \subset (\mathbb{Z}/p^n \mathbb{Z})^\times.
\]

**Example: Ramification subgroups of** \( \mathbb{Q}_p(\zeta_p, \sqrt[3]{2}) / \mathbb{Q}_p \)

We assume that \( p \neq 2 \) and also that \( v_p(2^{p-1} - 1) = 1 \) (by Fermat’s little theorem \( v_p(2^{p-1} - 1) > 0 \)). In fact, with a simple for loop in Sage I found that among the odd prime numbers \( p \leq 10^6 \) this condition fails for \( p = 1093 \) and \( p = 3511 \), and holds true for all other \( p \). (We thank Maarten Derickx for helping us out with the exceptional primes, see below).

Write \( L = \mathbb{Q}_p(\zeta_p, \sqrt[3]{2}) \). We have the tower of subfields \( \mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_p) \subset L \). The first step in this tower being understood already in a previous example, let’s look at the second step of the tower. The element \( \sqrt[3]{2} \) is a root of the polynomial \( f = X^p - 2 \in \mathbb{Q}_p[X] \). We have \( \overline{f} = (X - 2)^p \in \mathbb{F}_p[X] \). By the assumption \( v_p(2^{p-1} - 1) = 1 \) the polynomial \( f(X + 2) = (X + 2)^p - 2 \in \mathbb{Q}_p[X] \) is Eisenstein. Hence the element \( \alpha = \sqrt[3]{2} - 2 \in L \) is a uniformizer of a totally ramified degree \( p \) extension \( M/\mathbb{Q}_p \) contained in \( L \), and \( \mathcal{O}_M = \mathbb{Z}_p[\alpha] \).

Since the degrees of \( M \) and \( \mathbb{Q}_p(\zeta_p) \) are coprime, the degree of \( L \) over \( \mathbb{Q}_p \) is equal to \( p(p - 1) \), and \( \text{Gal}(L/\mathbb{Q}_p) = \mathbb{F}_p \times \mathbb{F}_p^\times \) where \( \sigma = (x, y) \in \mathbb{F}_p \times \mathbb{F}_p^\times \) acts by \( \sigma(\zeta_p) = \zeta_p^x \) and \( \sigma(\sqrt[3]{2}) = \zeta_p^y \sqrt[3]{2} \). Finally, in general it is not true that the compositum of two totally ramified extensions is totally ramified; however in case of \( L \), we know that the valuation of \( v_L(p) \) is divisible by \( p \) (look at the intermediate extension \( \mathbb{Q}_p(\zeta_p) \)) and also divisible by \( p - 1 \) (look at the intermediate extension \( \mathbb{Q}_p(\sqrt[3]{2}) \)). Thus \( p(p - 1)|v_L(p) \); since we also know that \( v_L(p) \leq p(p - 1) \), we must have \( v_L(p) = p(p - 1) \), i.e. the extension \( L/\mathbb{Q}_p \) is totally ramified.
At this point we already know two steps of the ramification filtration on $\text{Gal}(L/Q_p)$:

$$G_{-1} = \text{Gal}(L/Q_p) = \mathbb{F}_p \times \mathbb{F}_p^\times \subset G_0 = I(L/Q_p) = \mathbb{F}_p \times \mathbb{F}_p^\times \subset G_1 = I(L/Q_p)^\text{wild} = \mathbb{F}_p,$$

simply because the wild inertia is the pro-$p$-part of the inertia group. There must be one more jump in the filtration, and we want to compute in the straightforward way where this jump happens.

Let’s first find a uniformizer of $L$. Note that $v_L(\alpha) = p - 1$ since $L/M$ is totally ramified of degree $p - 1$, and $\alpha$ is a uniformizer of $M$. Similarly, put $\beta = 1 - \zeta_p$, then $\beta$ is a uniformizer of $Q_p(\zeta_p)$, and hence $v_L(\beta) = p$. Consequently, for $\gamma = \beta/\alpha$, we have $v_L(\gamma) = p - (p - 1) = 1$, and hence $\gamma$ is a uniformizer of $L$ and $O_L = \mathbb{Z}_p[\gamma]$.

Let $\sigma \in I(L/Q_p)^\text{wild}$. Then $\sigma(\zeta_p) = \zeta_p$ and $\sigma(\sqrt[p]{2}) = \zeta_p^x \sqrt[p]{2}$ for some $x \in \mathbb{F}_p$. We compute

$$v_L(\sigma(\gamma) - \gamma) = v_L(\sigma(\beta/\alpha) - \beta/\alpha)$$

$$= v_L(\beta) + v_L(1/\sigma(\alpha) - 1/\alpha)$$

$$= p - v_L(\alpha \sigma(\alpha)) + v_L(\sigma(\alpha) - \alpha)$$

$$= p - 2(p - 1) + v_L(\sigma(\alpha) - \alpha)$$

$$= -p + 2 + v_L(\zeta_p^x \sqrt[p]{2} - \sqrt[p]{2})$$

$$= -p + 2 + p$$

$$= 2,$$

(unless $x = 0$ of course). Hence the ramification filtration on $\text{Gal}(L/Q_p)$ is

$$G_i \quad F_p \times F_p^\times \quad F_p \times F_p^\times \quad F_p \quad 0$$

For the primes $p = 1093$ and $p = 3511$ we used the computer program Pari and saw that actually $\sqrt[p]{2} \in \mathbb{Q}_{1093}$ and $\sqrt[p]{2} \not\in \mathbb{Q}_{3511}$. In particular the extension $Q_p(\zeta_p, \sqrt[p]{2})$ simply equals $Q_p(\zeta_p)$. After quite some discussions with Maarten Derickx, he finally found that this is the what happens in general:

**Lemma 2.37.** If $p$ is a prime number such that $p^2|2^{p-1} - 1$, then $\sqrt[p]{2} \in Q_p$.

**Proof.** Since $p^2|2^{p-1} - 1$ we have for $a_0 = 2$ that $a_0^p \equiv 2 \mod p^2$. We now consider $(a_0 + pb)^p - 2$ modulo $p^3$, and solve for $b$:

$$(a_0 + pb)^p - 2 \equiv a_0^p + \binom{p}{1} a_0^{p-1} pb - 2 \equiv (a_0^p - 2) + p^2 a_0^{p-1} b \mod p^3.$$ 

Since $a_0$ is coprime to $p$, and $a_0^p - 2$ is divisible by $p^2$, there exists a $b$ such that the last equation is $0 \mod p^3$. Take this $b$ and put $a_1 = a_0 + pb$, so $a_1$ is a solution modulo $p^3$. Since $v_p(f'(a_1)) = v_p(pa_1^{p-1}) = 1$ ($a_1$ is a unit), and $v_p(f(a_1)) = v_p(a_1^p - 2) \geq 3$, we have $2v_p(f'(a_1)) = 2 < 3 = v_p(f(a_1))$, and hence the following variant of Hensel’s lemma applies.

**Lemma 2.38.** Let $f \in \mathbb{Z}_p[X]$ be a monic polynomial such that for some $a \in \mathbb{Z}_p$ we have $2v_p(f'(a)) < v_p(f(a))$, then there exists an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$. 

Remark 2.39. After working through the example we found on Wikipedia a page about “Wieferich primes”, i.e. prime numbers such that $p^2|2^{p-1}-1$. Currently, there are precisely 2 of these numbers known, namely 1093 and 3511. It is known that any other prime $p$ with this property is at least $10^{17}$, which we also confirmed up to $10^6$. Silverman showed that the abc-conjecture implies that there are infinitely many. Moreover, if $p$ is an odd prime, $x, y, z \in \mathbb{Z}$ are integers such that $x^p + y^p + z^p = 0$, and $p$ does not divide $xyz$, then $p$ is a Wieferich prime (this result is proved by Wieferich in 1901, so long before modularity of elliptic curves, hence also the name for these numbers. Using modularity, the authors also proudly know an alternative proof).

2.4 Algebraic number theory for infinite extensions

In this section, we will recall some concepts and results from algebraic number theory and generalise them to infinite algebraic extensions of $\mathbb{Q}$. The most important ones are the ring of integers and Frobenius elements.

Number fields and infinite algebraic extensions

Recall that a field extension $L/K$ is algebraic if every $\alpha \in L$ is a zero of some non-zero polynomial in $K[X]$. If $\alpha$ is algebraic, there exists a unique monic polynomial $f_\alpha \in K[X]$ of minimal degree having $\alpha$ as a zero; this $f_\alpha$ is the minimal polynomial of $\alpha$.

We recall that a number field is a finite, and hence algebraic, extension $F$ of $\mathbb{Q}$. Any number field has a primitive element $\alpha \in F$ such that $\alpha$ generates $F$ over $\mathbb{Q}$. The ring of integers $\mathcal{O}_F$ of $F$ is the set of $\alpha \in F$ whose minimal polynomial $f_\alpha$ has coefficients in $\mathbb{Z}$. One checks that sums and products of integral elements are again integral, so $\mathcal{O}_F$ is a subring of $F$. The ring $\mathcal{O}_F$ turns out to be a Dedekind domain, i.e. a noetherian, integrally closed integral domain in which any non-zero prime ideal is maximal.

Remark 2.40. There are two other ways to characterize $\mathcal{O}_F$:

- The ring $\mathcal{O}_F$ is the smallest among all subrings $R \subset F$ with $\text{Frac}(R) = F$ such that $R$ is a Dedekind domain.
- The ring $\mathcal{O}_F$ is the largest subring of $F$ that is finitely generated as a $\mathbb{Z}$-module.

Any non-zero ideal $I \subset \mathcal{O}_F$ admits a factorization into prime ideals

$$I = \prod_{i=1}^t p_i^{e_i} \cdot p_2^{e_2} \cdots p_t^{e_t} \quad \text{in } \mathcal{O}_F,$$

where the $p_i$ are pairwise distinct prime ideals of $\mathcal{O}_F$ and where the $e_i$ are positive integers. This factorization is unique up to permutation.

