Théorie des nombres

Benjamin Schraen

Année 2021-2022
Contents

1 Global and local fields 5
  1.1 Absolute values ................................................. 5
    1.1.1 Places of a field ........................................... 5
    1.1.2 Ultrametric absolute values ............................. 7
    1.1.3 Absolute values of $\mathbb{Q}$ ............................ 9
  1.2 Complete fields, local fields .................................. 10
    1.2.1 Complete fields ............................................ 10
    1.2.2 Local fields ............................................... 13
    1.2.3 Structure of the valuation ring of local field ......... 15
    1.2.4 Extensions of complete fields ......................... 16
    1.2.5 Hensel Lemma .............................................. 18
    1.2.6 Krasner Lemma ............................................. 20
    1.2.7 Classification of local fields .......................... 21
    1.2.8 Haar measures and normalization of absolute values ... 22
  1.3 Places of global fields .......................................... 24
    1.3.1 Extension of absolute values ............................ 24
    1.3.2 The product formula ....................................... 26
    1.3.3 Archimedean places of number fields .................... 27
  1.4 Ramification ..................................................... 28
    1.4.1 Dedekind rings ............................................ 28
    1.4.2 Extensions ............................................... 29
    1.4.3 Galois extensions ......................................... 34
    1.4.4 Link with localization and completion .................. 36
    1.4.5 Different and discriminant .............................. 37
    1.4.6 Frobenius element ........................................ 41
    1.4.7 The example of the cyclotomic extensions ............... 41

2 Adeles and ideles 45
  2.1 Adeles ......................................................... 45
    2.1.1 Topological groups and restricted products .......... 45
    2.1.2 Adeles .................................................... 47
# CONTENTS

## 2.1 Haar measures
- 2.1.3 Haar measures .................................. 48

## 2.2 Ideles
- 2.2.1 Definition and first properties ............... 52
- 2.2.2 Ideles and ideals ................................. 54
- 2.2.3 Fundamental domain of $I_F/F^\times$ and Dirichlet unit Theorem 56
- 2.2.4 Haar measures .................................. 58

## 3 Zêta functions
- 3.1 Duality in locally compact abelian groups ........ 61
  - 3.1.1 Dual of a locally compact abelian group ...... 61
  - 3.1.2 Duality in local fields .......................... 63
  - 3.1.3 Dualité dans les adèles .......................... 64
  - 3.1.4 Fourier transform ............................... 66
  - 3.1.5 Fourier transform on a local field .......... 67
  - 3.1.6 Fourier transform on adeles .................... 68
- 3.2 Local zeta functions ................................. 69
  - 3.2.1 Multiplicative characters ....................... 69
- 3.3 Global zeta functions ............................... 75
  - 3.3.1 Poisson formula ................................. 75
  - 3.3.2 Integrals on $I_F$ ............................... 76
  - 3.3.3 Hecke characters, global zeta functions ...... 76
  - 3.3.4 L’équation fonctionnelle globale ............ 78

## 4 Class field Theory
- 4.1 Abelian extensions of $p$-adic fields ............... 81
  - 4.1.1 Unramified extensions ......................... 81
  - 4.1.2 Local statements ............................... 83
  - 4.1.3 Proof of the unicity ............................ 84
- 4.2 Abelian extensions of number fields ................ 85
  - 4.2.1 Statements ..................................... 85
  - 4.2.2 Reformulation with ideals ..................... 87
- 4.3 First inequality .................................. 90
  - 4.3.1 Dirichlet density ............................... 90
  - 4.3.2 The first inequality ............................ 91
  - 4.3.3 Other consequences ............................ 91
Chapter 1

Global and local fields

All fields are supposed to be commutative.

1.1 Absolute values

1.1.1 Places of a field

Definition 1.1.1. An absolute value of a field $K$ is a map $|·| : K \to \mathbb{R}_{>0}$ such that

- $\forall x \in K, \quad |x| = 0 \iff x = 0$;
- $\forall (x, y) \in K^2, \quad |xy| = |x||y|$;
- $\forall (x, y) \in K^2, \quad |x + y| \leq |x| + |y|$.

An absolute value $|·|$ is said to be ultrametric if it has the stronger property

$$\forall (x, y) \in K^2, \quad |x + y| \leq \max(|x|, |y|)$$

and if $|K^\times| \neq \{1\}$.

A valued field is a field $K$ endowed with an absolute value $|·|$.

An ultrametric norm is also called nonarchimedean.

Example 1.1.2. a) The trivial absolute value is the absolute value defined by $|x| = 1 \iff x \neq 0$.

b) If $K = \mathbb{Q}$, the usual absolute value is an absolute value:

$$|x| = \max\{x, -x\}.$$ 

It is not ultrametric and is also called the archimédienne or real absolute value.
c) If \( p \) is a prime number and \( x \in \mathbb{Q} \), let

\[
|x|_p = p^{-v_p(x)}
\]

where \( v_p(x) \) is the \( p \)-adic valuation of \( x \), with convention \( |0|_p = 0 \). It is an ultrametric absolute value called \( p \)-adic absolute value.

If \( K \) is a field and \( |\cdot| \) is an absolute value over \( K \), the map \((x, y) \mapsto |x - y|\) defines a metric over \( K \).

**Lemma 1.1.3.** For the topology defined by an absolute value, a field \( K \) is a topological field. Moreover, the topology is discrete if and only if the absolute value is trivial.

**Proof.** In order to prove that \( K \) is a topological field, it is sufficient to prove that the maps from \( K \times K \) to \( K \) defined by \((x, y) \mapsto x - y\) and \((x, y) \mapsto xy\) are continuous and that the map from \( K^\times \) to \( K^\times \) defined by \( x \mapsto x^{-1} \) is also. Let’s check it for this last map. Let \( x_0 \in K^\times \) and \( \varepsilon > 0 \). We have

\[
|x^{-1} - x_0^{-1}| \leq \frac{1}{|x||x_0|}|x - x_0|.
\]

If \( |x - x_0| < \min\left(\frac{|x_0|}{2}, \frac{\varepsilon|x_0|^2}{2}\right) \), then \( |x^{-1}x_0^{-1}| < \varepsilon \).

If the absolute value is trivial, the topology is discrete since all singletons of \( K \) are open. If the absolute value is not trivial, there exists \( x \in K^\times \) such that \( |x| \neq 1 \). Up to replacing \( x \) by its inverse, we can assume that \( |x| < 1 \) and the sequence \((x^n)_{n \geq 0}\) converges to 0 with \( x^n \neq 0 \) for all \( n \geq 0 \). The singleton \(|0|\) is not open and the topology is not discrete. \( \square \)

**Definition 1.1.4.** We say that two absolute values over \( K \) are equivalent if they define the same topology over \( K \). A place of \( K \) is an equivalence class of non-trivial absolute values over \( K \).

**Lemma 1.1.5.** Let \( |\cdot|_1 \) and \( |\cdot|_2 \) two absolute values over \( K \). They are equivalent if and only if there exists a real number \( \alpha > 0 \) such that \( |\cdot|_2 = |\cdot|_1^\alpha \).

**Proof.** Let’s first remark that if \( |\cdot| \) is an absolute value of \( K \), the sets \( \{x \in K \mid |x| > 1\} \) and \( \{x \in K \mid |x| < 1\} \) depends only on the topology defined by \( |\cdot| \). Namely \( |x| < 1 \) if and only if the sequence \((x^n)_{n \geq 0}\) converges to 0.

Assume that the absolute values \( |\cdot|_1 \) et \( |\cdot|_2 \) define the same topology on \( K \). The remark just above implies that, for \( x, y \in K \), we have \( |x|_1 \leq |y|_1 \) if and only if \( |x|_2 \leq |y|_2 \). It is clear that \( |\cdot|_1 \) is trivial if and only if \( |\cdot|_2 \) is. We can thus assume that \( |\cdot|_1 \) and \( |\cdot|_2 \) are non trivial and choose \( x_0 \in K \) such that \( |x_0|_1 > 1 \). Thus \( |x_0|_2 > 1 \). It exists therefore \( \alpha > 0 \) such that \( |x_0|_2 = |x_0|^\alpha_1 \). Let \( x \in K \) such that
1.1. ABSOLUTE VALUES

| | | |

1.1.1 Absolute Values

We can write $|x|_1 = |x_0|^a$ and $|x|_2 = |x_0|^b$ for $a, b > 0$. Let $\frac{p}{q} \in \mathbb{Q}$ such that $\frac{p}{q} \leq a$. We have

$$|x_0|^{\frac{p}{q}} \leq |x_0|^a = |x|_1$$

so that $|x_0|^\frac{p}{q} \leq |x|_1$ and $|x_0|^\frac{p}{q} \leq |x|_2$. We deduce $|x|^\frac{p}{q} \leq |x|_2 = |x_0|^b$. This being true for all $\frac{p}{q} \leq a$, we obtain that $|a| \leq b$. By inverting the roles of $|\cdot|_1$ and $|\cdot|_2$, we show that $b \leq a$ and thus $a = b$. Then $|x|_2 = |x|_1^a$ for all $x$ such that $|x|_1 > 1$. The properties of absolute values imply that this equality is checked for all $x \in K$.

1.1.2 Ultrametric absolute values

**Proposition 1.1.6.** A non trivial absolute value $|\cdot|$ is ultrametric if and only if $|n| \leq 1$ for all $n \in \mathbb{Z}$. As a consequence, if $K$ has non zero characteristic, all non trivial absolute values of $K$ are ultrametric.

**Proof.** Assume $|\cdot|$ ultrametric. Then $|n| = |1 + \cdots + 1| \leq |1| = 1$.

Conversely assume that $|n| \leq 1$ for all $n \in \mathbb{Z}$. Let $x, y \in K$ such that $|x|, |y| \leq 1$. The binomial formula implies that, for $n \geq 0$

$$|(x + y)^n| \leq \sum_{i=0}^{n} \binom{n}{i} |x|^i |y|^{n-i} \leq n + 1.$$

Thus $|x + y| \leq (n + 1)^{\frac{1}{n}}$. Letting $n$ going to $+\infty$, we deduce that $|x + y| \leq 1$. We easily deduce that $|\cdot|$ is ultrametric.

If the characteristic of $K$ is a prime number $p$, then $\mathbb{Z}^1 = \mathbb{F}_p \subset K$. We deduce that if $x \in \mathbb{Z}^1$ is nonzero, then $x^{p-1} = 1$ and $|x| = 1$. Consequently $|\cdot|$ is ultrametric.

**Definition 1.1.7.** We say that an ultrametric absolute value of $K$ is discrete if the image of $K^\times$ is a discrete subgroup of $\mathbb{R}_{>0}$.

As discrete subgroups of $\mathbb{R}_{>0}$ are the $a^\mathbb{Z}$ for $a \in \mathbb{R}_{>0}$, we deduce that if $|\cdot|$ is discrete and non trivial, then $|K^\times|$ is a group isomorphic to $\mathbb{Z}$.

Here are some properties of ultrametric absolute values.

**Proposition 1.1.8.**

a) For $x, y \in K$ such that $|x| > |y|$, we have $|x + y| = |x|.$

b) An open ball $B(x, r) = \{y \in K \mid |y - x| < r\}$ is both open and close in $K$.

c) A closed ball $\overline{B}(x, r) = \{y \in K \mid |y - x| \leq r\}$ of nonzero radius is both open an close in $K$. 

d) Spheres of $K$ of nonzero radius is both open and close in $K$.

e) Two closed balls (resp. open) of $K$ are either disjoint or contained in each other.

**Proof.** Exercise. □

If $|·|$ is an ultrametric absolute value on $K$, we define

$$O = \{x \in K \mid |x| \leq 1\}$$ and $$p = \{x \in K \mid |x| < 1\}.$$ Then $O$ is a subring of $K$ called ring of valuation associated to $|·|$ and $p$ is an ideal of $O$.

**Proposition 1.1.9.** Let $|·|$ be an ultrametric absolute value of $K$.

(i) The ideal $p$ is maximal.

(ii) The ideal $p$ is the unique maximal ideal of $O$.

(iii) The ideal $p$ is principal if and only if the absolute value $|·|$ is discrete. In this case, the ring $O$ is a PID.

**Proof.** An element $x \in O$ is invertible in $O$ if and only if $|x| = 1$. Then $O^\times = O \setminus p$. This implies that every non trivial ideal of $O$ is included in $p$. As moreover, $p \subseteq O$, the ideal $p$ is the largest element of the set of non trivial ideals of $O$, it is this the unique maximal ideal of $O$. This proves (i) and (ii).

Let $\Gamma$ be the subgroup $|K^\times|$ of $\mathbb{R}_{>0}$ and let’s prove (iii).

Assume that the ideal $p$ is principal and let $\pi$ be a generator of $p$. Then $\Gamma \cap |\pi|, |\pi|^{-1}| = \{1\}$. The subgroup $\Gamma$ is therefore discrete in $\mathbb{R}_{>0}$.

Conversely assume that $\Gamma$ is discrete. We will directly prove that $O$ is a PID, which implies (iii). Let $\varpi \in K$ such that $|\varpi| = a$. If $I \subset O$ is a nonzero ideal, set $\gamma = \sup |I|$. As $|·|$ is non trivial, there exists $r > 0$ such that $r, 1[\cap |I| \neq \emptyset$ and since $\Gamma$ is a discrete subgroup of $\mathbb{R}_{>0}$, the set $|I| \cap \Gamma$ is finite. We deduce the existence of $x_0 \in I$ such that $|x_0| = \gamma$. We have $(x_0) \subset I$ and if $x \in I$, we have $|x| \leq |x_0|$ so that $\frac{x}{x_0} \in O$ and $x \in (x_0)$. Then $I = (x)$ and $O$ is a PID. □

When $(K, |·|)$ is an ultrametric valued field, the field $O/p$ is called the residue field of $(K, |·|)$.

**Definition 1.1.10.** Let $K$ be a field. A discrete valuation of $K$ is a map $v : K^\times \to \mathbb{Z}$ such that, for all $x, y \in K^\times$

(i) $v(xy) = v(x) + v(y)$;

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$. 

We set $v(0) = +\infty$.

A discrete valuation $v$ is normalized if moreover $v(K^\times) = \mathbb{Z}$.

If $v$ is a discrete valuation if a field $K$, then $x \mapsto e^{-v(x)}$ is a discrete absolute value of $K$. We obtain a bijection between the set of normalized discrete valuation discrètes of $K$ and the set of discrete ultrametric places of $K$.

### 1.1.3 Absolute values of $\mathbb{Q}$

**Theorem 1.1.11.** The places of $\mathbb{Q}$ are those who are associated with $|\cdot|_\infty$ and $|\cdot|_p$ with $p$ prime. Moreover these places are different from each other.

**Proof.** Let $|\cdot|$ be a nontrivial ultrametric absolute value. Let $\mathcal{O}$ be its valuation ring and $p$ be its maximal ideal. Then the ideal $p \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. If $p \cap \mathbb{Z} = \{0\}$, then $|x| = 1$ for all $x \in \mathbb{Z} \setminus \{0\}$ and $|\mathbb{Q}^\times| = \{1\}$, which contradicts the fact that $|\cdot|$ is nontrivial. Then it exists a prime $p$ such that $p \cap \mathbb{Z} = (p)$. We conclude that if $m \in \mathbb{Z}$ is prime to $p$, then $|m| = 1$ and $|p^{\alpha}x| = |p|^\alpha$ for all $\alpha \in \mathbb{Z}$, $r, s \in \mathbb{Z}$ prime to $p$. We conclude that $|\cdot|$ is equivalent to $|\cdot|_p$.