Let $M/F$ be an extension of number fields. Let $p$ be a prime ideal of $\mathcal{O}_F$. Then $\mathcal{O}_Mp$ is an ideal in $\mathcal{O}_M$ which is no longer a prime ideal in general. The decomposition of $\mathcal{O}_Mp = \prod_{i=1}^t \mathfrak{p}_i^{e_i}$ is the splitting behaviour of $p$. The integer $e_i$ is called the ramification index of $\mathfrak{p}_i$ over $p$, and the degree $f_i = [k(\mathfrak{p}_i) : k(p)]$ of the extension of residue fields is called the residue field degree. We say furthermore that

- $p$ is ramified if $e_i > 1$ for some $i \in \{1, 2, \ldots, t\}$, and unramified otherwise.
• \( p \) is \textit{totally ramified} if \( t = 1 \) and \( e_1 = [M : F] \).

• \( p \) is \textit{inert} if \( \mathcal{O}_M p \) is prime, or equivalently \( t = 1 \) and \( e_1 = 1 \).

• \( p \) is \textit{totally split} if \( t = [M : F] \).

In any extension \( M/F \) of number fields, there are only finitely many primes ramified. By contrast, in the section on Chebotarev’s density theorem below, we will see that the set of inert (resp. totally split) primes has positive density.

\textit{Example 2.41.} The ring of integers of the quadratic extension \( \mathbb{Q}(i)/\mathbb{Q} \) is \( \mathbb{Z}[i] \); it is called the ring of \textit{Gauss numbers}. The ring \( \mathbb{Z}[i] \) is a principal ideal domain, and its primes are given by

• \( \pi = 1 + i \),

• \( \pi = a + bi \) with \( a^2 + b^2 = p \), \( p \equiv 1 \mod 4 \), \( a > |b| > 0 \),

• \( \pi = p \) if \( p \equiv 3 \mod 4 \).

The prime numbers \( p \equiv 1 \mod 4 \) split in \( \mathbb{Z}[i] \) into \( p = (a + bi)(a - bi) \). The prime number 2 is equal to \((1 + i)(1 - i)\). Since 1 + \( i \) and 1 - \( i \) differ by the unit \( i \), we have as ideals \( (2) = (1 + i)^2 \), so the prime 2 ramifies in \( \mathbb{Q}(i)/\mathbb{Q} \).

\textit{Example 2.42.} Recall that even though we have ideal factorization in \( \mathcal{O}_F \), in general the element factorization into irreducible elements is not unique. Typical example:

\[
21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}) \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}
\]

\textbf{Rings of integers of algebraic extensions of \( \mathbb{Q} \)}

Now let \( F \) be any (not necessarily finite) algebraic extension of \( \mathbb{Q} \). As in the case where \( F \) is a number field, we define the \textit{ring of integers} \( \mathcal{O}_F \) as the ring of elements \( x \in F \) that are integral over \( \mathbb{Q} \). If \( F \) is infinite over \( \mathbb{Q} \), the ring \( \mathcal{O}_F \) is not noetherian, and hence is not a Dedekind domain. In general, \( \mathcal{O}_F \) equals the union of all rings \( \mathcal{O}_L \), where \( L \) runs over the number fields contained in \( F \), and hence is a ‘limit’ of Dedekind domains.

\textbf{Lemma 2.43.} Let \( F \) be an algebraic extension of \( \mathbb{Q} \), and let \( M \) be an algebraic extension of \( F \).

(i) For any prime ideal \( \mathfrak{p} \) in \( \mathcal{O}_F \) there exists a prime ideal \( \mathfrak{P} \subset \mathcal{O}_M \) such that \( \mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p} \).

(ii) Let \( \mathfrak{p} \) be a non-zero prime ideal of \( \mathcal{O}_F \) above the prime number \( p \). Then \( \mathcal{O}_F/\mathfrak{p} \) is an algebraic extension of \( \mathbb{F}_p \).

(iii) If \( M/F \) is a Galois extension, then the action of the Galois group \( G = \text{Gal}(M/F) \) on the set of primes of \( M \) lying above a prime \( \mathfrak{p} \) of \( F \) is transitive.

\textit{Proof.} Exercise 2.36

In contrast to the finite case, unique factorization of ideals fails for infinite algebraic extensions of \( \mathbb{Q} \).
CHAPTER 2. ALGEBRAIC NUMBER THEORY

Example 2.44. Consider the ring of integers \( \mathbb{Z} \) of \( \mathbb{Q} \). We will show that all prime ideals \( p \) of \( \mathbb{Z} \) satisfy \( p^2 = p \).

Let \( p \in \mathbb{Z} \) be the prime under \( p \), and \( v: \mathbb{Q} \to \mathbb{R} \cup \{ \infty \} \) the valuation corresponding to \( p \), normalized so that \( v(p) = 1 \). We will prove that the image of \( v \) equals \( \mathbb{Q} \cup \{ \infty \} \subset \mathbb{R} \cup \{ \infty \} \).

For each number field \( L \), let \( p_L = p \cap \mathfrak{O}_L \), and \( v_L = v|_L \). Then \( v_L \) is a non-normalized valuation corresponding to \( p_L \). Write \( e_L \) for the ramification index of \( p_L \) over \( p \). Then the image of \( v \) equals the union, over all number fields \( L \), of the images of the maps \( v_L \); we note that this equals \( \{ \infty \} \cup \bigcup_L \frac{1}{e_L} \mathbb{Z} = \{ \infty \} \cup \mathbb{Q} \). The square of \( p \) can be computed locally at \( \mathfrak{O}_p \). But locally we have \( \mathfrak{p} \mathfrak{O}_p = \{ x \in \mathbb{Q} \mid v(x) \geq 0 \} = \{ x \in \mathbb{Q} \mid v(x) \in \{ \infty \} \cup \mathbb{Q}_{\geq 0} \} \). This implies

\[
p^2 \mathfrak{O}_p = \{ x \in \mathbb{Q} \mid v(x) \in \{ \infty \} \cup 2 \cdot \mathbb{Q}_{\geq 0} \} = \{ x \in \mathbb{Q} \mid v(x) \in \{ \infty \} \cup 2 \cdot \mathbb{Q}_{\geq 0} \} = p \mathfrak{O}_p.
\]

Frobenius elements

Let \( F \) be a number field, let \( M \) be a (possibly infinite) Galois extension of \( F \), and let \( \mathfrak{O}_M \) be its ring of integers. Let \( \mathfrak{P} \) be a prime ideal of \( \mathfrak{O}_M \) lying over a prime ideal \( p \) of \( \mathfrak{O}_F \), and let \( k(\mathfrak{P}) = \mathfrak{O}_M / \mathfrak{P} \) and \( k(p) = \mathfrak{O}_F / p \) be the residue fields. Then \( k(p) \) is a finite field, say of cardinality \( q \). By Lemma 2.43(ii), \( k(\mathfrak{P}) \) is an algebraic extension of \( k(p) \). Let \( D_\mathfrak{P} = \{ \sigma \in \text{Gal}(M/F) \mid \sigma \mathfrak{P} = \mathfrak{P} \} \) be the decomposition group of \( \mathfrak{P} \). By reduction to the case of finite extensions, one sees that every algebraic extension of a finite field is Galois, and that we have a surjective continuous group homomorphism

\[ r: D_\mathfrak{P} \longrightarrow \text{Gal}(k(\mathfrak{P})/k(p)). \]

The right-hand side is a pro-cyclic group (either a finite cyclic group of a topological group isomorphic to \( \hat{\mathbb{Z}} \)), topologically generated by the Frobenius element \( \text{Frob}_\mathfrak{P} : x \mapsto x^q \). The kernel of \( r \) is called the \textit{inertia group} of \( \mathfrak{P} \) over \( p \), and any element in \( D_\mathfrak{P} \subseteq \text{Gal}(M/F) \) mapping to \( \text{Frob}_\mathfrak{P} \) is called a \textit{Frobenius element} at \( \mathfrak{P} \) and denoted by \( \text{Frob}_\mathfrak{P} \).

Let \( \mathfrak{p} \) be a prime of \( F \) such that the extension \( M/F \) is unramified at \( \mathfrak{p} \). Then any prime \( \mathfrak{P} \) of \( M \) lying over \( \mathfrak{p} \) determines a unique element \( \text{Frob}_\mathfrak{P} \in \text{Gal}(M/F) \). Any other prime of \( M \) over \( \mathfrak{p} \) has the form \( \sigma \mathfrak{P} \) with \( \sigma \in \text{Gal}(M/F) \), and we have \( D_{\sigma \mathfrak{P}} = \sigma D_\mathfrak{P} \sigma^{-1} \) and \( \text{Frob}_{\sigma \mathfrak{P}} = \sigma \text{Frob}_\mathfrak{P} \sigma^{-1} \). The set of all \( \text{Frob}_\mathfrak{P} \) with \( \mathfrak{P} \) a prime of \( M \) over \( \mathfrak{p} \) is therefore a conjugacy class in \( \text{Gal}(M/F) \), called the \textit{Frobenius conjugacy class} at \( \mathfrak{p} \). When no confusion is possible, any element of this conjugacy class (or even the conjugacy class itself) is denoted by \( \text{Frob}_\mathfrak{p} \).

Example 2.45. Assume \( \mathfrak{p} \) is unramified in \( F \). Then \( \mathfrak{p} \) is totally split in \( M \) if and only if the Frobenius conjugacy class at \( \mathfrak{p} \) equals the trivial conjugacy class \( \{ \text{id} \} \subseteq \text{Gal}(M/F) \).

Example 2.46. Let \( l \) be a prime number, and take \( F = \mathbb{Q} \) and \( M = \mathbb{Q}(\zeta_{l^\infty}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{l^n}) \).

We have a canonical isomorphism

\[
\mathbb{Z}_l^\times \overset{\sim}{\longrightarrow} \text{Gal}(\mathbb{Q}(\zeta_{l^\infty})/\mathbb{Q}) \quad a \mapsto (\zeta_{l^{n}} \mapsto \zeta_{l^{n}}^a \mod l^n).
\]

For every prime number \( p \neq l \), the element \( p \in \mathbb{Z}_l^\times \) is mapped to the Frobenius element at \( p \). (Note that this Frobenius element is unique because the extension is Abelian.)
Densities of sets of primes; Chebotarev’s theorem

Let $F$ be a number field, and let $P$ be the set of all prime ideals of $\mathcal{O}_F$. For any subset $S \subseteq P$, the natural density of $S$ is defined by the following limit (provided it exists):

$$d_0(S) = \lim_{X \to \infty} \frac{\# \{ p \in S \mid N(p) \leq X \}}{\# \{ p \in P \mid N(p) \leq X \}}$$

The Dirichlet density of $S$ is defined by

$$d(S) = \lim_{s \to 1} \sum_{p \in S} N(p)^{-s} - \sum_{p \in P} N(p)^{-s}$$

where the limit is taken over positive real numbers $s$ tending to 1 from above. One can show that the Dirichlet density always exists, and if the naïve density exists, then it is equal to the Dirichlet density.

**Theorem 2.47.** Let $F$ be a number field, and let $M$ be a finite Galois extension of $F$ that is unramified outside a finite set $\Sigma$ of places of $F$. Let $X$ be a subset of $G = \text{Gal}(M/F)$ that is stable under conjugation. Let $S_X$ be the set of primes $p$ of $F$ such that $p \not\in \Sigma$ and such that the Frobenius conjugacy class at $p$ is contained in $X$. Then the naïve density of $S_X$ exists and equals $\#X/\#G$.

There also exists a version for infinite extensions.

**Theorem 2.48.** Let $F$ be a number field, and let $M$ be a (possibly infinite) Galois extension of $F$ that is unramified outside a finite set $\Sigma$ of places of $F$. Let $\mu$ be the unique Haar measure on the compact group $G = \text{Gal}(M/F)$ such that $\mu(G) = 1$. Let $X$ be a subset of $G$ that is stable under conjugation and such that the boundary $\bar{X} \setminus X^0$ has measure 0. Let $S_X$ be the set of primes $p$ of $F$ such that $p \not\in \Sigma$ and such that the Frobenius conjugacy class at $p$ is contained in $X$. Then the naïve density of $S_X$ exists and equals $\mu(X)$.

### 2.5 Adèles and idèles

We will now “unify” the various completions of a number field $F$ by introducing the adèle ring of $F$. This is a topological ring $\mathbb{A}_F$ that admits every completion $F_v$ as a quotient, but behaves in a more civilised way than the product $\prod_v F_v$ of topological rings. For example, $\mathbb{A}_F$ is locally compact, while $\prod_v F_v$ is not.

The unit group $\mathbb{A}_F^\times$ of $\mathbb{A}_F$ deserves a careful study of its own. It is a fundamental object in the modern formulation of class field theory. Likewise, its non-commutative generalisations $\text{GL}_n(\mathbb{A}_F)$ (note that $\mathbb{A}_F^\times = \text{GL}_1(\mathbb{A}_F)$) play a central role in the modern theory of automorphic forms, and hence in the Langlands programme.

**The adèle ring of $\mathbb{Q}$**

We start by looking at the case $F = \mathbb{Q}$. We define the ring of finite adèles $\mathbb{A}_\mathbb{Q} = \mathbb{A}_\mathbb{Q}^\infty$ as the tensor product $\mathbb{A}^\infty = \mathbb{Q} \otimes \mathbb{Z}[\hat{\mathbb{Z}}]$, where we view $\mathbb{Q}$ and $\mathbb{Z}[\hat{\mathbb{Z}}]$ as $\mathbb{Z}$-modules. Like any tensor product of commutative rings, $\mathbb{A}^\infty$ inherits a multiplication map, given explicitly by

$$\left( \sum_{i=1}^n q_i \otimes z_i \right) \cdot \left( \sum_{j=1}^m q'_j \otimes z'_j \right) = \sum_{i,j} q_i q'_j \otimes z_i z'_j$$
for all $\sum_{i=1}^n q_i \otimes z_i$ and $\sum_{j=1}^m q'_j \otimes z'_j$ in $\mathbb{A}^\infty$.

The ring $\mathbb{A}^\infty$ is equipped with the strongest topology such that the map

$$\mathbb{Q} \times \hat{\mathbb{Z}} \longrightarrow \mathbb{A}^\infty$$

$$(x, z) \longmapsto x + z$$

is continuous, where $\mathbb{Q}$ is given the discrete topology. More concretely, the subsets of the form

$$U_{x, y} = x \cdot \hat{\mathbb{Z}} + y \subset \mathbb{A}^\infty \text{ with } x \in \mathbb{Q}^\times \text{ and } y \in \mathbb{Q}$$

form a basis for the topology on $\mathbb{A}^\infty$. This definition implies that $\mathbb{A}^\infty$ is a locally profinite topological ring containing $\hat{\mathbb{Z}}$ as an open subring.

**Definition 2.49.** The ad`ele ring $\mathbb{A} = \mathbb{A}_\mathbb{Q}$ is the product ring $\mathbb{A}^\infty \times \mathbb{R}$, equipped with the product topology.

**The ad`ele ring as a restricted product**

In many texts the ring $\mathbb{A}$ is introduced as a “restricted product” ranging over all prime numbers $p$, of the fields $\mathbb{Q}_p$ with respect to the subrings $\mathbb{Z}_p \subset \mathbb{Q}_p$. This restricted product arises from the following computation. Observe first that we can view $\mathbb{Q}$ as the inductive limit $\mathbb{Q} = \lim_{\rightarrow} \mathbb{Z}[1/N]$.

Using this, we compute

$$\left( \lim_{N \in \mathbb{Z}^+} \mathbb{Z}[1/N] \right) \otimes \hat{\mathbb{Z}} = \lim_{N \in \mathbb{Z}^+} \left( \mathbb{Z}[1/N] \otimes \hat{\mathbb{Z}} \right) = \lim_{N \in \mathbb{Z}^+} \left( \prod_{p \mid N} \mathbb{Q}_p \times \prod_{p \nmid N} \mathbb{Z}_p \right). \quad (2.4)$$

For each $N$, we embed $\prod_{p \mid N} \mathbb{Q}_p \times \prod_{p \nmid N} \mathbb{Z}_p \subset \prod_{p \text{ prime}} \mathbb{Q}_p$. Hence, $\mathbb{A}^\infty$ equals the so called *restricted product*

$$\prod_{p \text{ prime}}' (\mathbb{Q}_p, \mathbb{Z}_p) = \left\{ (\alpha_p) \in \prod_{p \text{ prime}} \mathbb{Q}_p \mid \text{ for almost all primes } p \text{ we have } x_p \in \mathbb{Z}_p \right\}.$$

A basis for the topology on the restricted product is given by the sets

$$U_{x, y} = \left\{ (\alpha_p) \in \mathbb{A}^\infty \mid v_p(\alpha_p - y) \geq v_p(x) \right\}$$

with $x \in \mathbb{Q}^\times$ and $y \in \mathbb{Q}$.

The full ad`ele ring is obtained from $\mathbb{A}^\infty$ by attaching a component for the infinite place as well. As a restricted product, we have

$$\mathbb{A} = \prod_{Q\text{-places } v} (\mathbb{Q}_v : \mathbb{Z}_v)$$

where for $v = \infty$, we take by definition $\mathbb{Z}_v = \mathbb{Q}_v = \mathbb{R}$. 
CHAPTER 2. ALGEBRAIC NUMBER THEORY

The adèle ring of a number field

If \( F \) is a number field, the analogue of \( \hat{\mathbb{Z}} \) is the ring of \( \text{profinite} \ F \)-integers, \( \hat{\mathcal{O}}_F = \hat{\mathbb{Z}} \otimes \mathcal{O}_F = \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \mathcal{O}_F/N \mathcal{O}_F = \varprojlim_{I \subset \mathcal{O}_F} \mathcal{O}_F/I \), where \( I \) ranges over all the non-zero ideals of \( \mathcal{O}_F \). As before, we define the ring of \( \text{finite} \ F \)-adèles by \( \mathbb{A}_\infty^F = F \otimes \hat{\mathcal{O}}_F \), where the topology is the strongest such that the map

\[
F \times \hat{\mathcal{O}}_F \rightarrow \mathbb{A}_\infty^F
\]

\[
(x, z) \mapsto x + z
\]

is continuous. Then \( \mathbb{A}_\infty^F \) is a locally profinite topological ring containing \( \hat{\mathcal{O}}_F \subset \mathbb{A}_\infty^F \) as an open subring. The ring of \( \mathbb{F} \)-adèles is then defined by

\[
\mathbb{A}_F = \left( F \otimes \mathbb{Q} \right) \times \mathbb{A}_\infty^F.
\]

Lemma 2.50.

1. The topological ring \( \mathbb{A}_F \) is a locally compact Hausdorff space.

2. The topology on \( F \) induced from \( \mathbb{A}_F \) is the discrete topology.

3. The subset \( F \) is closed in \( \mathbb{A}_F \).

4. The quotient \( \mathbb{A}_F/F \) is compact.

Proof. For simplicity, we do the case \( F = \mathbb{Q} \); the general case is left as an exercise.

To prove (1), we start by showing that \( \mathbb{A}_\infty^F \) is Hausdorff. Let \( \alpha, \beta \) be two distinct points of \( \mathbb{A}_\infty^F \). For \( N \in \mathbb{Z}_{\geq 1} \) sufficiently large, the points \( N\alpha \) and \( N\beta \) lie in \( \hat{\mathbb{Z}} \subset \mathbb{A}_\infty^F \). Because \( \hat{\mathbb{Z}} \) is profinite and hence Hausdorff, there exist open subsets \( U, V \subset \hat{\mathbb{Z}} \) with \( N\alpha \in U, N\beta \in V \) and \( U \cap V = \emptyset \). Then \( \frac{1}{N}U, \frac{1}{N}V \) have this property for \( \alpha, \beta \). Hence \( \mathbb{A}_\infty^F \) is Hausdorff. Since \( \mathbb{R} \) is also Hausdorff, the space \( \mathbb{A} = \mathbb{R} \times \mathbb{A}_\infty^F \) is a product of two Hausdorff spaces and is therefore also Hausdorff.