Suppose now that $|\cdot|$ isn’t ultrametric and fix $f(x) = \sup\{0, \log|x|\}$ for $x \in \mathbb{Z}$. There exists $m \in \mathbb{Z}$ such that $f(m) > 0$. For all $(m, n) \in \mathbb{Z}$ and $k \in \mathbb{N}$, we have
\[
f(m^k) = kf(m), \quad f(mn) \leq f(m) + f(n), \quad f(m + n) \leq \ln(2) + \sup\{f(m), f(n)\}.
\]
Let $a$ and $b$ be two integers such that $a, b > 1$. We can consider the $a$-adic expansion of $b$:
\[
b = x_0 + x_1a + \cdots + x_na^n
\]
with $0 \leq x_i \leq a - 1$ and $x_n \neq 0$. Let $c = \sup\{f(i) \mid 0 \leq i < a\}$. Then we have $f(x_ia^i) \leq c + if(a)$ for all $i$ and then
\[
f(b) \leq n\ln(2) + nf(a).
\]
Since $a^n \leq b$, we have $n\ln(a) \leq \ln(b)$ and
\[
\frac{f(a)}{\ln(a)} \leq \frac{\ln(2) + f(b)}{\ln(b)} + \frac{c}{\ln(a)}.
\]
We can replace $a$ by $a^k$ and let $k$ tends toward $+\infty$, we get
\[
\frac{f(a)}{\ln(a)} \leq \frac{\ln(2) + f(b)}{\ln(b)}.
\]
Doing the same with $b$, we get
\[
\frac{f(a)}{\ln(a)} \leq \frac{f(b)}{\ln(b)}.
\]
Even if we change the roles of \(a\) and \(b\), \(a \mapsto f(a)\ln(a)\) is constant on \(\mathbb{Z}_{\geq 2}\), It is equal to \(\alpha \in \mathbb{R}_{>0}\), which proves the result.

Now we give an example of absolute value on the field \(\mathbb{F}_q(T)\) where \(\mathbb{F}_q\) is a finite field such that \(\text{Card}(\mathbb{F}_q) = q\). Let \(P \in \mathbb{F}_q[T]\) be an irreducible polynomial. The ring \(\mathbb{F}_q[T]\) is a factorial ring, so that we can define the \(P\)-adic valuation of an element of \(\mathbb{F}_q(T)\) and define \(|.|_P = q^{-v_P(\cdot)}\). It is an ultrametric absolute value on \(\mathbb{F}_q(T)\). We can also define, for \(R, S \in \mathbb{F}_q[T]\), with \(S \neq 0\),

\[
\frac{|R|}{|S|}_\infty := q^{\deg(R) - \deg(S)}.
\]

It is an ultrametric absolute value corresponding to the choice of \(P = T^{-1}\) on \(\mathbb{F}_q(T^{-1}) = \mathbb{F}_q(T)\).

**Theorem 1.1.12.** The places of \(\mathbb{F}_q(T)\) are associated with the absolute values of the form \(|.|_P\) or \(|.|_\infty\). Moreover these places are different from each other.

**Proof.** Exercise.

### 1.2 Complete fields, local fields

#### 1.2.1 Complete fields

Let \((K, |.|)\) be a valued field. We say that \(K\) is complete if it is complete for the distance induced by \(|.|\).

If \((K, |.|)\) is a valued field, we denote \(\hat{K}\) the completion of \(K\) with respect to \(|.|\). For all \(x, y \in K\), we have \(|x| - |y| \leq |x - y|\) which makes \(|.| : K \to \mathbb{R}\) uniformly continuous and extends to a continuous map \(|.| : \hat{K} \to \mathbb{R}\).

**Lemma 1.2.1.** The set \(\hat{K}\) is endowed with a unique structure of topological field which is compatible with the topology of \((K, |.|)\)

**Proof.** The set \(\hat{K}\) is endowed with a unique topological ring structure compatible to the topological structure defined on \(K\) [Bourbaki, Topologie Générale, §III.6]. To prove that \(\hat{K}\) is a field. We have to verify that if \((x_n)_{n \geq 0}\) is a Cauchy sequence of elements of \(K\) which doesn’t converge to 0, then the sequence \((x_n^{-1})_{n \geq 0}\) is a Cauchy sequence. This is easy to check using the following relation

\[
\forall x, y \in K^\times, \quad |x^{-1} - y^{-1}| = |x^{-1}||y^{-1}||x - y|.
\]
Lemma 1.2.2. The map $|·|_R$ is an absolute value on $\hat{K}$.

Proof. Most of the properties of absolute values are easily verified when we pass to the limit. It remains to check that $|x|_R = 0 \implies x = 0$. Suppose that $|x|_R = 0$. Then it exists $(x_n)_{n \geq 0}$ a sequence of elements of $K$ which converges to $x$ and $|x_n|$ converges to $0$. This implies that $(x_n)_{n \geq 0}$ converge to $0$ in $K$, so that $x = 0$. \qed

The absolute value $|·|_\hat{K}$ is the unique continuous extension from $|·|$ to $K$, we denote it as $|·|$ by abuse of langage.

Remark 1.2.3. If $(K, |·|)$ is an ultrametric valued field, then $|K| = |\hat{K}|$. Actually, we have $|a| = |b|$ if $|a - b| < |a|$.

The completion of a valued field have the following universal property.

Proposition 1.2.4. Let $(K, |·|)$ a valued field, $L$ a complete valued field and $f : K \to L$ a continuous field homomorphism, then there exists a unique continuous field homomorphism $\hat{f} : \hat{K} \to L$ whose restriction at $K$ is $f$.

Proof. A continuous field homomorphism is uniformly continuous, the existence of $\hat{f}$ is a universal property of the completion of a metric space. We can easily verify that $\hat{f}$ is a morphism of field. \qed

Corollary 1.2.5. If $(K, |·|)$ is a valued field and $(L, |·'|)$ a valued field contains $K$ such that the restriction of $|·'|$ to $K$ is equivalent to $|·|$ and such that $K$ is dense in $L$, then $(L, |·'|)$ is isomorphic to the completion of $K$.

Example 1.2.6. 1. The completion of $\mathbb{Q}$ for the norm $|·|_\infty$ is isomorphic to $\mathbb{R}$.

2. Let $k$ a field and $K = k(T)$. Let $v$ be the $T$-adic valuation on $k(T)$. The completion of $K$ for the valuation $v$ is isomorphic to the field of Laurent’s series $k((T))$, which means

$$k((T)) = \left\{ \sum_{n=-N}^{+\infty} a_n T^n \mid N \in \mathbb{N}, a_n \in k \right\}.$$

Definition 1.2.7. Let $p$ a prime. The completion of $\mathbb{Q}$ for the norm $|·|_p$ is called the field of $p$-adic numbers and is denoted by $\mathbb{Q}_p$. We denote $\mathbb{Z}_p$ the ring of integers of $\mathbb{Q}_p$, its elements are called the $p$-adic integers.

Lemma 1.2.8. Let $K$ an ultrametric complete field. Let $(x_n)_{n \geq 0}$ be a sequence of elements of $K$. Then

- the sequence $(x_n)_{n \geq 0}$ converges in $K$ if and only if the limit of the sequence $(x_{n+1} - x_n)_{n \geq 0}$ is 0;
• the series $\sum_{n \geq 0} x_n$ converges in $K$ if and only if the limit of the sequence $(x_n)_{n \geq 0}$ is $0$.

**Proof.** This two assertions are obviously equivalent. Let’s prove the first one. We need to show that if the sequence $(x_{n+1} - x_n)_{n \geq 0}$ tends towards $0$, then the sequence $(x_n)_{n \geq 0}$ is a Cauchy sequence. Let $\varepsilon > 0$ and let $N \in \mathbb{N}$ such that $n \geq N$ implies $|x_{n+1} - x_n| < \varepsilon$. Then, for all $k \geq 1$,

$$|x_{n+k} - x_n| \leq \max(|x_{n+1} - x_n|, \ldots, |x_{n+k} - x_{n+k-1}|) < \varepsilon.$$

Thus the sequence $(x_n)_{n \geq 0}$ is a Cauchy sequence. \hfill $\square$

Let $K$ a complete field for a discrete ultrametric absolute value. Let $\mathcal{O}$ be its valuation ring, $p$ the maximal ideal of $\mathcal{O}$ and $k$ the residue field $\mathcal{O}/p$. Since $|\cdot|$ is discrete, there exists a real number $\varepsilon < 1$ such that $|K^\times| = \varepsilon^\mathbb{Z}$. We call uniformizer of $K$ an element $\pi \in \mathcal{O}$ such that $|\pi| = \varepsilon$. Equivalently, $\pi$ is a element of $K$ such that $p = (\pi)$.

**Proposition 1.2.9.** Let $\Sigma$ be a set of representatives of $k$ in $\mathcal{O}$. Then all elements of $\mathcal{O}$ can be written uniquely as a convergent series

$$x_0 + x_1 \pi + \cdots + x_n \pi^n + \cdots$$

where $x_i$ are elements of $\Sigma$.

**Proof.** First of all we see that such a series converges in $K$ since $|x_i \pi^n| \leq |\pi|^i \to_{n \to +\infty} 0$.

We prove the existence of the expansion. Let $x_0 \in \Sigma$ such that $x$ and $x_0$ have the same image in $k$. Then $x - x_0 \in p = (\pi)$, and there exists $y \in \mathcal{O}$ such that $x = x_0 + y \pi$. Replacing $x$ by $y$, there exists $x_1 \in \Sigma$ such that $x - (x_0 + x_1 y) \in (\pi^2)$. By induction, we obtain the existence of a sequence $(x_n)_{n \geq 0}$ such that

$$x - (x_0 + x_1 \pi + \cdots + x_n \pi^n) \in (\pi^{n+1})$$

for all $n \geq 0$, so that the series $\sum_{n \geq 0} x_n \pi^n$ converges to $x$.

We prove the uniqueness. Suppose that we can express $x = \sum_{n \geq 0} x_n \pi^n = \sum_{n \geq 0} x'_n \pi^n$ with $x_n, x'_n \in \Sigma$ and let $m$ be the smallest integer such that $x_m \neq x'_m$. Then

$$x_m \pi^m - x'_m \pi^m \in (\pi^{m+1})$$

which makes $x_m - x'_m \in (\pi)$. This contradicts $x_m \neq x'_m$ and the fact that $\Sigma$ is a representative system of $k$ in $\mathcal{O}$. \hfill $\square$
Remark 1.2.10. 1. Let \((K, |·|)\) be an ultrametric valued field and let \((\hat{K}, |·|)\) be its completion. Then \(O_{\hat{K}}\) is the closure of \(O_K\) in \(\hat{K}\). Namely, if \((x_n)_{n\geq 0}\) is a sequence of elements of \(K\) which converges to an element \(x \in O_{\hat{K}}\) such that \(x \neq 0\), then \(|x_n| = |x| \leq 1\) for \(n\) big enough. Since the maximal ideal \(p_{\hat{K}}\) is open in \(O_{\hat{K}}\), we have \(O_{\hat{K}} = O_K + p_{\hat{K}}\). Moreover
\[p_{\hat{K}} \cap O_K = \{ x \in K \mid |x| < 1 \} = p_K.\]
We conclude that the natural application
\[O_K/p_K \to O_{\hat{K}}/p_{\hat{K}}\]
is an isomorphism. Thus \(K\) and \(\hat{K}\) have the same residue field.

2. As \(|K^\times| = |\hat{K}^\times|\), an uniformizer of \(K\) is an uniformizer of \(\hat{K}\).

1.2.2 Local fields

We say that a valued field is local if it is locally compact as a topological space and its absolute value is nontrivial. A local field is complete.

In a local field, all closed balls are compact subsets. In particular, if \(K\) is ultrametric, the ring \(O\) is a compact subset of \(K\).

Proposition 1.2.11. Let \(K\) a complete ultrametric valued field. Then \(K\) is local if and only if its valuation is discrete and its residue field is finite.

Proof. Suppose que \(K\) is local. Let’s prove that its valuation is discrete. We can write
\[O = \overline{B}(0, 1) = S(0, 1) \bigcup_{0 < r < 1} \overline{B}(0, r).\]
Since \(O\) is compact, the sphere \(S(0, 1)\) and the closed balls \(\overline{B}(0, r)\) are open, this union is finite and there exists \(0 < r < 1\) such that
\[O = S(0, 1) \bigcup \overline{B}(0, r).\]
Thus \(|K^\times| \cap [r, 1] = \emptyset\) and \(|K^\times|\) is a discrete subgroup of \(\mathbb{R}^\times_+\).

Let’s prove now that the residue field of \(K\) is finite. Since \(O\) is a closed ball of \(K\), it is a compact subset. Moreover the maximal ideal \(p = B(0, 1)\) is an open subset of \(K\). Let \(\Sigma\) be a representative system of \(k = O/p\) in \(O\). Then we have
\[O = \bigcup_{x \in \Sigma} (x + p).\]
where each \( x + \mathfrak{p} \) is an open subset of \( K \). We conclude from the compactness of \( \mathcal{O} \) that \( \Sigma \) and \( k \) are finite.

Suppose conversely that \( k \) is a finite field and that the absolute value is discrete. Fix \( \Sigma \) a set of representatives of \( k \) in \( \mathcal{O} \). We will prove that \( \mathcal{O} \) is compact. As \( K \) is a metric space and \( \mathcal{O} \) is closed in \( K \), it is sufficient to prove that \( \mathcal{O} \) is precompact.

Fix \( r \in ]0,1[ \). Let \( \pi \in \mathfrak{p} \) be an uniformizer of \( K \) and let \( n \in \mathbb{N} \) such that \( |\pi^n| < r \).

If \( x \in \mathcal{O} \), we have the following formula

\[
x \in x_0 + x_1 \pi + \cdots + x_{n-1} \pi^{n-1} + (\pi^n) = B(x_0 + x_1 \pi + \cdots + x_{n-1} \pi^{n-1}, |\pi|^n).
\]

We conclude that \( \mathcal{O} \) has a finite covering by open balls of radius \( r' > r \). Thus \( \mathcal{O} \) is precompact. We conclude that all closed balls of radius 1 are compact and that all point of \( K \) have a compact neighbourhood. Thus \( K \) is locally compact. \( \square \)

**Example 1.2.12.** The ring \( \mathbb{Z}_p \) is the closure of the ring \( \mathbb{Z}_{(p)} = \{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z} \} \) which is also the localisation of \( \mathbb{Z} \) in the prime ideal \((p)\). The residue field of \( \mathbb{Q}_p \) is isomorphic to the field \( \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \). The following lemma of commutative algebra shows that the field \( \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \) is isomorphic to the finite field \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \).

We conclude that \( \mathbb{Q}_p \) is a local field. So we can choose the representative system of \( \mathbb{F}_p \) as the set \( \Sigma = \{0, 1, \ldots, p-1\} \). Moreover \( p \) is an uniformizer of \( \mathbb{Q}_p \). We conclude that all \( p \)-adic integers can be written uniquely as a convergent series

\[
\sum_{n \geq 0} a_n p^n
\]

where \( a_n \in \{0, 1, \ldots, p-1\} \).

**Lemma 1.2.13.** Let \( A \) be a commutative ring and \( \mathfrak{p} \) be a maximal ideal of \( A \). Then, for all \( n \geq 1 \), the morphism \( A/\mathfrak{p}^n \rightarrow A/\mathfrak{p}^n A_p \) is an isomorphism.

**Remark 1.2.14.** Let \((K, |\cdot|)\) be a valued field. Then \( K \) is the fraction field of \( \mathcal{O} \). Moreover, if \( x \in \mathcal{O} \) is a nonzero element such that \( |x| < 1 \), then \( K = \mathcal{O}[x^{-1}] \). Namely, if \( y \in K \), there exists \( n \geq 1 \) such that \( |x|^n |y| \leq 1 \), and then \( x^ny \in \mathcal{O} \).

In particular, we have \( \mathbb{Q}_p = \mathbb{Z}_p[p^{-1}] \) and we conclude that all \( p \)-adic numbers can be written in unique form of a Laurent series

\[
\sum_{n=-N}^{+\infty} a_n p^n
\]

where \( a_n \in \{0, 1, \ldots, p-1\} \) and \( N \in \mathbb{N} \).
1.2.3 Structure of the valuation ring of local field

Let \((A_n)_{n \geq 0}\) be a sequence of sets endowed with maps \(\pi_{n,m} : A_m \to A_n\) for \(n \leq m\) such that \(\pi_{n,m} \circ \pi_{m,\ell} = \pi_{n,\ell}\) for all \(n \leq m \leq \ell\) and \(\pi_{n,n} = \text{Id}_{A_n}\) for all \(n \geq 0\). The projective limit of the family \(A_n\) is defined as the subset of \(\prod_{n \geq 0} A_n\) of sequences \((a_n)_{n \geq 0} \in \prod_{n \geq 0} A_n\) such that \(\pi_{n,m}(a_m) = a_n\) for all \(n \geq m\). We denote it by \(\lim\limits_{\leftarrow} A_n\).