We now check local compactness of \( \mathbb{A} \). For all \( x \in \mathbb{Q}^\times \) and \( y \in \mathbb{Q} \), we consider the open subset \( U_{x,y} = \hat{\mathbb{Z}}x + y \subset \mathbb{A}_\infty^F \). The sets \( U_{x,y} \) form a basis for the topology on \( \mathbb{A}_\infty^F \) and are compact, so \( \mathbb{A}_\infty^F \) is locally compact. Since \( \mathbb{R} \) is also locally compact, the space \( \mathbb{A} = \mathbb{R} \times \mathbb{A}_\infty^F \) is a product of two locally compact spaces and is therefore also locally compact.

For (2), we observe that \( U = (-1, 1) \times \hat{\mathbb{Z}} \subset \mathbb{A} \) is open and \( U \cap \mathbb{Q} = \{0\} \). Hence the point 0 is open for the topology on \( \mathbb{Q} \) induced from \( \mathbb{A}_\mathbb{Q} \). By translating \( U \) with elements of \( \mathbb{Q} \), we see similarly that every point in \( \mathbb{Q} \) is open for the topology induced from \( \mathbb{A}_\mathbb{Q} \).

Claim (3) follows from (2) and the (easily verified) fact that every discrete subspace of a Hausdorff space is closed.

Finally, to prove (4), we consider the compact subset \([-1, 1] \times \hat{\mathbb{Z}} \subset \mathbb{A} \). It is left as an exercise to show that this surjects onto \( \mathbb{A}/\mathbb{Q} \) (Exercise 2.52).
Partial adèle rings: omitting a set of places

It is often convenient to look at adèle rings where certain places are excluded from the products. A fairly standard notation is the following. Let $\Sigma_1, \Sigma_2$ be two sets of places of $F$. Then we define

$$A_{F, \Sigma_1} \overset{\text{def}}{=} \prod_{v \in \Sigma_1} (F_v : \mathcal{O}_{F_v}),$$

$$A_{\Sigma_2} \overset{\text{def}}{=} \prod_{v \notin \Sigma_2} (F_v : \mathcal{O}_{F_v}),$$

so sets in the superscript denote “excluded places” and sets in the subscript denote “included places”. For instance, this explains the notation $A_\infty^{\infty} \mathbb{Q}$ for the finite adèles of $\mathbb{Q}$.

**Example 2.51.** Let $q$ be a prime number. Then $A_{\infty, q} \mathbb{Q}$ denotes the ring of finite adèles away from the prime number $q$. It is canonically isomorphic to the quotient of $A_{\mathbb{Q}}$ by the ideal $\mathbb{R} \times \mathbb{Q}_q$ (note: not a subring of $A_{\mathbb{Q}}$).

The idèle group

If $(R, \mathcal{T})$ is a topological ring, its unit group $R^\times$ is equipped with a canonical topology $\mathcal{T}^\times$ making $R^\times$ into a topological group. One way to define $\mathcal{T}^\times$ is as the subspace topology induced from the injection

$$R^\times \to R \times R,$$

$$x \mapsto (x, x^{-1}),$$

where $R \times R$ is equipped with the product topology. Equivalently, $\mathcal{T}^\times$ is the weakest topology on $R^\times$ for which both the inclusion $R^\times \to R$ and the inversion map $R^\times \to R^\times$ are continuous.

**Remark 2.52.** The topology $\mathcal{T}^\times$ is a refinement of the subspace topology from $R$; it may or may not be a strict refinement. If $F$ is a local field, then the topology on $F^\times$ is just the subspace topology from $F$; see Exercise 2.55. On the other hand, the topology on $A_F^\times$ (see below) is strictly finer than the subspace topology from $A_F$.

**Definition 2.53.** The group of finite idèles of a number field $F$ is defined as the unit group $A_{\infty, F}$ of $A_{\infty, F}$. Similarly, the group of idèles, or idèle group, of $F$ is defined as the unit group $A_F^\times$ of $A_F$.

We view $A_{\infty, F}^\times$ and $A_F^\times$ as topological groups equipped with the topology defined above. As a restricted product, we have

$$A_{\infty, F}^\times = \prod_{\text{finite } F\text{-places } v} (F_v^\times : \mathcal{O}_{F_v}^\times).$$

It is not hard to check that there is a canonical isomorphism

$$A_F^\times \cong (F \otimes_{\mathbb{Q}} \mathbb{R})^\times \times A_{\infty, F}^\times.$$

of topological groups.

Recall that for every place $v$ of $F$ we have a local norm

$$|\cdot|_{F_v} : F_v^\times \to \mathbb{R}_{>0}.$$
CHAPTER 2. ALGEBRAIC NUMBER THEORY

The adèlic norm $|\cdot|=|\cdot|_{\mathbb{A}_F}$ on $\mathbb{A}_F^\times$ is the product over all the local norms:

$$|\cdot|_{\mathbb{A}_F} : \mathbb{A}_F^\times \to \mathbb{R}_{>0}$$

$$(x_v) \mapsto \prod_v |x_v|_{F_v},$$

where $v$ runs over the set of all places of $F$. Note that this product is well defined because $|x_v|_{F_v} = 1$ for all but finitely many $v$.

In Exercise 2.48, you will prove the product formula for the adèlic norm $|\cdot|_{\mathbb{A}_F}$, i.e. $|x|_{\mathbb{A}_F} = 1$ for all principal idèles $x \in F^\times \subset \mathbb{A}_F^\times$.

Class groups and idèle class groups

Recall from algebraic number theory the notion of fractional $\mathcal{O}_F$-ideals. By definition these are the non-zero $\mathcal{O}_F$-submodules $I \subset F$ such that for some $x \in F^\times$ we have $xI \subset \mathcal{O}_F$. The principal fractional ideals are then those submodules that are generated by an element of $F^\times$. The class group of $F$ is then the set of fractional $\mathcal{O}_F$-ideals modulo the set of principal ideals of $F$. This class group is finite for all $F$. In Exercise 2.59, we show that $\mathbb{A}_F^\times\mathbb{A}_F / F^\times \hat{\mathcal{O}}_F = \text{Class group } F$.

In the modern formulation of class field theory, one introduces the idèle class group, which is the locally compact topological group

$$C_F = F^\times \backslash \mathbb{A}_F^\times.$$ 

The above isomorphism describes the class group as a quotient of the idèle class group $C_F$ by an closed subgroup of finite index.

**Remark 2.54.** In the notation for the quotient $F^\times \backslash \mathbb{A}_F^\times$, we have written the quotient by $F^\times$ on the left. Because $\mathbb{A}_F^\times$ is commutative, we could just as well have written this quotient as $\mathbb{A}_F^\times / F^\times$. However, writing the subgroup on the left is more consistent in the non-commutative setting; there one encounters quotients such as $\text{GL}_2(F) / \text{GL}_2(\mathbb{A}_F)$, in which there is a difference with the corresponding quotient on the right.

Weak and strong approximation

Let $\Omega$ be the set of all places of $\mathbb{Q}$.

Let $X$ be an (affine or projective) algebraic variety over $\mathbb{Q}$ (or more generally a global field). We have injective maps

$$X(\mathbb{Q}) \subseteq X(\mathbb{A}) \subseteq \prod_{v \in \Omega} X(\mathbb{Q}_v)$$

of topological spaces; here $X(\mathbb{Q})$ is equipped with the discrete topology, $X(\mathbb{Q}_v)$ with the $v$-adic topology, $X(\mathbb{A})$ with the restricted product topology, and $\prod_{v \in \Omega} X(\mathbb{Q}_v)$ with the product topology. (Defining the topology on $X(\mathbb{A})$ for general varieties $X$ requires discussing integral models. We will not do this here, since in the particular cases that we are interested in, there is an “obvious” notion of integral points.)
Note that both of the above inclusions are continuous, but the topology on \( X(\mathbb{A}) \) is in general finer than the subspace topology inherited from \( \prod_{v \in \Omega} X(\mathbb{Q}_v) \). However, if the variety \( X \) is projective, then \( X(\mathbb{Z}_v) \) is equal to \( X(\mathbb{Q}_v) \) for every finite place \( v \), and consequently the topological spaces \( X(\mathbb{A}) \) and \( \prod_{v \in \Omega} X(\mathbb{Q}_v) \) can be identified.

We say that \( X \) satisfies \textit{weak approximation} if (the image of) \( X(\mathbb{Q}) \) is a dense subspace of \( \prod_{v \in \Omega} X(\mathbb{Q}_v) \). In other words \( X \) satisfies weak approximation if and only if every non-empty open subset of \( \prod_{v \in \Omega} X(\mathbb{Q}_v) \) contains a rational point. Because of the definition of the product topology, this is equivalent to saying that for every finite subset \( S \subset \Omega \), the subset \( X(\mathbb{Q}) \) is dense in \( \prod_{v \in S} X(\mathbb{Q}_v) \).

We say that \( X \) satisfies \textit{strong approximation} if \( X(\mathbb{Q}) \) is dense in \( X(\mathbb{A}) \) equipped with the restricted product topology.

Note that if \( X \) satisfies strong approximation, then \( X \) also satisfies weak approximation because the inclusion map from \( X(\mathbb{A}) \) to \( \prod_{v \in \Omega} X(\mathbb{Q}_v) \) is continuous with dense image. However, the converse does not hold; since the topology on \( X(\mathbb{A}) \) is finer than the subspace topology inherited from \( \prod_{v \in \Omega} X(\mathbb{Q}_v) \), the closure of \( X(\mathbb{Q}) \) in \( X(\mathbb{A}) \) is in general smaller than the intersection of \( X(\mathbb{A}) \) with the closure of \( X(\mathbb{Q}) \) in \( \prod_{v \in \Omega} X(\mathbb{Q}_v) \).

Example 2.55. The affine line satisfies weak approximation but not strong approximation: \( \mathbb{Q} \) is dense in \( \prod_{v \in \Omega} \mathbb{Q}_v \), but is discrete as a subspace of \( \mathbb{A} \). For example, there are no rational numbers \( x \) satisfying \( |x|_v \leq 1 \) for all finite places \( v \) and \( |x - 1/2|_\infty < 1/2 \).

There are analogous notions “away from a fixed set of places”. If \( \Sigma \) is any subset of \( \Omega \), then \( X \) satisfies \textit{weak approximation away from} \( \Sigma \) if \( X(\mathbb{Q}) \) is dense in \( \prod_{v \in \Omega \setminus \Sigma} X(\mathbb{Q}_v) \), and \( X \) satisfies \textit{strong approximation away from} \( \Sigma \) if \( X(\mathbb{Q}) \) is dense in \( X(\mathbb{A}^{\Sigma}) \) (defined in the same way as \( X(\mathbb{A}) \) but using the set of places \( \Omega \setminus \Sigma \) instead of \( \Omega \)).

\textbf{Dirichlet characters and Hecke characters, revisited}

We will now take a closer look at characters in the adèlic setting.

By Exercise 2.61, there is a canonical isomorphism

\[
\mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times \overset{\sim}{\longrightarrow} \mathbb{Q}^\times \setminus \mathbb{A}^\times
\]

of topological groups. If \( \chi: (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \mathbb{C}^\times \) is a Dirichlet character modulo some positive integer \( n \), then \( \chi \) induces a continuous group homomorphism

\[
\hat{\mathbb{Z}}^\times \rightarrow \mathbb{C}^\times
\]

\[
u \mapsto \chi(u \mod n).
\]

In view of the isomorphism \([2.5]\), it is natural to extend this to a continuous group homomorphism

\[
\mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times \rightarrow \mathbb{C}^\times
\]

\[
(t, u) \mapsto t^s \cdot \chi(a \mod n)
\]

where \( s \in \mathbb{C} \) can be chosen freely. Finally, we can use \([2.5]\) to identify this with a homomorphism

\[
\omega_{\chi,s}: \mathbb{A}^\times \rightarrow \mathbb{C}^\times
\]

that is trivial when restricted to \( \mathbb{Q}^\times \).
Definition 2.56. Let $F$ be a number field. A Hecke character for $F$ is a continuous group homomorphism
\[ \omega : \mathbb{A}_F^\times \to \mathbb{C}^\times \]
that is trivial on the subgroup $F^\times$ of $\mathbb{A}_F^\times$.

2.6 Class field theory

Let $\mathbb{Q}(\mu_\infty) = \lim_{\leftarrow n \geq 1} \mathbb{Q}(\mu_n)$ be the (infinite) algebraic extension of $\mathbb{Q}$ obtained by adjoining all roots of unity. Recall that there exist canonical isomorphisms
\[ (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \quad \text{for all } n \geq 1, \]
and hence a canonical isomorphism
\[ \hat{\mathbb{Z}}^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}). \]

In particular, $\mathbb{Q}(\mu_\infty)$ is an Abelian extension of $\mathbb{Q}$. By the famous Kronecker–Weber theorem, every Abelian extension of $\mathbb{Q}$ can be embedded into $\mathbb{Q}(\mu_\infty)$. It turns out that for general number fields, the description of all Abelian extensions is much more involved; for this reason, class field theory was developed.

Let $F$ be a number field, let $\bar{F}$ be an algebraic closure of $F$, and let $G = \mathrm{Gal}(\bar{F}/F)$. The commutator subgroup of $G$ is the closed subgroup $[G, G] \subseteq G$ (topologically) generated by all commutators $[g, h] = ghg^{-1}h^{-1}$ with $g, h \in G$. The Abelianisation of $G$ is the quotient
\[ G^{\text{ab}} = G/[G, G] \]
of topological groups. There is a unique maximal extension $F^{\text{ab}}$ of $F$ inside $\bar{F}$ that is Abelian over $F$; it is called the maximal Abelian extension of $F$ and equals the fixed field of $[G, G]$ inside $\bar{F}$. Galois theory gives an isomorphism
\[ G^{\text{ab}} \xrightarrow{\sim} \mathrm{Gal}(F^{\text{ab}}/F). \]

The aim of class field theory is to describe $F^{\text{ab}}$ and $G^{\text{ab}}$ in terms of “data coming from $F$”. In modern terms, the relevant object is the idèle class group introduced earlier.

Theorem 2.57 (Main theorem of class field theory). Let $F$ be a number field.

1. There is a canonical inclusion-reversing bijection between the partially ordered set of finite Abelian extensions of $F$ (inside $\bar{F}$) and the partially ordered set of closed subgroups of finite index in $C_F$.

2. If $L$ is a finite Abelian extension of $F$ and $N_L$ is the corresponding closed subgroup of finite index in $C_F$, then there is a canonical isomorphism
\[ C_F/N_L \xrightarrow{\sim} \mathrm{Gal}(L/F). \]

As a consequence, one obtains a canonical isomorphism
\[ C_F/U_F \xrightarrow{\sim} \mathrm{Gal}(F^{\text{ab}}/F). \]
of topological groups, where $U_F$ is the intersection of all closed subgroups of finite index in $C_F$.

One possible choice for a closed subgroup of finite index is the image of $(F \otimes \mathbb{Q})^\times \times \hat{O}_F^\times$ in $C_F$. The corresponding finite Abelian extension of $F$ is the Hilbert class field $H_F$ of $F$. This is the maximal unramified Abelian extension of $F$ (where the extension $\mathbb{C}/\mathbb{R}$ is regarded as being ramified for this purpose). The Galois group $\text{Gal}(H_F/F)$ is canonically isomorphic to the ideal class group of $F$; see Exercise 2.62. Another choice is the smaller subgroup where at the real places one only takes the subgroup of positive elements; this gives rise to the narrow Hilbert class field of $F$, the maximal Abelian extension that is unramified at all finite places.

Example 2.58. The imaginary quadratic field $K = \mathbb{Q}(\sqrt{-15})$ has discriminant $-15 = -3 \cdot 5$. The field $H = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ is an unramified quadratic extension of $K$, and can in fact be shown to be the Hilbert class field of $K$.

Example 2.59. The Hilbert class field of $K = \mathbb{Q}(\sqrt{-23})$ is $H_K = K(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$. In this example the description of $H_K$ is harder to “guess” than in the previous example. However, there exists a general method to determine Hilbert class fields (and other Abelian extensions) of imaginary quadratic fields, namely the theory of complex multiplication.

Example 2.60. Let $K$ be the cubic field $\mathbb{Q}(\alpha)$ of discriminant $-3299$, where $\alpha^3 - \alpha^2 + 9\alpha - 8 = 0$. The Hilbert class field of $K$ is $H_K = K(\beta)$, where $\beta^3 - (\alpha + 1)\beta - 1 = 0$. To “guess” $H_K$ in cases of this kind, one can use the (as yet unproved) Stark conjectures.

2.7 Exercises

Profinite groups

Exercise 2.1. Show that a group object in the category of groups $\text{Grp}$ is an abelian group, in the following sense. Let $A$ be an abelian group. Then, notice that, $m: A \times A \to A$ and $i: A \to A$ are morphisms of groups, and hence $(A, m, i)$ is a group object in $\text{Grp}$. Show that all group objects in $\text{Grp}$ are of this form.

Exercise 2.2. Let $Y$ be a projective limit of a projective system of topological spaces $(Y_i)_{i \in I}$. Let $X$ be a topological space, and $f: X \to Y$ be a continuous morphism. Show that if for every $i \in I$ the composition $X \to Y \to Y_i$ is surjective, then $f$ has dense image.

Exercise 2.3. Show that in the category of topological spaces, a projective limit of compact Hausdorff spaces is non-empty.

Exercise 2.4. Let $X$ be a topological space. Show that $X$ is homeomorphic to a projective limit of finite discrete spaces if and only if $X$ is Hausdorff, compact and totally disconnected.

Exercise 2.5. Let $G$ be a topological group. Show that $G$ is totally disconnected and locally compact (i.e. “locally profinite”) if and only if there exists an open profinite subgroup $K \subset G$.

Exercise 2.6. (a) Show that the only continuous group homomorphism from $\hat{\mathbb{Z}}$ to the additive group of $\mathbb{C}$ is the trivial homomorphism.
(b) Show that every continuous group homomorphism $\hat{\mathbb{Z}} \to \mathbb{C}^\times$ has finite image.

(c) Let $p$ be a prime number. Show that the only continuous group homomorphism from $\mathbb{Q}_p$ to the additive group of $\mathbb{C}$ is the trivial homomorphism.

(d) Let $p$ be a prime number. Show that the image of a continuous group homomorphism $\mathbb{Q}_p \to \mathbb{C}^\times$ is either trivial or infinite, and give an example of the second case.

**Exercise 2.7.** Let $k$ be a commutative ring.

(a) Give the $k$-algebra $R$ over $k$ such that $\text{Spec}(R) = \mathbb{G}_{m,k} \times_k \mathbb{G}_{m,k}$.

(b) The multiplication mapping $m: \text{Spec}(R) \to \mathbb{G}_{m,k}$ induces on global sections a mapping $k[X^\pm 1] \to R$; describe this map explicitly.

(c) Compute the endomorphism ring $\text{End}_{k,\text{Grp}}(\mathbb{G}_{m,k})$.

If you are unfamiliar with schemes, you may assume $k$ is an algebraically closed field (or even $k = \mathbb{C}$).

**Exercise 2.8.** Let $G$ be a topological group.

(a) Let $H \subset G$ be an open subgroup. Show that $H$ is also closed.

(b) Show that the converse does not hold by giving an example of a closed subgroup that is not open.

(c) Assume $G$ is compact. Show that any open subgroup $H$ of $G$ contains an open normal subgroup.

Now assume that $G$ is profinite.

(a) Show that any open subgroup has finite index.

(b) Show that any continuous morphism $\rho: G \to \text{GL}_n(\mathbb{C})$ has finite image.