If \(A_n\) are groups (resp. rings) and that \(\pi_n\) are morphisms of groups, then \(\lim\limits_{\leftarrow} A_n\) is naturally endowed with a structure of group (resp. rings). If groups are commutative, then their projective limit is commutative, same with the case of rings.

If the \(A_n\) are topological spaces and \(\pi_n\) are continuous, then we endow \(\lim\limits_{\leftarrow} A_n\) with the topology induced by the product topology on \(\prod_n A_n\). For example, we can endow \(A_n\) with the discrete topology, so \(\pi_n\) are automatically continuous.

Proposition 1.2.15. 1. If \(\pi_{n,m}\) are all surjective, then each application \(\pi_n : \lim\limits_{\leftarrow} A_n \to A_n\) is surjective.

2. If \(A_n\) are finite, then \(\lim\limits_{\leftarrow} A_n\) is a compact topological space.

Proof. Exercice.

Proposition 1.2.16. Let \(K\) a local field of the integer ring \(O\) and let \(\pi\) be a uniformizer of \(K\). There exists an isomorphism of topological rings

\[ O \xrightarrow{\sim} \lim\limits_{\leftarrow} O/(\pi^n). \]

Proof. Let \(\varphi\) be the application which sends \(x \in O\) to \((x \mod \pi^n)_{n \geq 0}\). It is clearly a morphism of rings. To verify that \(\varphi\) is continue, we have to show that the composition maps \(O \xrightarrow{\varphi} \lim\limits_{\leftarrow} O/(\pi^n) \xrightarrow{\pi_m} O/(\pi^m)\) are continuous for all \(m \geq 0\). The inverse image of a subset of \(O/(\pi^m)\) by \(\pi_m \circ \varphi\) is a finite intersection of closed balls of nonzero radius, it’s an open subset of \(O\). Thus \(\varphi\) is continuous.

The map \(\varphi\) is injective. Namely, if \(\varphi(x) = 0\), we have \(x \in \bigcap_{n \geq 0} (\pi^n)\) which makes \(|x| = 0\) and thus \(x = 0\). Since \(O\) is compact, the application \(\varphi\) induces a homeomorphism of \(O\) on its image which is closed in \(\lim\limits_{\leftarrow} O/(\pi^n)\). We only need to prove that this image is dense. Let \(x = (x_n)_{n \geq 0}\) be an element of \(\lim\limits_{\leftarrow} O/(\pi^n)\) and let \(U\) be a neighborhood of 0. By definition of the product topology, there exists an integer \(N \geq 0\) such that \((\prod_{n \geq N} O/(\pi^n)) \cap \lim\limits_{\leftarrow} O/(\pi^n) \subset U\). Then we have \(\varphi(x_N) - x \in U\), which proves that \(\varphi(O)\) is dense in \(\lim\limits_{\leftarrow} O/(\pi^n)\) and finishes the proof.

Example 1.2.17. If \(p\) is a prime, we have isomorphisms of topological rings

\[ \mathbb{Z}_p \simeq \lim\limits_{\leftarrow} \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \lim\limits_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}. \]
1.2.4 Extensions of complete fields

Let \((K, |·|)\) be a valued field. A normed \(K\)-vector space is a pair \((V, ||·||)\) where \(V\) is a \(K\)-vector space and \(||·|| : V \to \mathbb{R}_{\geq 0}\) is a map satisfying the following properties

- \(\forall v \in V, \text{ we have } ||v|| = 0 \iff v = 0;\)
- \(\forall (\lambda, v) \in K \times V, \text{ we have } ||\lambda v|| = |\lambda||v||;\)
- \(\forall (v, w) \in V^2, \text{ we have } ||v + w|| \leq ||v|| + ||w||.\)

Remark 1.2.18. When the absolute value \(||·||\) is ultrametric, we often request a stronger condition

\[
\forall (v, w) \in V^2, \quad ||v + w|| \leq \sup\{||v||, ||w||\}.
\]

Example 1.2.19. If \(n \in \mathbb{N}\), we can endow the vector space \(K^n\) with the norm

\[
||(x_1, \ldots, x_n)||_\infty = \sup\{|x_i|, i = 1, \ldots, n\}.
\]

If \(V\) is a finite dimensional \(K\)-vector space, we say that two norms \(||·||_1\) and \(||·||_2\) are equivalent if there exists two real numbers \(0 < C < C'\) such that

\[
C||·||_2 \leq ||·||_1 \leq C'||·||_2.
\]

Remark 1.2.20. On a \(K\)-vector space, two norms \(||·||_1\) and \(||·||_2\) are equivalent if and only if they define the same topology. Namely, if \(\overline{B}_1\) and \(\overline{B}_2\) are the respective unit balls, there exists two elements \(\varpi_1\) and \(\varpi_2\) of \(K\) such that

\[
\varpi_1\overline{B}_2 \subset \overline{B}_1 \subset \varpi_2\overline{B}_2.
\]

Proposition 1.2.21. Let \(K\) be a complete field and let \(V\) be a normed \(K\)-vector space of finite dimension \(n\). Then any \(K\)-linear isomorphism from \(K^n\) onto \(V\) is a homeomorphism. In particular, \(V\) is a complete metric space. On a finite dimensional \(K\)-vector space, all the norms are equivalent.

Proof. The last assertion is a consequence of the above remark and the completeness is a consequence of the first assertion. Namely if \(G\) and \(H\) are two isomorphic topological groups, \(H\) is complete if and only if \(G\) is complete (warning, this is not always true for an arbitrary metric space). We will prove the first assertion by induction on \(n\). Since all the \(K\)-linear automorphisms of \(K^n\) are continuous, we only need to show that there exists an automorphism of \(K^n\) which is a homeomorphism.

If \(n = 1\), this is clear: we choose a nonzero element \(v \in V\). Then we have \(V = Kv\) and we check immediately that the isomorphism \(\lambda \mapsto \lambda v\) from \(K\) to
1.2. COMPLETE FIELDS, LOCAL FIELDS

$V$ is a homeomorphism. Suppose that the result is proved for $n$ and let $V$ be a normed $K$-vector space of dimension $n + 1$. We choose a nonzero vector $v \in V$ and $W$ a supplement of $Kv$ in $V$. By recurrence, $W$ is a normed vector space of dimension $n$ and is complete. So it is a closed vector subspace of $V$. This implies that the projection $\mu$ of $V$ on $Kv$ parallel to $W$ is continuous and in particular that the $K$-linear application $V \to Kv \times W$ defined by $v \mapsto (\mu(v), v - \mu(v))$ is continuous. The converse map is clearly continuous. We conclude that the normed vector spaces $V$ and $K \times W$ are isomorphic as topological vector spaces.

**Theorem 1.2.22.** Let $(K, |\cdot|_K)$ be a complete valued field and let $L$ be a finite extension of $K$. Then there exists a unique norm on $L$ whose restriction to $K$ coincides with $|\cdot|_K$. Moreover $L$ is complete for this norm.

**Proof.** The uniqueness is a consequence of the precedent proposition.

Let $(e_1, \ldots, e_d)$ be a base of $L$ on $K$ such that $e_1 = 1$ and let $|\cdot|_1$ be the sup norm of $L$ on $K$ with respect to this choice of base. This means

$$\sum_{i=1}^{d} x_i e_i \bigg|_1 = \sup_{i=1\ldots d} |x_i|.$$

It is a norm of $K$-vector space on $L$ which induces the norm $|\cdot|$ on $K$. Moreover if we set $C = d \sup_{1 \leq i,j \leq d} |e_i e_j|$, we have $|xy|_1 \leq C|x|_1|y|_1$ for all $x$ and $y$ in $L$. For $x \in L$, we set

$$|x|_2 = \sup\{|xa|_1|a|_1^{-1} | a \in L^\times\}.$$

We check that it is a norm of $K$-vector space on $L$ which extends $|\cdot|_K$. The norm $|\cdot|_2$ is moreover submultiplicative, which means that $\forall x, y \in L |xy|_2 \leq |x|_1|y|_1$

Then we set, for $x \in L^\times$,

$$|x|_3 = \inf\{|x^n|_2^{\frac{1}{n}} | n \geq 1\}.$$

We check that $|\cdot|_3$ is a norm of $K$-vector space which extends $|\cdot|_K$, is submultiplicative and moreover has the property that $|x^n|_3 = |x|_3^n$ for all $x \in L$ and $n \geq 1$. Let's check the last property. We first prove that

$$|x|_3 = \lim_{n \to +\infty} |x^n|_2^{\frac{1}{n}}.$$

Let $x \in L^\times$, let $\varepsilon > 0$ and let $m$ such that $|x^m|_3^{\frac{1}{m}} \leq |x|_3 + \varepsilon$. Let $n \geq 1$ and let $n = qm + r$ be the euclidian division of $n$ by $m$, with $r < m$. We have

$$|x^n|_2 \leq |x^m|_2^{\frac{1}{m}} |x^r|_2$$
and

\[ |x^n|_2^{\frac{k}{2}} \leq (|x|_3 + \varepsilon)^m |x'|^{\frac{k}{2}}. \]

For \( n \) is big enough such that \( |x'|^{\frac{k}{2}} \leq (1 + \varepsilon) \) for all \( r < m \), we have

\[ |x^n|_2^{\frac{k}{2}} \leq (1 + \varepsilon)(|x|_3 + \varepsilon)^{1 - \frac{k}{2}}. \]

We conclude that the sequence \((|x^n|_2^{\frac{k}{2}})_{n \geq 1}\) converges to \(|x|_3\) and thus that \(|x^n|_3 = |x|^n_3\) for all \( n \geq 1 \). To check that \(|x|_3 \neq 0\) if \( x \neq 0 \) we can remark that \(|x^n_2|_3 x^{-n_2} \geq 1\), which implies \(|x|_3 x^{-1}_3 \geq 1\).

We have to prove that \(|\cdot|_3\) is multiplicative. We note first that \(|\cdot|_3\) is the unique norm of \(K\)-vector space on \(L\) such that \(|x^n|_3 = |x|^n_3\) for all \( x \in L \) and for all \( n \geq 1 \) and such that \(|1| = 1\). Namely two such norms have to be equivalent and we deduce easily that they have to be the same. Let \( a \in L^* \) and for all \( x \in L \), let

\[ |x|_a = \sup\{|xa^n|_3 a^{-n} | n \geq 1\}. \]

It is a norm of \(K\)-vector space on \(L\) which has the property \(|x^n|_a = |x|^n_a\) for all \( n \geq 1 \) and \( x \in L \). Moreover it induces \(|\cdot|_K\) on \(K\), so that that \(|\cdot|_a = |\cdot|_3\). As we easily check that \(|a x|_a = |a|_3 |x|_a\) for all \( x \in L \), for all \( a \in L^* \), we conclude that \(|\cdot|_3\) is multiplicative and is an extension of \(|\cdot|_K\) to \(L\).

\[ \square \]

**Corollary 1.2.23.** Let \((K, |\cdot|_K)\) a complete valued field and let \(\overline{K}\) a algebraically closure of \(K\). Then there exist an unique norm on \(\overline{K}\) which extends \(|\cdot|_K\).

### 1.2.5 Hensel Lemma

**Theorem 1.2.24.** Let \(K\) be an ultrametric complete field. Let \(f \in \mathcal{O}_K[X]\) and let \(x \in \mathcal{O}_K\) such that \(\left|\frac{f(x)}{f'(x)^2}\right| < 1\). Then there exists a unique \(y \in \mathcal{O}_K\) such that \(f(y) = 0\) and \(|y - x| \leq \left|\frac{f(x)}{f'(x)^2}\right|\).

**Proof.** Let \(\alpha_0 \in \mathcal{O}_K\) such that \(\left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1\). Set

\[ \alpha_1 := \alpha_0 - \frac{f(\alpha_0)}{f'(\alpha_0)}. \]

We have \(\frac{f(\alpha_0)}{f'(\alpha_0)} < |f'(\alpha_0)| \leq 1\) so that \(\alpha_1 \in \mathcal{O}_K\). Set

\[ \varepsilon_0 := |\alpha_1 - \alpha_0| = \left|\frac{f(\alpha_0)}{f'(\alpha_0)}\right|, \quad \eta_0 := |f'(\alpha_0)|. \]

**Lemma 1.2.25.** We have \(|f(\alpha_1)| \leq \varepsilon_0^2\) and \(|f'(\alpha_1)| = \eta_0\).
1.2. COMPLETE FIELDS, LOCAL FIELDS

Proof. Since \( f(\alpha_0 + X) \in \mathcal{O}_K[X] \), we have, with \( h := -\frac{f(\alpha_0)}{f'(\alpha_0)} \),

\[
f(\alpha_1) = f(\alpha_0) + hf'(\alpha_0) + h^2 R
\]

where \( R \in \mathcal{O}_K \). We conclude that

\[
|f(\alpha_1)| \leq |h|^2 = \varepsilon_0^2.
\]

Similarly

\[
f'(\alpha_1) \in f'(\alpha_0) + h\mathcal{O}_K
\]

which gives \( |f'(\alpha_1) - f'(\alpha_0)| \leq |h| = \varepsilon_0 \). Since \( \varepsilon_0 < \eta_0 = |f'(\alpha_0)| \), we have

\[
|f'(\alpha_1)| = |f'(\alpha_0)| = \eta_0.
\]

Consequently, we can conclude that

\[
\left| \frac{f(\alpha_1)}{f'(\alpha_1)} \right| \leq \frac{\varepsilon_0^2}{\eta_0} < \eta_0
\]

which makes \( \left| \frac{f(\alpha_1)}{f'(\alpha_1)} \right| \). This result makes it possible to define by induction a sequence of elements of \( \mathcal{O}_K \) by setting \( \alpha_{n+1} := \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)} \) for all \( n \geq 0 \). By setting

\[
\varepsilon_n := |\alpha_{n+1} - \alpha_n|,
\]

we have

\[
\forall n \in \mathbb{N}, \quad |f(\alpha_{n+1})| \leq \varepsilon_n^2, \quad |f'(\alpha_n)| = \eta_0, \quad \varepsilon_n < \eta_0.
\]

Thus \( \varepsilon_{n+1} \leq \frac{\varepsilon_n^2}{\eta_0} < \varepsilon_n \) and, by induction we obtain

\[
\forall n \in \mathbb{N}, \quad \varepsilon_n \leq \frac{\varepsilon_0^{2^n}}{\eta_0^{2^n-1}} = \eta_0 \left( \frac{\varepsilon_0}{\eta_0} \right)^{2^n}.
\]

Since \( \varepsilon_0 < \eta_0 \), we conclude that \( \varepsilon_n \to 0 \) and the sequence \( (\alpha_n)_{n \geq 0} \) converges to an element \( \alpha \in \mathcal{O}_K \) such that \( f(\alpha) = 0 \) and \( |\alpha - \alpha_0| \leq \varepsilon_0 = \frac{f(\alpha_0)}{f'(\alpha_0)} \). Starting with \( \alpha_0 = x \), we can choose \( y = \alpha \).

The uniqueness of \( y \) is left as an exercise. \( \square \)

Corollary 1.2.26. Let \( K \) a complete valued field. Let \( f \in \mathcal{O}_K[X] \) with reduction \( \overline{f} \in k[X] \). If \( \overline{\alpha} \in k \) is a root of \( \overline{f} \) such that \( \overline{f}(\overline{\alpha}) \neq 0 \), there exists a unique \( x \in \mathcal{O}_K \) lifting \( \overline{x} \) and such that \( f(x) = 0 \).

Let \( K \) be an ultrametric local field. Its residue field is a finite field \( \mathbb{F}_q \) of cardinal \( q \). Let \( \zeta \in \mathbb{F}_q^\times \). It’s a root of the polynomial \( f(X) = X^{q-1} - 1 \). Since \( f'(\zeta) \neq 0 \) in \( \mathbb{F}_q \), we conclude that there exists a unique element \( [\zeta] \in \mathcal{O}_K \) such that
Let \( K \) be an ultrametric complete valued field and let \( \overline{K} \) be an algebraic closure of \( K \). Let \( \alpha \) and \( \beta \) be two elements of \( \overline{K} \) such that \( \alpha \) is separable over \( K(\beta) \) and such that

\[
|\alpha - \beta| < \min\{|\alpha - \alpha'| \mid \pi_{\alpha,K}(\alpha') = 0, \alpha' \neq \alpha\}
\]

(\( \pi_{\alpha,K} \) being the minimal polynomial of \( \alpha \) over \( K \)). Then \( K(\alpha) \subset K(\beta) \).