**Exercise 2.8.1.** Let $\rho$ be as in the previous exercise. Show that any $\rho: G \to \text{GL}_n(\mathbb{C})$ has up to conjugation image in $\text{GL}_n(F)$ where $F \subset \mathbb{C}$ is some number field.

**Hint:** Some prior knowledge on representation theory is useful for this question. You can use that for any algebraically closed field $k$ of characteristic 0, and any finite group $H$, the group algebra $k[H]$ is isomorphic to a product of matrix algebras.

**Exercise 2.9.** Let $G$ be locally profinite group.

(a) Let $C^\infty_c(G)$ be the space of locally constant functions $f: G \to \mathbb{C}$ that are compactly supported. Show that there exists an, up to scalar unique, non-trivial linear functional $\mu: C^\infty_c(G) \to \mathbb{C}$ that is invariant under left translation by $G$, i.e. $\mu \in C^\infty_c(G)^* = \text{Hom}_\mathbb{C}(C^\infty_c(G), \mathbb{C})$ is such that for all $f \in C^\infty_c(G)$ and all $g \in G$ we have $\mu(f) = \mu(\overline{g}f)$ where $\overline{g}f$ is the function $x \mapsto f(g^{-1}x)$.

(b) The functional $\mu$ is the left Haar measure of $G$. We write $\int_G f \, d\mu$ for $\mu(f)$. The group $G$ is called unimodular if $\mu$ is invariant under right translations. Give an example of a locally profinite group which is unimodular, and one which is not.
Exercise 2.10. Let $G$ be a profinite group and $\rho: G \to \text{GL}_n(\mathbb{Q}_\ell)$ be a continuous morphism. Show that $\rho$ has up to conjugation image in the group $\text{GL}_n(\mathbb{Z}_\ell)$.

Exercise 2.11. Let $G$ be a profinite group of pro-order prime to $\ell$, i.e. $G$ is isomorphic to a projective limit of finite groups that are of order prime to $\ell$. Show that any continuous morphism $G \to \text{GL}_n(\mathbb{Q}_\ell)$ has finite image.

Exercise 2.12. Let $G$ be a profinite group and $\rho: G \to \text{GL}_n(\mathbb{Q}_\ell)$ be a continuous morphism. Show that $\rho$ has, up to conjugation, image in $\text{GL}_n(\mathbb{F}_\ell)$ where $\mathbb{F}_\ell \subset \mathbb{Q}_\ell$ is a finite extension of $\mathbb{Q}_\ell$.

Exercise 2.13. Let $p$ be a prime number. Consider the group $\text{SL}_2(\mathbb{Z}_p)$ of invertible $2 \times 2$-matrices
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]
with coefficients in $\mathbb{Z}_p$, such that $ad - bc = 1$. We give $\text{SL}_2(\mathbb{Z}_p)$ a topology by pulling back the product topology on $\text{M}_2(\mathbb{Z}_p)$ via the injection $\text{SL}_2(\mathbb{Z}_p) \hookrightarrow \text{M}_2(\mathbb{Z}_p)$, $g \mapsto (g, g - 1)$.

(a) Show that the group $\text{SL}_2(\mathbb{Z}_p)$ is profinite.

(b) Show that we have an isomorphism $\text{SL}_2(\mathbb{Z}_p) \cong \lim_{\leftarrow} \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

(c) Show that the mapping $\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}_p)$ does not have dense image. Show that the mapping $\text{GL}_2(\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}_p)$ does not have dense image.

Exercise 2.14. Let $\{G_i, i \in I, \leq\}$ be a filtered projective system of groups, so where $I$ is an index set that is partially ordered by $\leq$, and where for each $i \in I$ we have a finite group $G_i$, and for each pair of indices $i, j \in I$ with $i \leq j$ we have a surjection $f_{ji}: G_j \to G_i$. We require that for all inequalities of the form $i \leq j \leq k$ in $I$ we have that $f_{ki} = f_{ji} \circ f_{kj}$, and for all $i \in I$ that $f_{ii} = \text{Id}_{G_i}$.

(a) Show that the projective limit $G = \lim_{\leftarrow} G_i$ is either finite or uncountably infinite.

(b) Show that as a topological space, $\mathbb{Z}_2$ is isomorphic to the Cantor set.

Infinite Galois Theory

Exercise 2.15. Show that any profinite group $G$ arises as the Galois group of some, possibly infinite, Galois extension $L/F$ of fields.

Exercise 2.16. Consider the set $S$ of formal products $x = \prod_{p \text{ prime}} p^{n_p}$, where $n_p \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

(a) Show that the set $S$ parametrizes naturally the (algebraic) extensions $M \subset \overline{\mathbb{F}_q}$ of $\mathbb{F}_q$.

(b) Let $x, y \in S$ and $M_x, M_y \subset \overline{\mathbb{F}_q}$ be the corresponding fields. Express in terms of $x, y$ when $M_x$ is a subfield of $M_y$, and determine in this case the profinite group $\text{Gal}(M_y/M_x)$.

Exercise 2.17. Show that the topologies defined in (2.2) and (2.3) are equivalent.

Exercise 2.18. Let $L/M/F$ be (possibly infinite) Galois extensions of the number field $F$. Show that the mapping $\text{Gal}(L/F) \to \text{Gal}(M/F)$ is surjective.
Exercise 2.19. In the spirit of Grothendieck, there is a more categorical way to formulate Galois theory (Theorem 2.15): Let $F$ be an algebraic field with absolute Galois group $G = \text{Gal}(\overline{F}/F)$. Define

$$C_F = \text{The category of } F\text{-algebras } M \text{ such that every element } x \in M \text{ satisfies } f(x) = 0 \text{ for some separable polynomial } f \in F[X].$$

G-spaces = The category of compact, totally disconnected topological spaces $X$ that are equipped with a continuous $G$-action, and the space of orbits $X/G$ is finite.

Let $X$ be a $G$-space. Write $\text{Map}(X, F)$ for the $F$-algebra of continuous functions $X \to F$ with pointwise addition and pointwise multiplication. The group $G$ acts on $\text{Map}(X, F)$ by translation on the functions $g(f) = (x \mapsto f(g^{-1}x)) \ (g \in G, f \in \text{Map}(X, F))$. Use Theorem 2.15 to show that the functor $C_F \to G\text{-spaces}, M \mapsto \text{Hom}_F(M, F)$ is quasi-inverse to the functor that assigns the algebra of invariant functions $\text{Map}(X, F)$ to the $G$-set $X$.

Exercise 2.20. Let $p_1, p_2, p_3, \ldots \in \mathbb{Z}_{\geq 1}$ be the (infinite) list of all the (positive) prime numbers in $\mathbb{Z}$. Consider the extension $M = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots)$ of $\mathbb{Q}$ obtained by adjoining square roots $\sqrt{p_1}, \sqrt{p_2}, \ldots$, of the prime numbers.

(a) Explain that $M$ is an infinite Galois extension and determine its Galois group $\text{Gal}(M/\mathbb{Q})$ as a profinite group. (Hence, also determine its topology!).

(b) Show that the group $\text{Gal}(M/\mathbb{Q})$ has uncountably many subgroups of index 2 that are not closed for its topology.

(c) Explain that in the statement of infinite Galois theory, one cannot remove the condition that the subgroups are closed.

Local fields


Exercise 2.22. Let $L/F$ be a finite Galois extension of $p$-adic fields. Show that for all $x \in L$ and all $\sigma \in \text{Gal}(L/F)$ we have $|\sigma(x)| = |x|$.

Exercise 2.23. Consider the power series ring $R = \mathbb{R}[[T]]$. Show that there exist an element $\sqrt{1 + T} \in R$ whose square is $1 + T \in R$.

Exercise 2.24. Let $F$ be a topological field of characteristic 0 with non-discrete topology. Show that $F$ is a $p$-adic field if and only if it is locally profinite.

Exercise 2.25. Let $v$ be a (finite or infinite) place of $\mathbb{Q}$. Show that any field automorphism $\sigma \in \text{Aut}_{\text{fields}}(\mathbb{Q}_v)$ is automagically continuous. Deduce that $\text{Aut}_{\text{fields}}(\mathbb{Q}_v) = 1$.

Hint: Try to characterize the topology by some algebraic property. For the $p$-adic fields $\mathbb{Q}_p$ show that $|\sigma|_p = 1$ if and only if $\sigma$ has an $m$-th root in $\mathbb{Q}_p$ for all positive integers $m$ prime to $p(p - 1)$.

Exercise 2.26. Show that Theorem 2.28 implies Proposition 2.27.
Exercise 2.27. On page 58 we computed the higher ramification groups $\text{Gal}(\mathbb{Q}_p(\zeta_p, \sqrt[3]{c})/\mathbb{Q}_p)_i$ for all (odd) prime numbers $p$. The goal of this exercise is to generalize this computation to $\mathbb{Q}_p(\zeta_p, \sqrt[3]{c})$ for all $c \in \mathbb{Z}_p, c \neq 0$.

(a) Assume $v_p(c) = 0$ and $[\mathbb{Q}_p(\zeta_p, \sqrt[3]{c}) : \mathbb{Q}_p] = p(p - 1)$. Show that the ramification filtration on $\text{Gal}(\mathbb{Q}_p(\zeta_p, \sqrt[3]{c})/\mathbb{Q}_p)$ is

$$G_i \ F_p \times F_p^\times \ F_p \times F_p^\times \ F_p \ 0$$

(b) Assume $0 < v_p(c) < p$. Show that the ramification filtration on $\text{Gal}(\mathbb{Q}_p(\zeta_p, \sqrt[3]{c})/\mathbb{Q}_p)$ is

$$G_i \ F_p \times F_p^\times \ F_p \times F_p^\times \ F_p \ 0$$

(c) Give an explicit necessary and sufficient condition on $p$, similar to the one we found when $c = 2$ that predicts when $[\mathbb{Q}_p(\zeta_p, \sqrt[3]{c}) : \mathbb{Q}_p] = p - 1$.

Exercise 2.28. Give an example of a prime number $p$ such that $\sqrt[3]{15} \in \mathbb{Q}_p$.

Hint: You may want to use a computer for this, because the smallest such prime number $p$ is larger than 25000.

Exercise 2.29. Let $p = 3$. Find a uniformizer of the field $\mathbb{Q}_p(\zeta_p^2, \sqrt[3]{2})$.

Exercise 2.30. Recall the conjecture that any finite group arises as a Galois group of a Galois extension of $\mathbb{Q}$. In contrast, explain that over $\mathbb{Q}_p$ the Galois group of a finite Galois extension is always solvable and moreover give an example of a finite solvable group $G$ such that for all prime numbers $p$ and all finite Galois extensions $F/\mathbb{Q}_p$ we have $G \neq \text{Gal}(F/\mathbb{Q}_p)$.

Exercise 2.31. Determine all prime numbers $p$ such that $\mathbb{Q}_p$ has a finite Galois extension $F/\mathbb{Q}_p$ whose Galois group is the symmetric group $S_4$. You may use the fact that the polynomial $f = x^4 - 2x + 2$ has Galois group $S_4$ over $\mathbb{Q}_2$.

Exercise 2.32. Give an example of a prime number $p$, two totally ramified extensions $M_1, M_2$ of $\mathbb{Q}_p$ both contained in a fixed algebraic closure $\overline{\mathbb{Q}_p}$, such that the compositum $M_1M_2 \subset \overline{\mathbb{Q}_p}$ is not totally ramified.

Exercise 2.33. Compute the Galois group of the splitting field of $x^5 + x + 1$ over $\mathbb{Q}_3$.

Algebraic number theory for infinite extensions

Exercise 2.34. (a) Give an example of an infinite algebraic extension $M/\mathbb{Q}$ and a prime $p$ that is totally split in $M$.

(b) Give an example of an infinite algebraic extension $M/\mathbb{Q}$ and a prime $p$ that is inert in $M$.

Exercise 2.35. Let $f_1, \ldots, f_n \in \mathbb{Z}[X]$ be monic polynomials of degree at least 2. Prove that there exists a prime $p$ such that all the $f_i$ are reducible modulo $p$. 
Exercise 2.36. Prove Lemma 2.43. Make for each of the items a reduction to the finite case. For the finite cases you may refer to any standard text on algebraic number theory, such as the book of Neukirch [6].

Exercise 2.37. Let $F$ be a number field. Let $G$ be a finite group, equipped with the discrete topology. Let $\varphi: \text{Gal}(\overline{F}/F) \to G$ be a continuous homomorphism. For every prime $p$ of $F$ and every prime $\mathfrak{p}$ of $\overline{F}$ over $p$, let $I_{\mathfrak{p}}$ denote the inertia group at $\mathfrak{p}$. Show that $\varphi$ is unramified at almost all primes of $F$, i.e. for almost all primes $p$ of $F$ we have $\varphi(I_{\mathfrak{p}}) = \{1\}$ for all primes $\mathfrak{p}$ of $\overline{F}$ over $p$.

Exercise 2.38. Let $v$ be a finite place of $F$ and choose an embedding $\iota: \overline{F} \to \overline{F}_v$. Show that the induced mapping $\psi_v: \text{Gal}(\overline{F}_v/F_v) \to \text{Gal}(\overline{F}/F)$ is injective.

**Hint:** look up Krasner’s lemma (you may use this lemma in your solution).

Exercise 2.39 (The ring of integers of $\mathbb{Q}(\mu_{\ell^n})$). Let $\ell^n$ be a power of a prime number $\ell$ in $\mathbb{Z}$. Let $\mu_{\ell^n} \subset \mathbb{Q}^\times$ be the roots of unity of order dividing $\ell^n$. We show in this exercise that $\mathbb{Z}[\mu_{\ell^n}]$ is the ring of integers of $\mathbb{Q}(\mu_{\ell^n})$.

(a) Let $p \in \mathbb{Z}$ be a prime number different from $\ell$. Show that $p$ is unramified in $\mathbb{Q}(\mu_{\ell^n})$.

(b) Use Minkowski’s theorem to show that $\ell$ ramifies in $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$.

(c) Show that the principal ideal $\ell \cdot \mathbb{Z}[\mu_{\ell^n}]$ decomposes into the $\ell^{n-1}(\ell - 1)$-th power of a principal prime ideal.

(d) Deduce that $\mathbb{Z}[\mu_{\ell^n}]$ is regular at all prime numbers, and therefore integrally closed.

(e) Conclude that $\mathbb{Z}[\mu_{\ell^n}]$ is the ring of integers of $\mathbb{Q}(\mu_{\ell^n})$.

Exercise 2.40. Let $n$ be a positive integer, and let $\mathbb{Q}(\mu_n)$ be the $n$-th cyclotomic field. Prove that the ring of integers of $\mathbb{Q}(\mu_n)$ equals $\mathbb{Z}[\mu_n]$.

Exercise 2.41 (The cyclotomic character). We write $\mathbb{Q}(\mu_{\ell^n})$ for the extension of $\mathbb{Q}$ obtained by adjoining for each positive integer $n \in \mathbb{Z}_{\geq 1}$ the $\ell^n$-th roots of unity to $\mathbb{Q}$. Let $p$ be a prime number different from $\ell$.

(a) Recall that for each $n \in \mathbb{Z}_{\geq 1}$, there exists a unique isomorphism $\chi_{\ell,n}: \text{Gal}(\mathbb{Q}(\zeta_{\ell^n})) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^{\chi_{\ell,n}(\sigma)}$ for all $\ell^n$-th roots of unity $\zeta \in \mathbb{Q}(\zeta_{\ell^n})$. Show that the collection of maps $\{\chi_{\ell,n}: \mathbb{Z} \to (\mathbb{Z}/\ell^n\mathbb{Z})^\times\}$ induces an isomorphism $\chi_\ell: \text{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}) \cong \mathbb{Z}_\ell^\times$.

(b) Explain that for all $\zeta \in \mathbb{Z}_\ell^\times$ and all roots of unity $\zeta \in \mu_{\ell^n}$ of $\ell$-power order, the exponentiation $\zeta^n$ is well-defined. Then show that $\chi_\ell$ is characterized by the property that for all $\zeta \in \mu_{\ell^n}$ we have $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$.

(c) Let $p$ be a prime number different from $\ell$. Let $p$ be an $\mathbb{Q}(\zeta_{\ell^n})$-prime dividing $p$. Show that the composition $\mu_{\ell^n} \subset \mathbb{Z}[\mu_{\ell^n}] \to \mathbb{Z}[\mu_{\ell^n}]/p$ is injective.

(d) Deduce that $\chi_\ell(Frob_p) = p$ for all roots of unity $\zeta \in \mu_{\ell^n}$ of $\ell$-power order and all prime numbers $p$ different from $\ell$.

(e) Let $I_\ell \subset \text{Gal}(\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q})$ be the inertia group. What is the image of $I_\ell$ under $\chi_\ell$?
Exercise 2.42. This exercise is a continuation of Exercise 2.20

1. Compute for every prime ideal \( p \subset \mathcal{O}_M \) the algebraic extension \( M_p \) of \( \mathbb{Q} \) contained in \( M \) corresponding to inertia group \( I(p/p) \subset \text{Gal}(M/\mathbb{Q}) \). So \( M_p = M^{I(p/p)} \).

2. Prove that there exists a morphism \( \varphi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\} \) of abstract groups that is ramified at infinitely many prime numbers.

Note: By Exercise 2.37, the morphism \( \varphi \) cannot be continuous.

Exercise 2.43. Let \( p \) be a prime number. Show that there are infinitely many prime ideals \( q \) of \( \mathbb{Z}[\zeta_p] \) such that 2 is a \( p \)-th power in the finite field \( \mathbb{Z}[\zeta_p]/q \).

Exercise 2.44. \(^2\) The exact sequence \( \{\pm 1\} \to F^\times \to F^\times \) is equivariant for the Galois action of \( \text{Gal}(F/F) \) on \( F^\times \). Taking the long exact sequence of Galois cohomology, we obtain

\[
F^\times,_{\text{Gal}(F/F)} \to F^\times,_{\text{Gal}(F/F)} \to H^1(\text{Gal}(F/F), \{\pm 1\}) \to H^1(\text{Gal}(F/F), F^\times). \tag{2.6}
\]

(a) Show that \( \text{Hom}_{\text{cts}}(\text{Gal}(F/F), \{\pm 1\}) = H^1(\text{Gal}(F/F), \{\pm 1\}) \).

(b) Show using Hilbert 90 and the result from previous exercise, that Sequence (2.6) induces an isomorphism \( F^\times/F^{\times,2} \iso \text{Hom}_{\text{cts}}(\text{Gal}(F/F), \{\pm 1\}) \).

(c) Assume that \( F = \mathbb{Q} \). Let \( \chi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\} \) be a non-trivial, continuous morphism that corresponds to the element \( \alpha \in \mathbb{Q}^\times/\mathbb{Q}^{\times,2} \) from the previously found bijection. Consider the field of invariants, \( E = \overline{\mathbb{Q}}^{\ker(\chi)} \), i.e. \( E \) is the set of \( x \in \overline{\mathbb{Q}} \) such that for all \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) with \( \chi(\sigma) = 1 \) we have \( \sigma(x) = x \). Explain that \( E/\mathbb{Q} \) is a quadratic extension and give a generator of this field in terms of \( \alpha \).

Adèles and idèles

Exercise 2.45. (a) Determine the prime ideals \( P \subset A \) that are open for the topology on \( A \).

(b) Prove that there are uncountably many prime ideals \( P \) of \( A \) that are not open.

Exercise 2.46. Consider the canonical inclusion map \( f : A \to \prod_v \text{place of } \mathbb{Q}, \mathbb{Q}_v \). Prove or disprove the following statements.

1. The map \( f \) is continuous.
2. The map \( f \) is open.
3. The map \( f \) is a homeomorphism onto its image.

Exercise 2.47. (a) Explain that in \( \mathbb{Q} \otimes \prod_p \text{prime } \mathbb{Z}_p \) the tensor product does not commute with the product.