**Proof.** Let \( \text{Gal}(\overline{K}/K(\beta)) \) be the group of automorphisms of \( \overline{K} \) which fix \( K(\beta) \). If \( K^s \) is the separable closure of \( K(\beta) \) inside \( \overline{K} \), we have \((K^s)^{\text{Gal}(\overline{K}/K(\beta))} = K(\beta) \). It is thus sufficient to prove that \( \alpha \) is fixed by all the elements of \( \text{Gal}(\overline{K}/K(\beta)) \). Let \( \sigma \in \text{Gal}(\overline{K}/K(\beta)) \). Then \( \sigma(\alpha) \) is a conjugate of \( \alpha \) over \( K(\beta) \) and thus over \( K \). As a consequence \( \pi_{\alpha,L}(\sigma(\alpha)) = 0 \) and we have

\[
|\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \beta + \beta - \alpha| = |\sigma(\alpha) - \sigma(\beta) + \beta - \alpha| \\
\leq \sup\{|\sigma(\alpha - \beta)|, |\beta - \alpha|\} = |\beta - \alpha| \\
< \min\{|\alpha - \alpha'| \mid \pi_{\alpha,K}(\alpha') = 0, \alpha' \neq \alpha\}.
\]

We conclude that \( \sigma(\alpha) = \alpha \) and thus that \( \alpha \in K(\beta) \). \( \square \)
Corollary 1.2.29. Let $K$ be an ultrametric complete valued field and let $P$ be an irreducible and separable polynomial of degree $d$. Let $||\cdot||$ be $K$-vector space norm over the space $K_d[X]$ of degree $\leq d$ polynomials. There exists some real number $\delta > 0$ such that, for $Q \in K_d[X]$ with $||P - Q|| < \delta$, then $Q$ is irreducible and separable and the fields $K[X]/(P)$ and $K[X]/(Q)$ are isomorphic.

Proof. We reduce ourselves easily to the case where $K$ separable and the fields $\mathbb{Q}$ number $p$ $K$ is isomorphic to $\mathbb{Q}$ continuous. There exists $\delta > 0$ such that, for $Q \in K_d[X]$ with $||P - Q|| < \delta$, then $Q$ is irreducible and separable and the fields $K[X]/(P)$ and $K[X]/(Q)$ are isomorphic.

Assume first that $K$ is nontrivial. To see $Q$, $\mathbb{Q}$ $K$ is nontrivial, and $K$ is nontrivial. Consequently it induces a place $v$ of $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to the place $v$ is denoted $\mathbb{Q}_v$ and is a closed subfield of $K$. Thus $K$ is a locally compact $\mathbb{Q}_v$-vector space and Riesz Theorem (see TD) implies that $K$ is a finite dimensional $\mathbb{Q}_v$-vector space. The absolute value of $K$ is not ultrametric then $\mathbb{Q}_v \simeq \mathbb{R}$ and $K$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. If $K$ is ultrametric, so is $\mathbb{Q}_v$ and there exists a prime number $p$ such that $\mathbb{Q}_v \simeq \mathbb{Q}_p$.

Assume from now that $K$ is characteristic $p$ for a prime number $p$. The residue field $k$ of $K$ is a finite field of cardinal $q$, which is a power of $p$. We have the Teichmüller lift $[\cdot] : k \mapsto K^\times$ that we extend to $k$ by $[0] = 0$. Then we have

1.2.7 Classification of local fields

Theorem 1.2.30. Let $K$ be a local field. Then $K$ is isomorphic to one of the following valued fields:

- $\mathbb{R}$ or $\mathbb{C}$ if $K$ is not ultrametric;
- a finite extension of $\mathbb{Q}_p$ for $p$ a prime number if $K$ has characteristic 0 and is ultrametric;
- $k((T))$ where $k$ is a finite field if $K$ has nonzero characteristic.

Proof. Assume first that $K$ has characteristic zero. Let $|\cdot|$ be an absolute value inducing the topology of $K$. The restriction of $|\cdot|$ to $\mathbb{Q}$ is nontrivial (on the contrary, $\mathbb{Q}$ would be isomorphic to a subfield of the residue field of $K$, which is finite). Consequently it induces a place $v$ of $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to the place $v$ is denoted $\mathbb{Q}_v$ and is a closed subfield of $K$. Thus $K$ is a locally compact $\mathbb{Q}_v$-vector space and Riesz Theorem (see TD) implies that $K$ is a finite dimensional $\mathbb{Q}_v$-vector space. The absolute value of $K$ is not ultrametric then $\mathbb{Q}_v \simeq \mathbb{R}$ and $K$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. If $K$ is ultrametric, so is $\mathbb{Q}_v$ and there exists a prime number $p$ such that $\mathbb{Q}_v \simeq \mathbb{Q}_p$.

Assume from now that $K$ has characteristic $p$ for a prime number $p$. The residue field $k$ of $K$ is a finite field of cardinal $q$, which is a power of $p$. We have the Teichmüller lift $[\cdot] : k \mapsto K^\times$ that we extend to $k$ by $[0] = 0$. Then we have
\[ xy = [x][y] \text{ for all } x \text{ and } y \text{ in } k. \] We have moreover \([x + y] = [x] + [y] \]. Namely it is sufficient to check that \([x + y] = 0\) when \(x + y = 0\) and a \(q - 1\)-root of 1 lifting \(x + y\) when \(x + y \neq 0\). The first case is clear since \(x = -y\) implies \([x] = [-y] = [-1][y] = -[y]\). The second case can be deduced from the relation

\[ ([x] + [y])^q = [x]^q + [y]^q = [x^q] + [y^q] = [x] + [y] \]

which is true in characteristic \(p\). This gives us a field homomorphism \([\cdot] : k \rightarrow K\). Choosing an uniformizer \(\pi\) of \(K\), we extend this morphism into a field homomorphism \(k((T)) \rightarrow K\) defined by

\[ \sum_{n \geq -N} a_n T^n \mapsto \sum_{n \geq -N} [a_n] \pi^n. \]

The unicity of the \(\pi\)-adic expansion of an element of \(K\) shows that it is an isomorphism of valued fields.

### 1.2.8 Haar measures and normalization of absolute values

Let \(X\) be a locally compact topological space, i.e. an Hausdorff topological such that each point has a basis of neighborhoods which are compact. A (positive) Radon measure over \(X\) is a measure \(\mu\) defined on a \(\sigma\)-algebra \(\mathcal{T}\) (“tribu” in french) containing the borelian \(\sigma\)-algebra such that:

- a) for all compact \(K \subset X\), we have \(\mu(K) < +\infty\);
- b) for all \(A \in \mathcal{T}\), \(\mu(A) = \inf\{\mu(U) \mid A \subset U, U \text{ open}\}\);
- c) for all open subset \(U\), \(\mu(U) = \sup\{\mu(K) \mid K \subset U, K \text{ compact}\}\).

If \(\mu\) is a Radon measure on \(X\), we can define a positive \(\mathbb{R}\)-linear form on the space \(C_c(X, \mathbb{R})\) of continuous function with compact support (positive means that \(\mu(f) \geq 0\) when \(f \geq 0\)). The map \(\mu \mapsto I_\mu\) induces a bijection between the set of Radon measures over \(X\) and the set of positive \(\mathbb{R}\)-linear forms over \(C_c(X, \mathbb{R})\).

If \(G\) is locally compact topological group, a left Haar measure over \(G\) is a Radon measure which is left invariant under left translation \(G\), i.e. for each measurable set \(A\), \(gA\) is measurable and \(\mu(gA) = \mu(A)\). We define similarly a right Haar measure.

**Theorem 1.2.31.** If \(G\) is a locally compact topological group, there exists a left Haar measure over \(G\) and this measure is unique up to multiplication by an element of \(\mathbb{R}_{>0}\).
Let $K$ be local field. A Haar measure over $K$ is an Haar measure for the locally compact topological group $(K, +)$. As $(K, +)$ is commutative, it is a left and right Haar measure.

**Example 1.2.32.**

a) If $K = \mathbb{R}$, the Lebesgue measure $dx$ is a Haar measure over $\mathbb{R}$. It is characterized by the property $dx([a, b]) = b - a$ for $a \leq b$.

b) If $K = \mathbb{C}$, we have an isomorphism of $\mathbb{R}$-vector spaces $\mathbb{C} \simeq \mathbb{R}^2$ given by $x + yi \mapsto (x, y)$. The measure $dx \otimes dy$ is a Haar measure over $\mathbb{C}$. It is characterized by the property $dx \otimes dy([a, b] \times [c, d]) = (b - a)(d - c)$.

c) If $K$ is an ultrametric local field and $\mu$ is a Haar measure over $K$, then $\mu(O) < +\infty$. Let $\pi$ be a uniformizer of $K$ and let $k$ be its residue field. If $n \geq N$, we can write

$$O = \prod_{(a_N, \ldots, a_{n-1}) \in k^{n-N}} \left( \sum_{i=N}^{n-1} \sum_{a \in k} [a] \pi^i \right) + \pi^n O.$$  

From the properties of a Haar measure, we have $\mu(a + \pi^n O) = \mu(\pi^n O)$ for all $a \in K$, so that

$$\mu(\pi^{-N} O) = |k|^{n-N} \mu(\pi^n O).$$

We deduce that $\mu(\pi^n O) = |k|^{-n} \mu(O)$ for all $n \in \mathbb{Z}$ and $\mu(a + \pi^n O) = |k|^{-n} \mu(O)$ for all $a \in K$ and $n \in \mathbb{Z}$. As every element of $K^\times$ can be written uniquely as $u\pi^n$ for some $u \in O^\times$ and $n \in \mathbb{Z}$, we see that

$$\forall a = u\pi^n \in K^\times, \quad \mu(a(-)) = |k|^{-n} \mu(-).$$

The previous computation shows that it is natural to normalize the absolute value of $K$ such that, the ultrametric case, $|\pi|_K = |k|^{-1}$. We say that $|\cdot|_K$ is the *normalized* absolute value over $K$. It has the property that

$$\forall a \in K^\times, \quad \mu(a(-)) = |a|_K^{-n} \mu(-).$$

**Remark 1.2.33.** In the archimedean case, we have, if $K = \mathbb{R}$, $dx(a(-)) = |a|_\infty dx$ so that the absolute value

$$|x|_\mathbb{R} = \sup\{x, -x\}$$

is normalized.

In the case of $\mathbb{C}$, we have $dx \otimes dy(a(-)) = |a\pi|_\mathbb{R} dx \otimes dy$. Even if the quantity $|a\pi|_\mathbb{R}$ does not define an absolute value over $\mathbb{C}$ (it does not satisfy the triangle inequality), we note it $|a|_C$ and call it the *normalized absolute value* over $\mathbb{C}$. It is only some power of the usual absolute value over $\mathbb{C}$. 

If $K$ is a local field, $|·|_K$ is the normalized absolute value over $K$ and $\mu$ is a Haar measure for $(K, \cdot)$, then $|·|_K^{-1}\mu$ is a Haar measure for the locally compact group $(K^\times, \cdot)$.

**Proposition 1.2.34.** Let $L/K$ be a finite extension of local fields. If $|·|_K$ and $|·|_L$ are the normalized absolute values of $K$ and $L$, then we have $|·|_K = \text{abs}_{K} N_{L/K}(-)$.  

**Proof.** We know that the unique absolute value of $L$ extending $|·|_K$ is $|·|_L = |N_{L/K}|^{1/[L:K]}$. This implies that there exists $\alpha \in \mathbb{R}_{>0}$ such that $|a|_L = |a|_K^{[L:K]}$ if $a \in K^\times$ so that we have $\alpha = 1$. \hfill $\square$

### 1.3 Places of global fields

**1.3.1 Extension of absolute values**

Let $L/K$ be a finite extension. Let $v$ be a place of $K$ and $|·|_v$ an absolute value associated to $v$. We note $K_v$ the completion of $K$ with respect to $|·|_v$ (which depends only on $v$). We say that a place $w$ of $L$ is an extension from $v$ to $L$ or yet above $v$ if any absolute value associated to restricted to $K$ is associated to $v$. We note this $w \mid v$. In this case, the closure of $K$ in $L_w$ is isomorphic to $K_v$ and provides a natural embedding of $K_v$ into $L_w$.

**Theorem 1.3.1.** 1) The place $v$ has at most $[L : K]$ distinct extensions to $L$: $w_1, \ldots, w_r$.

2) There exists a surjective morphism of $(L, K_v)$-algebras

$$f : L \otimes_K K_v \twoheadrightarrow \prod_{i=1}^{r} L_{w_i}.$$ 

3) If the extension $L/K$ is separable, then $f$ is an isomorphism and

$$[L : K] = \sum_{i=1}^{r} [L_{w_i} : K_v].$$

**Proof.** The ring $A := L \otimes_K K_v$ is a finite $K_v$-algebra. As a consequence its prime ideals are all maximal. Let’s show that they are finitely many. Namely if $p_1, \ldots, p_r$ are distinct such prime ideals of $A$, we have for all $1 \leq i \leq r$,

$$A = p_i + \prod_{j \neq i} p_j$$
(if not we would have \( \prod_{j \neq i} p_j \subset p_i \) and thus \( p_j \subset p_i \) for some \( j \neq i \) so that \( p_j = p_i \) by maximality). We deduce that the natural map

\[
f : A \hookrightarrow \prod_{i=1}^r A/p_i
\]

is surjective. Then \( r \leq \dim_{K_v} A = [L : K] \). Let \( p_1, \ldots, p_r \) be the list of the prime ideals of \( A \). Set \( L_i := A/p_i \) for \( 1 \leq i \leq r \). It is endowed with the structure of \( K_v \)-algebra provided by \( f \).

Let’s show that for all \( 1 \leq i \leq r \), \( L \) is dense in \( L_i \). The \( K_v \)-algebras \( A \) and \( L_i \) are finite dimensional and the map \( f \) is \( K_v \)-linear. As \( K_v \) is a complete field, it is thus continuous. The choice of a \( K \)-basis of \( L \) allows us to identify \( L \) with \( K^d \) and \( A \) with \( K_v^d \). The image of \( L \) in \( A \) by the map \( x \mapsto x \otimes 1 \) is then identified to \( K^d \) in \( K_v^d \) and is consequently dense in \( A \). As the map \( f \) is surjective, the image of \( L \) in \( \prod_i L_i \) is dense so that the image of \( L \) in \( L_i \) is dense. We can use this map to identify \( L \) with \( L_i \) with a dense subfield of \( L_i \). As \( L_i \) is a finite extension of \( K_v \), it has a unique place inducing the place \( v \) on \( K_v \). Therefore \( L_i \) induces a place \( w_i \) on \( L \) such that \( L_{w_i} \simeq L_i \).

Let’s show that the places \( w_1, \ldots, w_r \) are all distinct. Assume on the contrary that there exist \( 1 \leq i \neq j \leq r \) such that \( w_i = w_j \). This means that there exists an isomorphism \( \alpha : L_i \simeq L_j \) which is both \( L \)-linear and \( K_v \)-linear. Let \( p_{i,j} \) be the projection from \( A \) onto \( L_i \times L_j \). We thus have \( p_{i,j}(L) \subset \{(x,y) \in L_i \times L_j \mid \alpha(x) = y\} \). This is a sub-\( K_v \)-vector space, automatically closed so that \( p_{i,j}(A) \subset \{(x,y) \in L_i \times L_j \mid \alpha(x) = y\} \). This contradicts the surjectivity of \( p_{i,j} \).

Let’s show that all places of \( L \) above \( v \) is one of the \( w_i \). Let \( w \) be such a place. The injection of \( L \) into \( L_w \) and the embedding \( K_v \hookrightarrow L_w \) induce a morphism of \( K \)-algebras \( A = L \otimes_K K_v \hookrightarrow L_w \). The kernel of this morphism is a prime ideal of \( A \), and so it induces a morphism \( A \rightarrow L_i \hookrightarrow L_w \). By composing this map with the inclusion of \( L \) into \( A \), we obtain a sequence of embeddings

\[
L \hookrightarrow L_i \hookrightarrow L_w.
\]

As \( w \mid v \), the absolute value of \( L_w \) induces the unique place of \( L_i \) which is compatible to the topology of \( K_v \), so that the topology of \( L_i \) is induced by the topology of \( L_w \). As \( L_i \) is complete, it is closed inside \( L_w \). As \( L \) is dense in \( L_w \), we conclude that \( L_i \simeq L_w \) as topological fields and then that \( w = w_i \). Finally we proved assertion 1) and 2).