(b) Explain that in \( \mathbb{Z}[1/N] \otimes \prod_p \text{prime } \mathbb{Z}_p \) the tensor product does commute with the product (cf. equation (2.4)).

\(^2\)This exercise is for students who know, or are willing to learn, some basic Galois cohomology. A good reference for this is Serre’s book [8].
Exercise 2.48. Show that $|x|_\mathbb{A}_F = 1$ for all $x \in F \subset \mathbb{A}_F$ (the “product formula”).

**Hint:** First do the case where $F = \mathbb{Q}$.

Exercise 2.49. Show that $\mathbb{A}_F$ is canonically isomorphic to $F \otimes \mathbb{A}_\mathbb{Q}$.

Exercise 2.50. Let $L/F$ be a finite extension of number fields. Show that there is an induced ring homomorphism $\mathbb{A}_F \to \mathbb{A}_L$, and that this is a homeomorphism of $\mathbb{A}_F$ onto a closed subring of $\mathbb{A}_L$.

Exercise 2.51. (a) Let $(\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z}$ be the quotient of $\mathbb{R} \times \widehat{\mathbb{Z}}$ by the group $\mathbb{Z}$ that is diagonally embedded in $\mathbb{R} \times \widehat{\mathbb{Z}}$, so the image of the map $\mathbb{Z} \to (\mathbb{R} \times \widehat{\mathbb{Z}})$, $x \mapsto (x, x)$. Show that the mapping $(\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z} \to \mathbb{A}/\mathbb{Q}$, $x \mod \mathbb{Z} \mapsto (1, x) \in (\mathbb{R} \times \mathbb{A}^\infty)/\mathbb{Q}$, is an isomorphism of topological groups.

(b) Show that the mapping $\lim_{N \in \mathbb{Z} \geq 1} \mathbb{R}/N\mathbb{Z} \to (\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z}$, $(x_N) \mapsto (x_1, x_N - x_1)_{N \in \mathbb{Z} \geq 1}$, is an isomorphism of topological groups, and give a description of its inverse.

(c) Conclude that $\mathbb{A}/\mathbb{Q}$ is isomorphic to the solenoid $\mathbb{S} = \lim_{N \in \mathbb{Z} \geq 1} \mathbb{R}/N\mathbb{Z}$.

Exercise 2.52. Prove the identity

$$\mathbb{A} = \mathbb{Q} + ([-1, 1] \times \widehat{\mathbb{Z}}).$$

(In other words, any adèle $\alpha \in \mathbb{A}$ can be written, not necessarily uniquely, as $x + \beta$ with $x \in \mathbb{Q}$ and $\beta \in [-1, 1] \times \widehat{\mathbb{Z}}$.)

Exercise 2.53. Let $S$ be a finite set of places of $\mathbb{Q}$. The goal of this exercise is to prove that strong approximation for the adèles of $\mathbb{Q}$ outside $S$, i.e. the statement that $\mathbb{Q}$ is dense in $\mathbb{A}^S$, holds if and only if $S \neq \emptyset$.

(a) Prove that $\mathbb{Q}$ is not dense in $\mathbb{A}$ (i.e. strong approximation fails for $S = \emptyset$).

(b) Prove that $\mathbb{Q}$ is dense in $\mathbb{A}^\infty$ (i.e. strong approximation holds for $S = \{\infty\}$).

(c) Let $p$ be a prime number. Show that for all $\gamma \in \mathbb{A}$, all $\varepsilon > 0$, and every finite set $\Sigma$ of places of $\mathbb{Q}$ with $p \not\in \Sigma$ and $\infty \in \Sigma$, the open subset $\prod_{v \in \Sigma} B(\gamma_v, \varepsilon) \times \prod_{v \not\in \Sigma, v \neq p} \mathbb{Z}_v$ of $\mathbb{A}^{(p)}$ contains a rational number.

(d) Conclude that $\mathbb{Q}$ is dense in $\mathbb{A}^S$ for every non-empty finite set $S$ of places of $\mathbb{Q}$.

Exercise 2.54. Show that the subset $\mathbb{A}_F^\times \subset \mathbb{A}_F$ (equipped with the subspace topology) is closed but not open.

Exercise 2.55. Prove that if $F$ is a local field, then the topology on $F^\times$ defined in the text is the subspace topology induced from the inclusion $F^\times \to F$.

Exercise 2.56. Consider the set $S = \{p\}$, where $p$ is a prime number.

(a) Construct an explicit isomorphism from the quotient $\mathbb{A}_\mathbb{Q}^{S, \times} / \mathbb{Q}^\times \mathbb{Z}^{S, \times}$ to the circle $\mathbb{R}/\mathbb{Z}$. (In particular, $\mathbb{Q}^\times \mathbb{Z}^{S, \times}$ is closed in $\mathbb{A}_\mathbb{Q}^{S, \times}$.)

(b) Conclude that $\mathbb{Q}^\times$ is not dense in $\mathbb{A}_\mathbb{Q}^{S, \times}$. 
Exercise 2.57.  (a) Show that for every prime number $p$, strong approximation outside \{p\} is false for the idèles of $\mathbb{Q}$.

(b) Does there exist a finite set $S$ of places of $\mathbb{Q}$ such that strong approximation outside $S$ is true for the idèles of $\mathbb{Q}$?

Exercise 2.58. Let $S$ be a finite set of $F$-places. Show that the subset $F^\times \subset \hat{\mathbb{A}}^\times = \prod_{v \in S} F_v^\times$ is dense.

Exercise 2.59. Consider the set $\text{Frac}(\hat{\mathcal{O}}_F)$ consisting of those $\mathcal{O}_F$-submodules $I \subset \mathbb{A}_F$ such that $I \otimes \mathcal{O}_F$ is non-trivial for every $v$, and for some $x \in \mathbb{A}_F^\times$ we have $xI \subset \hat{\mathcal{O}}_F$.

(a) Show that the mapping $\text{Frac}(\mathcal{O}_F) \to \text{Frac}(\hat{\mathcal{O}}_F)$, $I \mapsto \hat{\mathcal{O}}_F \otimes \mathcal{O}_F I$ is a bijection.

(b) Deduce that the mapping $\text{Cl}(F) = \text{Frac}(\mathcal{O}_F)/F^\times \to \text{Frac}(\hat{\mathcal{O}}_F)/F^\times = \hat{\mathbb{A}}^\times_\hat{\mathcal{O}}_F F^\times$ is an isomorphism.

Exercise 2.60. Let $F$ be a number field. Let $V$ be a finite-dimensional vector space over $F$. Let $X_F$ be the set of $\mathcal{O}_F$-lattices in $V$, and let $\hat{X}_F$ be the set of $\mathcal{O}_F$-lattices in the $\mathbb{A}_F^\infty$-module $\hat{V} = \mathbb{A}_F^\infty \otimes_F V$.

(a) Show that the mapping $X_F \to \hat{X}_F$, $\Lambda \mapsto \hat{\Lambda} = \hat{\mathcal{O}}_F \otimes \mathcal{O}_F \Lambda$ is a bijection.

(b) Fix a lattice $\Lambda_0 \in V$. Show that the map $\text{GL}_F(V) \to X_F$, $g \mapsto g\Lambda_0$ induces a bijection $\text{GL}_F(V)/\text{GL}_{\mathcal{O}_F}(\Lambda_0) \sim \to X_F$. And similarly, $\text{GL}_{\mathbb{A}_F^\infty}(\hat{V})/\text{GL}_{\hat{\mathcal{O}}_F}(\hat{\Lambda}_0) \sim \to \hat{X}_F$.

(c) Deduce that the mapping $\text{GL}_F(V)/\text{GL}_{\mathcal{O}_F}(\Lambda_0) \to \text{GL}_{\mathbb{A}_F^\infty}(\hat{V})/\text{GL}_{\hat{\mathcal{O}}_F}(\hat{\Lambda}_0)$, $g \mapsto \mathbb{A}_F^\infty \otimes_F g \Lambda_0$, is a bijection.

Exercise 2.61. (a) Prove that the idèle class group $C_Q = \mathbb{Q}^\times \backslash \mathbb{A}^\times$ of $\mathbb{Q}$ is canonically isomorphic to $\mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times$.

(b) Prove (without using the main theorem of class field theory) that $U_Q$ equals the image of $\mathbb{R}_{>0}$ under the isomorphism $\mathbb{R}_{>0} \times \hat{\mathbb{Z}}^\times \sim \to C_Q$ from the previous part.

Class field theory

Exercise 2.62. Let $F$ be a number field, let $C_F = F^\times \backslash \mathbb{A}_F^\times$ be the idèle class group of $F$, and let $U$ be the image of $(F \otimes Q \mathbb{R}) \times \hat{\mathcal{O}}_F^\times \subset \mathbb{A}_F^\times$ in $C_F$.

(a) Show that $U$ is an open subgroup of $C_F$.

(b) Show that the finite Abelian extension of $F$ associated to $U$ by the main theorem of class field theory is the maximal unramified extension of $F$. (Here the extension $\mathbb{C}/\mathbb{R}$ of Archimedean local fields is regarded as being ramified.)

Exercise 2.63. Let $F$ be a number field.

(a) Assume that $F$ has two $\ell$-adic places $\lambda_1$, $\lambda_2$ whose inertial degree and ramification degree over $\mathbb{Q}$ are the same. Show that any continuous character $\chi : \text{Gal}(F_{\lambda_1}/F_{\lambda_2}) \to \mathbb{Q}^\times_{\ell}$ globalizes to a character of the absolute Galois group of $F$, i.e. there exists a continuous character $\check{\chi} : \text{Gal}(\hat{F}/F) \to \mathbb{Q}^\times_{\ell}$ such that $\check{\chi}|_{\text{Gal}(F_{\lambda_1}/F_{\lambda_2})} = \chi$. 

(b) Now assume that $\ell$ is inert in $F$. Let $\lambda$ be the $F$-place above $\ell$. Give a necessary and sufficient condition for a character $\chi : \text{Gal}(F_{\lambda}/F_{\lambda}) \to \mathbb{Q}_p^\times$ to globalize.
Bibliography