It remains to prove 3). Assume that the extension \( L/K \) is separable. There exists a polynomial \( P \in K[X] \) irreducible and separable such that \( L \simeq K[X]/(P) \). We have then \( L \otimes_K K_v \simeq K_v[X]/(P) \). As \( P \) is also separable in \( K_v[X] \), we deduce that \( A = L \otimes_K K_v \) is isomorphic to a product of fields and does not contain any nonzero nilpotent. The kernel of the map \( f \) is the intersection of the prime ideals of \( A \), i.e. the set of nilpotent elements of \( A \). We conclude that que \( f \) is injective. \( \square \)
1.3.2 The product formula

If $K$ is a local field and $v$ is a place of $K$, we note $|·|_v$ the unique normalized absolute value of $K$ whose equivalence class is $v$.

**Proposition 1.3.2.** Let $L/K$ be a separable finite extension of global fields. Let $x \in L$ and let $v$ be a place of $K$. Then we have

$$|N_{L/K}x|_v = \prod_{w|v} |N_{L_w/K_v}x| = \prod_{w|v} |x|_w.$$

**Proof.** By definition $N_{L/K}x$ is the determinant of the $K$-linear automorphism of $L$ defined by $y \mapsto xy$. After extension of scalars, this is also the determinant of the $K_v$-linear automorphism of $L \otimes_K K_v$ defined by $y \mapsto (x \otimes 1)y$. The formula $L \otimes_K K_v \simeq \prod_{v|w} L_w$ shows that

$$|N_{L/K}x|_v = \prod_{w|v} |N_{L_w/K_v}x| = \prod_{w|v} |x|_w. \quad \square$$

**Theorem 1.3.3** (Product formula). Let $K$ be a global field and let $x \in K^\times$.

1) We have $|x|_v = 1$ for almost all place $v$ (i.e. for all except a finite number of them).

2) We have $\prod_v |x|_v = 1$.

**Proof.** We first prove the following lemma.

**Lemma 1.3.4.** Let $x \in K$. Then $|x|_v \leq 1$ for almost all $v$.

**Proof.** Let’s start with the case where $K$ is a number field. Let $x \in K$. As $K \simeq \mathcal{O}_K \otimes \mathbb{Z} \mathbb{Q}$, there exists a nonzero $m \in \mathbb{Z}$ such that $mx \in \mathcal{O}_K$. If $v$ is an ultrametric place of $K$, it is above an ultrametric place of $\mathbb{Q}$ corresponding to a prime number $p$. As $|\mathbb{Z}|_p \leq 1$ and elements of $\mathcal{O}_K$ are integral over $\mathbb{Z}$, we have $|\mathcal{O}_K|_v \leq 1$. Moreover $|m|_p = 1$ for almost all prime numbers $p$ and, there are only finitely many places $v$ of $K$ above each prime number so that $|m|_v = 1$ for almost all place $v$ of $K$. As there are only finitely many places of $K$ which are archimedean (i.e. above $\infty$), we have $|x|_v \leq 1$ for almost all $v$.

The case of a function field is similar if we replace $\mathbb{Q}$ by $k(T)$ and $\mathbb{Z}$ by $k[\mathbb{T}]$ where $k$ is a finite field. Namely there are only finitely many places $v$ of $K$ such that $|k[T]|_v \leq 1$. \quad \square

The lemma implies immediately part 1) of the theorem. Namely we can apply the lemma to $x$ and to $x^{-1}$. 

2) We have $\prod_v |x|_v = 1$. 

**Proof.** We prove this in two steps. 

1) Let $x \in K$. Then $|x|_v \leq 1$ for almost all $v$.

2) Let $x \in K$.

**Proof.** We start with the case where $K$ is a number field. Let $x \in K$. As $K \simeq \mathcal{O}_K \otimes \mathbb{Z} \mathbb{Q}$, there exists a nonzero $m \in \mathbb{Z}$ such that $mx \in \mathcal{O}_K$. If $v$ is an ultrametric place of $K$, it is above an ultrametric place of $\mathbb{Q}$ corresponding to a prime number $p$. As $|\mathbb{Z}|_p \leq 1$ and elements of $\mathcal{O}_K$ are integral over $\mathbb{Z}$, we have $|\mathcal{O}_K|_v \leq 1$. Moreover $|m|_p = 1$ for almost all prime numbers $p$ and, there are only finitely many places $v$ of $K$ above each prime number so that $|m|_v = 1$ for almost all place $v$ of $K$. As there are only finitely many places of $K$ which are archimedean (i.e. above $\infty$), we have $|x|_v \leq 1$ for almost all $v$.

The case of a function field is similar if we replace $\mathbb{Q}$ by $k(T)$ and $\mathbb{Z}$ by $k[\mathbb{T}]$ where $k$ is a finite field. Namely there are only finitely many places $v$ of $K$ such that $|k[T]|_v \leq 1$. \quad \square

The lemma implies immediately part 1) of the theorem. Namely we can apply the lemma to $x$ and to $x^{-1}$. 

2) We have $\prod_v |x|_v = 1$. 

**Proof.** We prove this in two steps. 

1) Let $x \in K$. Then $|x|_v \leq 1$ for almost all $v$.

2) Let $x \in K$.

**Proof.** We start with the case where $K$ is a number field. Let $x \in K$. As $K \simeq \mathcal{O}_K \otimes \mathbb{Z} \mathbb{Q}$, there exists a nonzero $m \in \mathbb{Z}$ such that $mx \in \mathcal{O}_K$. If $v$ is an ultrametric place of $K$, it is above an ultrametric place of $\mathbb{Q}$ corresponding to a prime number $p$. As $|\mathbb{Z}|_p \leq 1$ and elements of $\mathcal{O}_K$ are integral over $\mathbb{Z}$, we have $|\mathcal{O}_K|_v \leq 1$. Moreover $|m|_p = 1$ for almost all prime numbers $p$ and, there are only finitely many places $v$ of $K$ above each prime number so that $|m|_v = 1$ for almost all place $v$ of $K$. As there are only finitely many places of $K$ which are archimedean (i.e. above $\infty$), we have $|x|_v \leq 1$ for almost all $v$.

The case of a function field is similar if we replace $\mathbb{Q}$ by $k(T)$ and $\mathbb{Z}$ by $k[\mathbb{T}]$ where $k$ is a finite field. Namely there are only finitely many places $v$ of $K$ such that $|k[T]|_v \leq 1$. \quad \square

The lemma implies immediately part 1) of the theorem. Namely we can apply the lemma to $x$ and to $x^{-1}$. 

2) We have $\prod_v |x|_v = 1$. 

**Proof.** We prove this in two steps. 

1) Let $x \in K$. Then $|x|_v \leq 1$ for almost all $v$.

2) Let $x \in K$.
Let's prove part 2). We remark that if $K/K_0$ is a finite separable extension of global fields, the product formula for $K_0$ implies the product formula for $K$. Namely, if the product formula is true for $K_0$ and $x \in K^\times$, we have

$$\prod_w |x|_w = \prod_v |x|_w = \prod_v |N_{L/K}x|_v = 1$$

since $N_{L/K}x \in K^\times$. If $K$ is a number field, then $K$ is a finite separable extension of $\mathbb{Q}$. Therefore it is sufficient to prove the formula for $\mathbb{Q}$. If $x \in \mathbb{Q}^\times$, we can write $x = \pm \prod_p p^{\alpha_p}$. We have $|x|_\infty = \prod_p p^{\alpha_p}$ and $|x|_p = p^{-\alpha_p}$ so that the product formula is satisfied.

If $K$ is a function field, there exists a separable extension $K/k(T)$ (exercice) where $k = \mathbb{F}_q$ is a finite field. It is sufficient to check the product formula for the fields $k(T)$ with $k$ a finite field. The places of $k(T)$ are indexed by the unitary irreducible polynomials $P$ of $\mathbb{F}_q[T]$ and by $T^{-1}$. Let $x = \varepsilon \prod_p P^{\alpha_p} \in k(T)^\times$ with $\varepsilon \in k^\times$. As $\mathbb{F}_q[T]/(P) \cong \mathbb{F}_{q^{\deg P}}$, we have $|x|_P = q^{-\alpha_p \deg P}$. Moreover $|x|_{T^{-1}} = q^{\deg x}$ so that

$$|x|_{T^{-1}} \prod_P |x|_P = 1.$$

\[ \qed \]

### 1.3.3 Archimedean places of number fields

Let $K$ be a number field. This is a finite extension of $\mathbb{Q}$ and let $d$ be its degree. The integer $d$ is equal to the number of different fields embeddings of $K$ into $\mathbb{C}$. Such an embedding is called to be real if its image is contained in $\mathbb{R}$. It is called complex if not. The complex conjugation over $\mathbb{C}$ acts without fixed point on the set of complex embeddings so that there is an even number $2r_2$ of complex embeddings. If $r_1$ is the number of real embeddings, we have $d = r_1 + 2r_2$. Let $j_1, \ldots, j_{r_1}$ be the real embeddings of $K$ in $\mathbb{C}$ and $j_{r_1+1}, j_{r_1+1}, \ldots, j_{r_1+r_2}, j_{r_1+r_2}$ be the complex embeddings.

**Theorem 1.3.5.** The archimedean places of $K$ are the equivalence classes of the following absolute values

$$x \mapsto |j_k(x)|_\mathbb{C}, \quad k = 1, \ldots, r_1 + r_2.$$ 

**Proof.** Let $j$ be diagonal embedding $K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ given by $x \mapsto (j_1(x), \ldots, j_{r_1+r_2}(x))$. It induces a morphism $K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. We have to check that this morphism is an isomorphism. It is sufficient to check this after base change from $\mathbb{R}$ to $\mathbb{C}$:

$$K \otimes_{\mathbb{Q}} \mathbb{C} \to \mathbb{C}^{r_1} \times (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C})^{r_2} \cong \mathbb{C}^{r_1} \times \mathbb{C}^{2r_2} \cong \mathbb{C}^d.$$ 

The composite map is given by $x \otimes 1 \mapsto (\sigma(x))_{\sigma:K \to \mathbb{C}}$. Therefore it is sufficient to check that there exists a $\mathbb{Q}$-basis $(e_1, \ldots, e_d)$ of $K$ such that the images of the
CHAPTER 1. GLOBAL AND LOCAL FIELDS

$e_i \otimes 1$ is a $\mathbb{C}$-basis of $\mathbb{C}^d$, i.e. that the $d \times d$-matrix $(\sigma(e_i))$ is invertible. This is a direct consequence of the fact the maps $\sigma$ form a $\mathbb{C}$-free family of maps from $K$ to $\mathbb{C}$.

\[ \square \]

1.4 Ramification

1.4.1 Dedekind rings

A Dedekind ring is a commutative ring $A$ which is noetherian, normal and of Krull dimension 1 (i.e. its maximal ideals are exactly the nonzero prime ideals). Let’s recall that a commutative ring $A$ is normal if it is a domain and of every element of its fraction field which is integral over $A$ is in $A$. For example factorial rings, principal ideal domains etc. are normal. A principal ideal domain (PID) is a Dedekind ring (if its not a field). A fractional ideal of a Dedekind ring $A$ is a finitely generated $A$-submodule of its fraction field. If $p$ is a maximal ideal of ring $A$, the quotient $A/p$ is, by definition, a field called the residue field at $p$ and denoted $k(p)$.

If $I$ and $J$ are two fractional ideals of $A$, there product $IJ$ is the $A$-submodule of the fraction field $K$ of $A$ generated by products of elements in $I$ and $J$. This is also the image of the product map $I \otimes_A J \rightarrow K$.

Here the property of “unique factorization for ideals” in Dedekind rings.

Theorem 1.4.1. Let $A$ be a Dedekind ring.

1. Each maximal ideal $p$ of $A$ is invertible, i.e. there exists a fractional ideal $p^{-1}$ of $A$ such that $pp^{-1} = A$.

2. Each nonzero fractional ideal of $A$ can be uniquely written as a product of maximal ideals. Equivalently, the following map is an isomorphism from the free abelian group generated by the maximal ideals of $A$ to the abelian group of fractional ideals of $A$:

\[ \sum_p n_p p \mapsto \prod_p p^{n_p}. \]

If $I$ and $J$ are two nonzero ideals of $A$, we say that $I$ divides $J$ if $J \subseteq I$. Equivalently there exists an ideal $I'$ of $A$ such that $J = II'$.

A fractional ideal of $A$ is a fractional ideal generated by one elements as an $A$-module. They form a subgroup $P_A$ of the group $I_A$ of nonzero fractional ideals of $A$. Their quotient $I_A/P_A$ is called the class group of $A$.

Let $p$ be a maximal ideal of $A$. We can define a discrete valuation $v_p$ on the fraction field $K := \text{Frac } A$ sending a nonzero element $a \in K$ on the exponent $v_p(a)$ of the principal ideal $(a)$. Choosing a real number $0 < \varepsilon < 1$, we can define an
1.4. RAMIFICATION

absolute value \(|\cdot|_p\) on \(K\). This is an ultrametric discrete absolute value whose associated place depends only on \(p\) on not on \(\varepsilon\). We note \(K_p\) the completion of \(K\) for this absolute value.

**Lemma 1.4.2.** The valuation ring (i.e. closed unit ball) of \(K\) for \(|\cdot|_p\) is the ring \(A_p\). As a consequence the localization of the Dedekind ring \(A\) at a maximal ideal is a principal ideal domain. Moreover we have

\[
\{ x \in K \mid |x|_p < 1 \} = p A_p.
\]

**Proof.** The inclusion \(A_p \subset B(0,1)\) is easy. Conversely assume that \(x = \frac{a}{b} \in K\) is such that \(|x|_p \leq 1\), with \(a, b \in A\). In terms of ideals, this means that there exist two ideal \(c_1\) and \(c_2\), prime to \(p\), and an integer \(m \geq 0\) such that \((a)c_1 = (b)c_2 p^m\).

As \(c_1 \not\subset p\), there exists \(d \in c_1 \setminus p\). Then \(ad \in (b)\) so that we can write \(ad = bc\) for some \(c \in A\). Finally we have \(x = \frac{a}{b} = \frac{c}{d}\) with \(d \notin p\), i.e. \(x \in A_p\). The last equality follows similarly. \(\square\)

### 1.4.2 Extensions

Let \(A\) be a Dedekind ring. Let \(K\) be its fraction field and \(L\) a finite extension of \(K\). Let \(B\) be the integral closure of \(A\) in \(L\), that it the set of all elements of \(L\) which are integral over \(A\). This is clearly a normal subring of \(L\) and \(L\) is the fraction field of \(B\). We can even show a stronger result: \(L \simeq B \otimes_A K\), or equivalently for all \(x \in L\), there exists \(m \in A \setminus \{0\}\) such that \(mx \in B\).

From now, we make the following hypothesis: \(B\) is a finitely generated \(A\)-module.

**Theorem 1.4.3.** If \(B\) is a finitely generated \(A\)-module, then \(B\) is a Dedekind ring.

**Proof.** As \(B\) is a finitely generated \(A\)-module, then \(B\) is noetherian \(A\)-module and so a noetherian \(B\)-module, this is then a noetherian ring. It is normal by definition, it is thus sufficient to prove that a nonzero prime ideals \(q\) of \(B\) is maximal and that \(B\) is not field (so that 0 is not a maximal ideal). The ideal \(p := q \cap A\) is a nonzero prime ideal of \(A\). Namely, if \(x \in q \setminus \{0\}\), let \(P = X^d + a_1 X^{d-1} + \cdots + a_d\) be the minimal polynomial of \(x\) over \(K\). As all conjugate of \(x\) over \(K\) are in \(B\), this is a unitary polynomial of \(A[X]\) and its constant term \(a_d\) is non zero (if not \(P\) wouldn’t be irreducible in \(K[X]\)). As \(x \in \mathfrak{p} \in q\), we have

\[
0 \neq a_d = -x^d - a_1 x^{d-1} - \cdots - a_1 x \in \mathfrak{p}
\]

so that \(\mathfrak{p} \neq 0\). As \(A\) is Dedekind, \(\mathfrak{p}\) is a maximal ideal of \(A\) and \(B/q\) is a finite \(A/p\)-algebra which is moreover a domain. Hence it is a field and \(q\) is maximal. \(\square\)

Here are some example of cases where \(B\) is a finitely generated \(A\)-module.
Lemma 1.4.4. Let $L/K$ be a finite extension of field and let $b$ be the $K$-bilinear form on $L$ defined by $b(x, y) = \text{Tr}_{L/K}(xy)$. The extension $L/K$ is separable if and only if the form $b$ is non degenerate.

Proof. Let $(e_1, \ldots, e_d)$ be a $K$-basis of $L$. The form $b$ is non degenerate if and only if the $d \times d$-matrix $M = (\text{Tr}_{L/K}(e_ie_j))$ is invertible. Let $\Sigma$ be the set of $K$-embeddings of $L$ into an algebraic closure of $\overline{K}$.

Assume that the extension $L/K$ is separable. Then $\Sigma$ has cardinal $d$ and $\text{Tr}_{L/K} = \sum_{\sigma \in \Sigma} \sigma$ and $M = tNN$ where $N = (\sigma(e_i))_{\sigma \in \Sigma, 1 \leq i \leq d}$. Then $\det(M) = \det(N)^2$. The morphisme $\sigma : L^* \to \overline{K}^*$ are distinct characters and, by linear independance of characters, they form a $\overline{K}$-free family of maps from $L$ to $\overline{K}$. This implies that $\det(N) \neq 0$ and thus $\det(M) \neq 0$, that is the form $n$ is non degenerate. If $L/K$ is not separable, then $\text{Tr}_{L/K} = 0$. Namely if $K^1$ is the separable closure of $K$ in $L$, then $L/K^1$ is purely inseparable and nontrivial. If $x \in L$, its minimal polynomial over $K^1$ is of the form $X^p - a$ and so is its characteristic polynomial. This proves that $\text{Tr}_{L/K^1} = 0$ and that $\text{Tr}_{L/K} = \text{Tr}_{K^1/K} \circ \text{Tr}_{L/K^1} = 0$. 

Proposition 1.4.5. If $L$ is a separable extension of $K$, then $B$ is a finitely generated $A$-module.

Proof. If $L$ is a separable extension of $K$, the $K$-bilinéaire form $b : (x, y) \mapsto \text{Tr}_{L/K}(xy)$ is nondegenerate. If $M$ is an $A$-submodule of $L$, we define $M^* := \{x \in K \mid \text{Tr}(xM) \subset A\}$. Let $(e_1, \ldots, e_d)$ be a basis of $L$ over $K$. As $b$ is nondegenerate, there exists a $K$-basis $(e^*_1, \ldots, e^*_d)$ of $L$ such that $b(e_i, e^*_j) = \delta_{i,j}$ for all $1 \leq i, j \leq d$.

It is easy to check that

$$\left( \bigoplus_i A e_i \right)^* = \bigoplus_i A e^*_i.$$

As $L \simeq B \otimes_A K$, we can choose a $K$-basis $(e_1, \ldots, e_d)$ of $L$ over $K$ such that the $e_i$ are in $B$. In this situation, we have

$$\bigoplus_i A e_i \subset B \subset B^* \subset \bigoplus_i A e^*_i.$$

Consequently $B$ is a $A$-submodule of a finitely generate $A$-module. As $A$ is noetherian, $B$ is a finitely generated $A$-module. 

Example 1.4.6. Let $K$ be a number field and let $\mathcal{O}_K$ the ring of integers of $K$. Then $\mathcal{O}_K$ is a Dedekind ring. Moreover it is a finite free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proposition 1.4.7. Let $A = k[T]$ where $k$ is a perfect field of characteristic $p$. Then $B$ is a finitely generated $A$-module.
Proof. Let \( M \) be the normal closure of \( L/K \) and let \( C \) be the integral closure of \( A \) in \( C \). We have \( B \subset C \) and, if \( C \) is a finitely generated \( A \)-module, so is \( B \) since \( A \) is noetherian. We are therefore reduce to prove the claim when \( L \) is a normal extension of \( K \). In this case, there exits a subfield \( K \subset N \subset L \) such that \( L \) is a separable extension of \( N \) and \( N \) is a purely inseparable extension of \( K \) (take for \( N \) the subfield fixed by the group \( \text{Aut}_K(L) \) of automorphisms of \( L \) which fix \( K \)). Let \( D \) be the integral closure of \( A \) in \( N \). Then \( B \) is the integral closure of \( D \) in \( L \). As \( L \) is a separable extension of \( N \), the ring \( B \) is a finitely generated \( D \)-module by Proposition 1.4.5. If \( D \) is a \( A \)-module of finite type, then \( B \) is a finitely generated \( A \)-module. We are reduced to prove the claim when \( L \) is a purely inseparable extension of \( K \).

Now we assume that \( L/K \) is purely inseparable. Reasoning by induction on the degree of \( L \) over \( K \), we can assume that \( L \) is a finite extension of \( K \) generated by an element \( x \in L \) such that \( x^p \in K \) (and \( [L : K] = p \)). We are in the case where \( K = k(T) \) and \( k \) is a perfect field, this implies that \( x \) can be written \( P(T^1/p) \) with \( P(T) \in k(T) \) so that \( L \subset k(X^{1/p}) \) and even \( L = k(X^{1/p}) \) for degree reasons. The ring of integers of \( L \) over \( k[X] \) is easily checked to be the subring \( B = k[X^{1/p}] \) so that it is a finite free \( A \)-module of rank \( p \).

Corollary 1.4.8. Let \( K \) be a finite extension of \( \mathbb{F}_q(X) \). Then the integral closure of \( \mathbb{F}_q[T] \) in \( K \) is Dedekind and finitely generated as an \( \mathbb{F}_q[T] \)-module.

Proposition 1.4.9. Let \( (K, |·|_K) \) be a complete ultrametric valued field for a discrete absolute value and let \( A = \mathcal{O}_K \). Then \( B = \mathcal{O}_L \) and \( B \) is a finitely generated \( A \)-module.

Proof. The fact that \( B = \mathcal{O}_L \) is left as an exercise. Let \((e_1, \ldots, e_d)\) be a \( K \)-basis of \( L \). Let \(|·|_L\) be the absolute value of \( L \) extending \(|·|_K\) and let \(|·|\) be the \( K \)-linear norm on \( L \) defined by

\[
|| \sum_{i=1}^d a_i e_i || := \sup \{|a_i|_K\}.
\]

As \( K \) is complete and \( L \) is a finite dimensional \( K \)-vector space, all the \( K \)-linear norms over \( L \) are equivalent, there exists \( C > 0 \) such that

\[
\mathcal{O}_L = \{x \in L \mid |x|_L \leq 1\} \subset \{x \in L \mid ||x|| \leq C\}.
\]

Let \( \alpha \in K \) such that \( |\alpha| \geq C \), then we have

\[
\mathcal{O}_L \subset \bigoplus_{i=1}^d \mathcal{O}_K \alpha e_i.
\]

This proves that \( \mathcal{O}_L \) is an \( \mathcal{O}_K \)-submodule of a finitely generated \( \mathcal{O}_K \)-module. As \( \mathcal{O}_K \) is noetherian, the \( \mathcal{O}_K \)-module \( \mathcal{O}_L \) is finitely generated. \( \square \)
From now on we will always assume that we are in a situation where \( B \) is a finitely generated \( A \)-module. As seen previously, this is the case in the following cases:

- if \( L/K \) is separable;
- if \( A = k[X] \) with \( k \) perfect;
- if \( K \) is a complete ultrametric for a discrete absolute value.

Let \( p \) be a maximal ideal of \( A \). Then \( pB \) is a nonzero ideal of \( B \). It can be uniquely decomposed as a product of maximal ideals of \( B \):

\[
pB = \prod_q q^{e_q}.
\]

We will say that a maximal ideal \( q \) of \( B \) is a divisor of \( p \) if \( q \) is a divisor of \( pB \) in \( B \) or equivalently that \( e_q \geq 1 \). We also says that \( q \) is above \( p \), and we use the notation \( q \mid p \). The integer \( e_q \) is called the ramification index of \( q \) in \( L/K \). As \( B \) is a finite \( A \)-module, the field extension \( k(q)/k(p) \) is finite. Its index \( f_q := [k(q) : k(p)] \) is called the residual degree. If \( e_q = 1 \) and \( k(q)/k(p) \) is a separable extension we say that the extension \( L/K \) is unramified at \( q \). In the other case, we say that the extension is ramified.

**Proposition 1.4.10.** If \( p \) is a maximal ideal of \( A \), we have

\[
[L : K] = \sum_{q \mid p} f_q e_q.
\]

**Proof.** Let \( q_1, \ldots, q_r \) be the maximal ideals of \( B \) dividing \( p \) and set \( e_i = e_{q_i} \). As the \( q_i \) are distinct maximal ideals, we have, for each \( i \),

\[
q_i^{e_i} + \bigcap_{j \neq i} q_j^{e_j} = B
\]

so that the map \( B \to \prod_i B/q_i^{e_i} \) is surjective and its kernel is equal to \( \bigcap_i q_i^{e_i} = \prod_i q_i^{e_i} = p \). We deduce an isomorphism de \( A \)-algebras

\[
B/pB \cong \prod_i B/q_i^{e_i}.
\]

If \( I \) is a nonzero ideal of \( B \) and \( q \) a maximal ideal, there is no ideal strictly contained between \( I \) and \( Iq \) so that \( I/Iq \) is a 1-dimensional \( Bq \)-vector space and thus an \( f_q \)-dimensional \( A/p \)-vector space. Considering the decreasing sequence of ideals

\[
B \supseteq q_1 \supseteq q_1^2 \supseteq \cdots \supseteq q_1^{e_1} \supseteq q_1^{e_1} q_2 \supseteq \cdots \supseteq q_1^{e_1} \cdots q_r^{e_r} = p,
\]
1.4. RAMIFICATION

we see that $B/B_p$ is a successive extension of $e_{q_i}$-vector spaces of dimension $f_{q_i}$ for $1 \leq i \leq r$. This proves that

$$\dim_{A/p} B/B_p = \sum_{i=1}^{r} e_{q_i} f_{q_i}.$$ 

To finish the proof, we will show that $B/B_p$ is a $k(p) = A/p$-vector space of dimension $[L : K]$. The idea is to localize the situation in $p$. Namely $A_p$ is a principal ideal domain. Then $B_p \simeq B \otimes_A A_p$ is a finitely generated $A_p$-module which is torsion-free (contained in $L = \text{Frac} B$) and is consequence finite free. Moreover $L \simeq B \otimes_A K \simeq B_p \otimes_{A_p} K$ so that the rank of $B_p$ as an $A_p$-module is equal to $[L : K]$. Moreover

$$B_p/pB_p \simeq B \otimes_A (A_p/pA_p) \simeq B \otimes_A (A/p) \simeq B/pB$$

which proves that $\dim_{k(p)}(B/pB) = [L : K]$ and gives the desired formula. $\square$

Example 1.4.11. a) Assume that $B$ is generated by 1 element as an $A$-algebra, that is $B = A[x]$. Let $P \in A[X]$ be the minimal polynomial of $x$ over $K$ so that $B \simeq A[X]/(P)$. Let $p$ be a maximal ideal of $A$. The maximal ideals of $B$ dividing $p$ are in bijection with the maximal ideals of the ring $B/pB \simeq k(p)[X]/(\overline{P})$ where $\overline{P}$ is the image of $P$ in $k(p)[X]$. Let $\overline{P} = \prod_{i=1}^{r} P_i^{e_i} \in \text{factorization of } \overline{P}$ as a product of irreducible polynomial. We have

$$B/pB \simeq \prod_{i=1}^{r} k(p)[X]/(P_i^{e_i})$$

so that the maximal ideals of $B/pB$ are the $(P_i)$ and the maximal ideals of $B$ dividing $p$ are the $q_i := p + (\overline{P}_i(x))$ where $\overline{P}_i \in A[X]$ is a lift of $P_i$. We have $B/q_i \simeq k(p)[X]/(P_i)$ so that $f_{q_i} = \deg(P_i)$. Moreover $\prod_{i} q_i^{e_i} \subset pB$ and the equality $\sum_{i} e_if_{q_i} = \dim_{k(p)} B/pB$ implies that $pB = \prod_{i} q_i^{e_i}$ showing that $e_i = e_{q_i}$.

b) We consider the case where $A = \mathbb{Z}$, $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{5})$. Then $B = \mathbb{Z}[(1+\sqrt{5})/2] \simeq \mathbb{Z}[X]/(X^2 - X - 1)$. In $\mathbb{F}_{11}[X]$, we have $X^2 - X - 1 = (X - 4)(X + 3)$ so that $(11) = q_1q_2$ in $B$ with $q_1 = (11, 1+\sqrt{5}/2 + 3)$ and $q_2 = (11, 1+\sqrt{5}/2 - 4$. The extension $L/K$ is unramified at $q_1$ and $q_2$.

c) Let $p$ be a prime number, $A = \mathbb{Z}$, $L = \mathbb{Q}(\zeta_p)$ where $\zeta_p$ is a primitive root of 1. The minimal polynomial of $\zeta_p$ on $\mathbb{Q}$ is $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ and we can prove that the ring of integers $B = \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ of $L$ is $\mathbb{Z}[[\zeta_p]] \simeq \mathbb{Z}[X]/(\Phi_p)$. We want to understand the decomposition of $(p)$ in $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. We have

$$\mathbb{Z}[[\zeta_p]]/(p) \simeq \mathbb{F}_p[X]/(\Phi_p)$$
and $\Phi_p = \frac{X^{p-1}}{X-1} = \frac{(X-1)^p}{X-1} = (X - 1)^{p-1}$ dans $\mathbb{F}_p[X]$. This shows that there is a unique maximal ideal $q$ of $\mathbb{Z}[\zeta_p]$ over $(p)$, that is $q = (p, \zeta_p - 1)$. Moreover this ideal is totally ramified of ramification index $p - 1$ and residual degree 1. Let’s remark that we are in a case where the maximal ideal $q$ is principal. Namely, we have $\Phi_p(X) = \prod_{i=1}^{p-1} (X - \zeta_p^i)$ so that $p = \Phi_p(1) = \prod_{i=1}^{p-1} (1 - \zeta_p^i)$. This shows that $p \in (\zeta_p - 1)$ and $q = (\zeta_p - 1)$. The decomposition of $p$ in $\mathbb{Z}[\zeta_p]$ is consequently given by $$(p) = (\zeta_p - 1)^{p-1}.$$  

### 1.4.3 Galois extensions

Let $A$ be a Dedekind ring, $K$ its fraction field and $L$ a Galois extension of $K$. Let $B$ be the integral closure of $A$ in $L$. It is a finitely generated $A$-module by Proposition 1.4.5. As the conjugate of an integral element over $A$ is integral over $A$, the action of the Galois group $\text{Gal}(L/K)$ over $L$ preserves the subring $B$. Moreover if $q$ is a maximal ideal of $B$ and $\sigma \in \text{Gal}(L/K)$, we have

$$\sigma(q \cap A) = q \cap A = \sigma(q) \cap A$$

so that $\sigma(q)$ is another maximal ideal dividing $p := q \cap A$. Therefore, for any maximal ideal $p$ of $A$, the action of the group $\text{Gal}(L/K)$ preserves the finite set of maximal ideals of $B$ dividing $p$.

**Proposition 1.4.12.** For any maximal ideal $p$ of $A$, the action of $\text{Gal}(L/K)$ on the set of divisors of $p$ is transitive.

**Proof.** Let $q$ be a maximal ideal of $B$ dividing $p$ and assume that there exists a maximal ideal $q'$ different from all the $\sigma(q)$, $\sigma \in \text{Gal}(L/K)$. We have

$$B = q' + \bigoplus_{\sigma \in \text{Gal}(L/K)} \sigma(q)$$

so that we can decompose $1 = x + y$ with $x \in q'$ and $y \in \sigma(q)$ for all $\sigma \in \text{Gal}(L/K)$. This implies that $x \in q' \setminus \sigma(q)$ for all $\sigma$. Set $z := N_{L/K}(x) = \prod_{\sigma} \sigma(x)$. As $x \in B$, we have $z \in q \cap A = p$. As $p = q \cap A$, we have

$$z = \prod_{\sigma} \sigma(x) \in q$$

so that there exists $\sigma \in \text{Gal}(L/K)$ such that $\sigma(x) \in q$ and thus $x \in \sigma^{-1}(q)$. This is a contradiction. \qed
Corollary 1.4.13. Let $\mathfrak{p}$ be a maximal ideal of $A$ and $B\mathfrak{p} = \prod_{q | \mathfrak{p}} q^{e_q}$. The integers $e_q$ and $f_q$ does not depend on the choice of $q | \mathfrak{p}$ but only on $\mathfrak{p}$. Denoting their common values $e_\mathfrak{p}$ and $f_\mathfrak{p}$, we have

$$[L : K] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$$

where $g_\mathfrak{p}$ is the number of maximal ideals $q | \mathfrak{p}$.

Let $\mathfrak{p}$ be a maximal ideal of $A$ and $\mathfrak{q}$ be a maximal ideal of $B$ above $\mathfrak{p}$. The decomposition group of $\mathfrak{q}$ is the stabilizer $D_\mathfrak{q}$ of $\mathfrak{q}$ in $\text{Gal}(L/K)$. An element $\sigma \in \text{Gal}(L/K)$, induces a field isomorphism $\overline{\sigma} : B/\mathfrak{q} \cong B/\sigma(\mathfrak{q})$. If $\sigma \in D_\mathfrak{q}$, then $\overline{\sigma}$ is an automorphism of $k(\mathfrak{q})$ which fixes pointwise the subfield $k()$, i.e. $\overline{\sigma} \in \text{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$.

Theorem 1.4.14. Assume moreover that $k(\mathfrak{q})/k(\mathfrak{p})$ is a separable extension. Then it is a Galois extension and the map $\sigma \mapsto \overline{\sigma}$ induces a surjective group homomorphism from $D_\mathfrak{q}$ onto $\text{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$.

Proof. Let’s prove first that the extension is Galois. As it is already supposed to be separable, we just have to prove that it is a normal extension. Let $x \in k(\mathfrak{q})$. It is sufficient to prove that $x$ is a root of a polynomial of $k(\mathfrak{p})[X]$ which is split in $k(\mathfrak{q})[X]$. Let $\tilde{x} \in B$ be an element lifting $x$ and define $P(X) = \prod_{\sigma \in \text{Gal}(L/K)}(X - \sigma(\tilde{x}))$. Then $P \in A[X]$ and, as $P$ is split in $B$, the reduction mod $\mathfrak{p}$ of $P$ is split in $B/\mathfrak{q} = k(\mathfrak{q})$. The reduction mod $\mathfrak{p}$ of $P$ is thus as expected. Note that this proves that each conjugate of $x$ over $k(\mathfrak{p})$ is the reduction mod $\mathfrak{q}$ of a conjugate of $\tilde{x}$ over $K$.

We now prove that the group homomorphism $D_\mathfrak{q} \rightarrow \text{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ is surjective. Let $x \in k(\mathfrak{q})$ be a primitive element over $k(\mathfrak{p})$ (which exists since the extension is separable). Let $\tau \in \text{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$. The automorphism $\tau$ is completely determined by its value on $x$. Let $\tilde{x}$ be a lift of $x$ in $B$. The decomposition $B = \mathfrak{q} + \prod_{\sigma(\mathfrak{q}) \neq \mathfrak{q}} \sigma(\mathfrak{q})$ shows that we can decompose $\tilde{x} = x_1 + x_2$ with $x_1 \in \mathfrak{q}$ and $x_2 \in \prod_{\sigma(\mathfrak{q}) \neq \mathfrak{q}} \sigma(\mathfrak{q})$. Then $x_2$ is a lift of $x$ such that $x_2 \in \sigma(\mathfrak{q})$ if $\sigma(\mathfrak{q}) \neq \mathfrak{q}$. As remarked in the previous paragraph, there exists $\sigma \in \text{Gal}(L/K)$ such that $\sigma(x_2)$ is a lift of $\tau(x)$ modulo $\mathfrak{q}$. As a consequence $\sigma(x_2) \not\in \mathfrak{q}$, i.e. $x_2 \not\in \sigma^{-1}(\mathfrak{q})$ which implies that $\sigma^{-1}(\mathfrak{q}) = \mathfrak{q}$ and $\sigma \in D_\mathfrak{q}$.

The kernel $I_\mathfrak{q}$ of the group homomorphism $D_\mathfrak{q} \rightarrow \text{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ is called the inertia subgroup at $\mathfrak{q}$. As $D_\mathfrak{q}$ is the stabilizer of $\mathfrak{q}$ and the $\text{Gal}(L/K)$-orbit of $\mathfrak{q}$ has cardinal $g_\mathfrak{p}$, the cardinal of the group $D_\mathfrak{q}$ is equal to $e_\mathfrak{p} f_\mathfrak{p}$. If the extension $k(\mathfrak{q})/k(\mathfrak{p})$, the cardinal of the group $\text{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ is equal to $[k(\mathfrak{q}) : k(\mathfrak{p})] = f_\mathfrak{p}$ so that the cardinal of the inertia subgroup $I_\mathfrak{q}$ is $e_\mathfrak{p}$.
1.4.4 Link with localization and completion

In this section we fix $A$ a Dedekind ring of fraction field $K$ and $L$ a finite extension of $K$. Let $B$ be the integral closure of $A$ in $L$. We assume that we are in the case where $B$ is a finitely generated $A$-module.

Let $\mathfrak{p}$ be a maximal ideal of $A$, and $\mathfrak{q}$ a maximal ideal of $B$ above $\mathfrak{p}$. Let $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$ be the associated absolute values over $K$ and $L$.

**Lemma 1.4.15.** The place associated to $|\cdot|_\mathfrak{q}$ is above the place associated to $\mathfrak{p}$ if and only if $\mathfrak{q} | \mathfrak{p}$.

**Proof.** Exercice.

Let $\hat{K}_\mathfrak{p}$ and $\hat{L}_\mathfrak{q}$ be the completions of $K$ and $L$ with respect to $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$. It follows from Lemma 1.4.15 and from Theorem 1.3.1 that there exist a surjective map

$$L \otimes_K \hat{K}_\mathfrak{p} \twoheadrightarrow \prod_{\mathfrak{q} | \mathfrak{p}} \hat{L}_\mathfrak{q}$$

which is both $L$ and $\hat{K}_\mathfrak{p}$-linear.

**Lemma 1.4.16.** Let $\mathcal{O}_{\hat{K}_\mathfrak{p}}$ and $\mathcal{O}_{\hat{L}_\mathfrak{q}}$ be the valuation rings of $\hat{K}_\mathfrak{p}$ and $\hat{L}_\mathfrak{q}$. Then $\mathcal{O}_{\hat{L}_\mathfrak{q}}$ is the integral closure of $\mathcal{O}_{\hat{K}_\mathfrak{p}}$ in $\hat{L}_\mathfrak{q}$.

**Proof.** Exercice.

Let $\pi_\mathfrak{p}$ (resp. $\pi_\mathfrak{q}$) be an uniformizer of $\hat{K}_\mathfrak{p}$ (resp. $\hat{L}_\mathfrak{q}$). Then $(\pi_\mathfrak{q})$ is a maximal ideal dividing $\mathfrak{p}_\mathfrak{q}$.

**Proposition 1.4.17.** We have $f(\pi_\mathfrak{q}) = f_\mathfrak{q}$ and $e(\pi_\mathfrak{q}) = e_\mathfrak{q}$.

**Proof.** The first equality comes from the fact that the residue field of $\hat{K}_\mathfrak{p}$ (resp $\hat{L}_\mathfrak{q}$) is isomorphic to $A_\mathfrak{p}/A_\mathfrak{p} \simeq A/\mathfrak{p}$ (resp. $B_\mathfrak{q}/B_\mathfrak{q} \simeq B/\mathfrak{q}$). For the second assertion we remark that we can choose $\pi_\mathfrak{p} \in \mathfrak{p}A_\mathfrak{p}$ and $\pi_\mathfrak{q} \in \mathfrak{q}B_\mathfrak{q}$. The ring $B_\mathfrak{p} := (A - \mathfrak{p})^{-1}B$ is easily checked to be the integral closure of $A_\mathfrak{p}$ in $L$ and the equality $\mathfrak{p}B = \prod_{\mathfrak{q} | \mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$ of ideals of $B$ implies

$$\mathfrak{p}B_\mathfrak{p} = \prod_{\mathfrak{q} | \mathfrak{p}} (\mathfrak{q}B_\mathfrak{p})^{e_\mathfrak{q}}$$

as ideals of $B_\mathfrak{p}$. Now we remark that $\mathfrak{p}B_\mathfrak{p} = \pi_\mathfrak{p}B_\mathfrak{p}$ and that $\mathfrak{q}'B_\mathfrak{q} = B_\mathfrak{q}$ if $\mathfrak{q}' \neq \mathfrak{q}$ so that we have

$$\pi_\mathfrak{p}B_\mathfrak{q} = (\mathfrak{q}B_\mathfrak{q})^{e_\mathfrak{q}} = (\pi_\mathfrak{q}B_\mathfrak{q})^{e_\mathfrak{q}}$$

so that there exists $u \in B_\mathfrak{q}^\times$ such that $\pi_\mathfrak{p} = u\pi_\mathfrak{q}^{e_\mathfrak{q}}$ which gives us the equality $(\pi_\mathfrak{p}) = (\pi_\mathfrak{q})^{e_\mathfrak{q}}$ in $\mathcal{O}_{\hat{L}_\mathfrak{q}}$. 

\[\blacksquare\]
1.4. RAMIFICATION

Corollary 1.4.18. We have \([\hat{L} : \hat{K}] = e_q f_q\).

Proof. This is a consequence of the previous proposition and from the fact that \(\mathcal{O}_{\hat{L}}\) is a finitely generated \(\mathcal{O}_{\hat{K}}\)-module. \(\square\)

Corollary 1.4.19. If \(B\) is a finitely generated \(A\)-module, then \(L \otimes_K \hat{K} \simeq \prod_{q \mid p} \hat{L}_q\). In particular, this is the case if \(K\) (and \(L\)) are global fields.

Proof. In this case, we have \([L : K] = \sum_{q \mid p} e_q f_q\). \(\square\)

Corollary 1.4.20. 1) If \(K\) is a number field, the ultrametric places are exactly the equivalence classes of the \(|\cdot|_p\) where \(p\) is a maximal ideal of \(\mathcal{O}_K\).

2) If \(K\) is a finite extension of \(\mathbb{F}_q(T)\), the (ultrametric) places of \(K\) whose closed unit ball contains \(\mathbb{F}_q[T]\) are exactly the equivalence classes of the \(|\cdot|_p\) where \(p\) is a maximal ideal of the integral closure of \(\mathbb{F}_q[T]\) in \(K\).

Now we assume moreover that the extension \(L/K\) is Galois. If \(\sigma \in D_q\), we have \(\sigma(q) = q\) so that \(|\sigma(-)|_q = |\cdot|_q\). As a consequence the group \(D_q\) acts on \((L, |\cdot|_q)\) by isometries and this action extends into a continuous action of \(D_q\) on \(\hat{L}_q\). As the elements of \(D_q\) fix \(K\) and \(K\) is dense in \(\hat{K}_p\), the extension of \(\sigma\) to \(\hat{L}_q\) fix \(\hat{K}_p\). Therefore we obtain an injective group homomorphism \(D_q \hookrightarrow \text{Aut}_{\hat{K}_p}(\hat{L}_q)\).

We deduce inequalities

\[
e_q f_q = |D_q| \leq |\text{Aut}_{\hat{K}_p}(\hat{L}_q)| \leq [\hat{L}_q : \hat{K}_p].
\]

As the two extremal cases are equal, all inequalities are equalities. Thus the extension \(\hat{L}_q/\hat{K}_p\) is Galois and we have a group isomorphism

\[D_q \cong \text{Gal}(\hat{L}_q/\hat{K}_p).\]

1.4.5 Different and discriminant

Let \(A\) be a Dedekind ring and let \(K\) be its fraction field. We fix \(L\) a finite separable extension of \(K\) and let \(B\) be the integral closure of \(A\) in \(L\).

It follows from Lemma 1.4.4 that the \(K\)-bilinear form on \(L\) defined by \((x, y) \mapsto \text{Tr}_{L/K}(xy)\) is nondegenerate. Recall that if \(M\) is an \(A\)-submodule of \(L\), we define \(M^* := \{x \in L \mid \text{Tr}_{L/K}(xM) \subset A\}\). From the proof of Proposition 1.4.5 that \(B^*\) is a \(B\)-submodule of \(L\) finitely generated over \(A\) containing \(B\). This is a nonzero fractional ideal of \(B\) whose inverse is called the different of \(B\) over \(A\) and is noted \(\mathcal{D}_{B/A}\). As \(B \subset \mathcal{D}_{B/A}^{-1}\), we have \(\mathcal{D}_{B/A} \subset B^{-1} = B\) and then \(\mathcal{D}_{L/K}\) is a nonzero ideal of \(B\).
Recall that we have defined $I_B$ and $I_A$ the groups of fractional ideals of the Dedekind rings $B$ and $A$. There exists a group homomorphism $N : I_B \to I_A$ called the norm such that, for $q$ a maximal ideal of $B$, $N(q) := p^h$ where $p := q \cap A$. This is well defined because $I_B$ is a free abelian group over the maximal ideals of $B$.

**Remark 1.4.21.** If $A = \mathbb{Z}$ and $K = \mathbb{Q}$, then we can check that, for a nonzero ideal $I$ of $B$, the quotient ring $B / I$ is finite and $N(I) = |B / I|$. The discriminant of $B$ over $A$ is the ideal $\Delta_{B/A}$ of $A$ defined as the norm of $D_{B/A}$: $\Delta_{B/A} := N(D_{B/A})$.

**Lemma 1.4.22.** Let $\mathfrak{p}$ be a maximal ideal of $A$. Then $D_{B/A}B_{\mathfrak{p}} = D_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$ and $\Delta_{B/A}A_{\mathfrak{p}} = \Delta_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$.  

**Proof.** It is sufficient to prove the first equality. The second follows directly from the first and from $N(I)A_{\mathfrak{p}} = N(IB_{\mathfrak{p}})$ for each ideal $I$ of $B$, which is easy to check. In order to prove the first equality, it is sufficient to check that $B_{\mathfrak{p}}^* = B_{\mathfrak{p}}^*$, which follows from the $K$-linearity of $\text{Tr}_{L/K}$.

Let $d := [L : K]$ and let $(e_1, \ldots, e_d)$ a family of elements of $L$. We define  

$$\Delta(e_1, \ldots, e_d) := \det(\text{Tr}_{L/K}(e_ie_j))_{1 \leq i, j \leq d}.$$  

**Remark 1.4.23.** If $(e_1, \ldots, e_d)$ and $(e'_1, \ldots, e'_d)$ are two $K$-bases of $L$ and $P$ is the matrix of $(e'_1, \ldots, e'_d)$ in the basis $(e_1, \ldots, e_d)$, we have  

$$\Delta(e'_1, \ldots, e'_d) = \det(P)^2 \Delta(e_1, \ldots, e_d).$$

**Proposition 1.4.24.** The ideal $\Delta_{B/A}$ is the ideal of $A$ generated by the $\Delta(e_1, \ldots, e_d)$ where $e_i$ is a family of elements of $B$.

**Proof.** Let $I$ be the ideal of $A$ generated by the $\Delta(e_1, \ldots, e_d)$ where $e_i$ is a family of elements of $B$. To prove that $\Delta_{B/A} = I$, it is sufficient to prove that $\Delta_{B/A,p} = I_p$ for each maximal ideal $p$ of $A$. Clearly, the ideal $I_p$ of $A_p$ is the ideal generated by the elements $\Delta(e_1, \ldots, e_d)$ where $(e_i)$ is a family of elements of $B_p$. As $\Delta_{B/A,p} = \Delta_{B_p/A_p}$, we are reduced to prove the claim when $A$ is assumed to be a principal ideal domain.

We assume that $A$ is a principal domain. Then the $A$-module $B$ is finite free and there exists a $K$-basis $(e_1, \ldots, e_d)$ which is also an $A$-basis of $B$. It follows from Remark 1.4.23 that $I$ is the principal ideal generated by $\Delta(e_1, \ldots, e_d)$. We have an inclusion of finite free $A$-modules $B \subset B^*$ having the same rank, so that there exists an $A$-basis $(e_{1}^*, \ldots, e_{d}^*)$ of $B^*$ and nonzero elements $a_1 \mid a_2 \mid \cdots \mid a_d$ of $A$ such that $(a_1 e_{1}^*, \ldots, a_d e_{d}^*)$ is an $A$-basis of $B$. Let $(e'_1, \ldots, e'_d)$ be the dual
basis of \((e_1^*, \ldots, e_d^*)\) and let \(P\) be the matrix of the basis \((e_1', \ldots, e_d')\) in the basis \((a_1e_1, \ldots, a_de_d)\). We have \(P \in \text{GL}_d(A)\) and

\[
\Delta(e_1', \ldots, e_d') = \det(\text{Tr}_{L/K}(e_i'e_j))_{1 \leq i, j \leq d} = \prod_{j=1}^d a_j \det(\text{Tr}_{L/K}(e_i'a_je_j))_{1 \leq i, j \leq d} = \prod_{j=1}^d a_j.
\]

This implies that \(I = (\prod_j a_j)\). Moreover the equality \(D_{B/A}^{-1} = B^*/B\) shows that \(B^*/B\) has a Jordan-Hölder filtration by \(B\)-submodules whose successive subquotients are isomorphic to the \(B/\mathfrak{q}_i\) where \(D_{B/A} = \mathfrak{q}_1 \cdots \mathfrak{q}_r\) (counted with multiplicity). Let \(\pi_i \in A\) be such that \(\mathfrak{q}_i \cap A = (\pi_i)\), then the elementary divisors of \(B/\mathfrak{q}_i\) are the \((\pi_i, \ldots, \pi_i)\) (counted \(f_{\mathfrak{q}_i}\) times). This shows that the product of the elementary divisors of the \(A\)-module \(B^*/B\) generates the ideal \(\mathcal{N}(\Delta_B/A)\). This implies actually that

\[
\Delta_{B/A} = \left(\prod a_j\right) = I. \quad \square
\]

Assume that \(L\) and \(K\) are complete for compatible absolute values. In this case, we can choose \(A = \mathcal{O}_K\) and \(B = \mathcal{O}_L\). We define \(D_{L/K} := D_{\mathcal{O}_L/\mathcal{O}_K}\) and \(\Delta_{L/K} := \Delta_{\mathcal{O}_L/\mathcal{O}_K}\).

**Proposition 1.4.25.** Let \(p\) be a maximal ideal of \(A\) and \(\mathfrak{q}\) a maximal ideal of \(B\) dividing \(\mathfrak{q}\). Then the extension \(\hat{L}_\mathfrak{q}/\hat{K}_p\) is separable and

\[
\hat{D}_{\hat{L}_\mathfrak{q}/\hat{K}_p} = D_{\hat{L}_\mathfrak{q}} D_{B/A}, \quad \hat{\Delta}_{\hat{L}_\mathfrak{q}/\hat{K}_p} = \hat{\mathcal{O}}_{\hat{K}_p} \Delta_{B/A}.
\]

**Proof.** Recall that, the extension \(L/K\) being separable, we have an isomorphism

\[
L \otimes_K \hat{K}_p \cong \prod_{\mathfrak{q} \mid p} \hat{L}_\mathfrak{q}.
\]

Moreover we can extend the nondegenerate \(K\)-bilinear form \(\text{Tr}_{L/K}(-)\) on \(L\) to a nondegenerate \(\hat{K}_p\)-bilinear form on \(L \otimes_K \hat{K}_p\). Under this isomorphism this \(\hat{K}_p\)-bilinear form is \(\bigoplus_{\mathfrak{q} \mid p} \text{Tr}_{\hat{L}_\mathfrak{q}/\hat{K}_p}(-)\). Therefore all the bilinear forms \(\text{Tr}_{\hat{L}_\mathfrak{q}/\hat{K}_p}(-)\) are nondegenerate and all the extensions \(\hat{L}_\mathfrak{q}/\hat{K}_p\) are separable. Moreover we have a map

\[
B \otimes_A \hat{\mathcal{O}}_{\hat{K}_p} \prod_{\mathfrak{q} \mid p} \hat{\mathcal{O}}_{\hat{L}_\mathfrak{q}} \cong \hat{\mathcal{O}}^*_{\hat{L}_\mathfrak{q}} \hat{\mathcal{O}}^*_{\hat{L}_\mathfrak{q}}
\]

which is actually an isomorphism (left as an exercise). We obtain an isomorphism of \(\mathcal{O}_{\hat{L}_\mathfrak{q}}\)-modules

\[
(B^*/B) \otimes_A \hat{\mathcal{O}}_{\hat{K}_p} \cong \prod_{\mathfrak{q} \mid p} \hat{\mathcal{O}}^*_{\hat{L}_\mathfrak{q}} / \hat{\mathcal{O}}_{\hat{L}_\mathfrak{q}}
\]

from which the first equality follows. The second equality is then easily derived. \(\square\)
Let \( k \) be a field and let \( A \) be a finite dimensional \( k \)-algebra. We define the trace of an element \( a \in A \) as the trace of the \( k \)-linear endomorphism \( x \mapsto ax \) of \( A \).

**Lemma 1.4.26.** Let \( A \) be a finite dimensional \( k \)-algebra. Then the \( k \)-bilinear form \((x, y) \mapsto b_A(x, y) := \text{Tr}_{A/k}(xy)\) over \( A \) is non degenerate if and only if \( A \) is isomorphic to a product of finite separable extensions of \( k \).

**Proof.** If \( A \) is a product \( k_1 \times \cdots \times k_r \) of finite separable extensions of \( k \), then the matrix of the bilinear form \( b_A \) is, in some adapted basis, the block diagonal of matrices of the bilinear forms \( b_k \). Therefore the result follows from Lemma 1.4.4. Conversely if \( b_A \) is nondegenerate and \( A \) is isomorphic to a product of fields, then Lemma 1.4.4 shows that all these extensions have to be separable. We are reduced to prove that if \( b_A \) is nondegenerate, then \( A \) is isomorphic to a product of fields. Since \( A \) is finite dimensional over \( k \), we just have to prove that \( A \) has no nonzero nilpotent element. Let \( a \in A \) be a nilpotent element. If \( c \in A \), then \( ac \) is nilpotent and so is the endomorphism \( x \mapsto acx \) and \( \text{Tr}_{A/k}(ac) = 0 \). As \( b_A \) is nondegenerate, we have \( a = 0 \).

**Proposition 1.4.27.** Assume that \( L/K \) is finite separable extension of complete discretely valued fields. The extension \( L/K \) is unramified (at the maximal ideal of \( \mathcal{O}_K \)) if and only if \( \mathcal{D}_{L/K} = \mathcal{O}_L \) if and only if \( \Delta_{L/K} = \mathcal{O}_K \).

**Proof.** As \( \mathcal{O}_L \) is a finite free \( \mathcal{O}_K \)-module, let \((e_1, \ldots, e_d)\) be a \( \mathcal{O}_K \)-basis of \( e\mathcal{O}_L \). Let \( \pi_K \) be an uniformizer of \( K \) and \( \pi_L \) an uniformizer of \( L \). Then \((\pi_1, \ldots, \pi_d)\) is a \( k_K \)-basis of \( \mathcal{O}_L/(\pi_K) \). Moreover the image of discriminant \( \Delta(e_1, \ldots, e_d) \) in \( k_K = \mathcal{O}_K/(\pi_K) \) is the discriminant of the trace bilinear form on \( \mathcal{O}_L/(\pi_K) \). Therefore \( \mathcal{O}_L/(\pi_K) \) is isomorphic to a product of separable extensions of \( k_K \) if and only if \( \Delta_{L/K} = \mathcal{O}_K \). As \((\pi_K) = (\pi_L)^{[L/K]} \) and \( \mathcal{O}_L/(\pi_L) = k_L \), this is equivalent to the fact that \( L/K \) is unramified. As \( \Delta_{L/K} = N(\mathcal{D}_{L/K}) \) the last equivalence is clear.

**Corollary 1.4.28.** Let \( A \) be a Dedekind ring, \( K \) its fraction field, \( L \) a finite separable extension of \( K \) and \( B \) the integral closure of \( A \) in \( L \).

1) If \( q \) is a maximal ideal of \( B \), then \( L/K \) is ramified at \( q \) if and only if \( q \mid \mathcal{D}_{L/K} \).

2) If \( p \) is a maximal ideal of \( A \), then \( L/K \) is ramified at \( p \) if and only if \( p \mid \Delta_{L/K} \).

3) There are only finitely many maximal ideals of \( A \) which are ramified in \( L \).
1.4. RAMIFICATION

1.4.6 Frobenius element

Let \( A \) be a Dedekind ring of field of fractions \( K \). Let \( L \) be a finite extension of \( K \) and let \( B \) be the integral closure of \( A \) in \( L \). Let \( \mathfrak{q} \) be a maximal ideal of \( B \) and let \( := \mathfrak{p} \cap A \). Assume that \( L/K \) is unramified at \( \mathfrak{q} \) and that the residue field \( k(\mathfrak{q}) \) is finite. The residue field \( k(\mathfrak{p}) \) is then also finite. There is a natural isomorphism from the decomposition group \( D_\mathfrak{q} \) onto the Galois group \( \text{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \). As \( k(\mathfrak{q})/k(\mathfrak{p}) \) is an extension of finite fields, it is cyclic and generate by the Frobenius endomorphism \( x \mapsto x^q \) with \( q \) the cardinal of \( k(\mathfrak{p}) \). The element \( (\mathfrak{q}, L/K) \) of \( D_\mathfrak{q} \subset \text{Gal}(L/K) \) corresponding to the Frobenius automorphism is called the Frobenius element at \( \mathfrak{q} \). This is the unique element \( \sigma \) of \( \text{Gal}(L/K) \) such that

- \( \sigma(\mathfrak{q}) = \mathfrak{q} \);
- \( \forall b \in B, \quad \sigma(b) \equiv b^{[k(\mathfrak{p})]} \mod \mathfrak{q} \).

The order of the element \( (\mathfrak{q}, L/K) \) in \( \text{Gal}(L/K) \) is exactly \( f_\mathfrak{q} \).

Remark 1.4.29. The element \( (\mathfrak{q}, L/K) \) does not depend on the choices of the Dedekind rings \( A \) and \( B \) but only on the place of \( L \) corresponding to \( \mathfrak{q} \).

Assume that \( M/K \) is a Galois subextension of \( L/K \). If \( r \) is the restriction of the place \( \mathfrak{q} \) to \( M \), then the Frobenius element \( (r, L/K) \) is the image of \( (\mathfrak{q}, L/K) \) in \( \text{Gal}(M/K) \).

If \( \mathfrak{q}' \) is another maximal ideal of \( B \) dividing \( \mathfrak{p} \), there exists \( \sigma \in \text{Gal}(L/K) \) such that \( \sigma(\mathfrak{q}) = \mathfrak{q}' \). Then \( (\mathfrak{q}', L/K) = \sigma(\mathfrak{q}, L/K)\sigma^{-1} \). Therefore, if the extension \( L/K \) is abelian, the element \( (\mathfrak{q}, L/K) \) depends only on \( \mathfrak{p} \) and is denoted \( (\mathfrak{p}, L/K) \).

1.4.7 The example of the cyclotomic extensions

Let \( \zeta_n = e^{2\pi i/n} \in \mathbb{C} \) and let \( \mathbb{Q}(\zeta_n) \) be the extension of \( \mathbb{Q} \) generated by \( \zeta_n \). The polynomial \( X^n - 1 \) has \( \zeta_n \) for root and is completely split in \( \mathbb{Q}(\zeta_n) \) so that the extension \( \mathbb{Q}(\zeta_n)/\mathbb{Q} \) is Galois.

Theorem 1.4.30. The ring of integers of \( \mathbb{Q}(\zeta_n) \) is \( \mathbb{Z}[\zeta_n] \). Moreover a prime number \( p \) is ramified in \( \mathbb{Q}(\zeta_n)/\mathbb{Q} \) if and only if \( p \mid n \).

Proof. Let \( \mathcal{O} \) be the ring of integers of \( \mathbb{Q}(\zeta_n) \). We have \( \mathbb{Z}[\zeta_n] \subset \mathcal{O} \). This inclusion is an equality if and only if \( \mathbb{Z}_{(p)}[\zeta_n] = \mathcal{O}_{(p)} \) for each prime number \( p \).

Let \( p \) be a prime number. Let \( n = p^\alpha m \) with \( p \nmid m \). Let \( K = \mathbb{Q}(\zeta_p) \) and \( L = K(\zeta_m) = \mathbb{Q}(\zeta_n) \). Let \( \mathcal{O}_K \) be the ring of integers of \( K \). We have \( \mathbb{Z}[\zeta_p] \subset \mathcal{O}_K \).

The polynomial \( \Phi_{p^\alpha} := 1 + X^{p^\alpha-1} + X^{2p^\alpha-1} + \cdots + X^{(p-1)p^\alpha-1} \) is irreducible as an Eisenstein polynomial so that

\[ \mathbb{Z}_{(p)}[\zeta_{p^\alpha}] \simeq \mathbb{Z}[X]/(\Phi_{p^\alpha}). \]
Then \( \mathbb{Z}_p[\zeta_{p^r}] / (p) \cong \mathbb{F}_p[X] / (\Phi_{p^r}) \) with \( \Phi_{p^r} \) the reduction mod \( p \) of \( \Phi_{p^r} \). As

\[
\Phi_{p^r} = \frac{X^{p^r} - 1}{X^{p^r - 1} - 1} = (X - 1)^{p^{r - 1}(p - 1)}
\]

we see that there is a unique maximal ideal in \( \mathbb{Z}_p[\zeta_{p^r}] \) containing \( (p) \). As \( \mathbb{Z}_p[\zeta_{p^r}] \) is integral over \( \mathbb{Z}_p \), a maximal ideal of \( \mathbb{Z}_p[\zeta_{p^r}] \) has a nonzero intersection with \( \mathbb{Z}_p \) and thus has to contain \( (p) \). Therefore, \( \mathbb{Z}_p[\zeta_{p^r}] \) has a unique maximal ideal which is the inverse image \( (X - 1) \) by \( \mathbb{Z}_p[\zeta_{p^r}] \to \mathbb{F}_p[X] / (X - 1)^{p^{r - 1}(p - 1)} \), i.e. \( (p, \zeta_{p^r} - 1) \).

Now we can remark that \( \Phi_{p^r}(1) = p \) is a multiple of \( \zeta_{p^r} - 1 \) so that \( (\zeta - p^r - 1) \) generates the maximal ideal of \( \mathbb{Z}_p[\zeta_{p^r}] \). The following lemma shows that \( \mathbb{Z}_p[\zeta_{p^r}] \) is a principal ideal domain and thus integrally closed. Therefore \( \mathbb{Z}_p[\zeta_{p^r}] = \mathcal{O}_{L,(p)} \). Moreover we see that \( (p) \) the inertia index of \( p \) in \( K / \mathbb{Q} \) is \( p^r - p^{r - 1} \) and its residual degree is 1.

**Lemma 1.4.31.** Let \( A \) be a local domain whose maximal ideal \( \mathfrak{m} \) is principal and such that \( \bigcap_{n \geq 0} \mathfrak{m}^n = \{0\} \). Then \( A \) is a principal ideal domain.

**Proof.** If \( x \in A \setminus \{0\} \), let \( m = \max\{n \geq 0 \mid x \in \mathfrak{m}^n\} \). Then \( m < \infty \) and, if \( \pi \) is a generator of \( \mathfrak{m} \), we have \( x = \pi^m u \) with \( u \notin \mathfrak{m} \) so that \( u \in A^\times \). Therefore \( (x) = (\pi^m) \). Now if \( I \) is an ideal of \( A \), let \( m = \inf\{n \geq 0 \mid (x) = (\pi^n), x \in I\} \). There exists some \( a \in I \) such that \( (a) = (\pi^n) \) and it is clear that \( I = (\pi^n) \). \( \square \)

Now let \( A := \mathbb{Z}_p[\zeta_{p^r}] \). We have proved that \( A \) is a principal ideal domain with a unique maximal ideal \( (\pi) \) (actually we can choose \( \pi = \zeta_{p^r} - 1 \)). Moreover \( \mathcal{O}_{L,(p)} = \mathcal{O}_p \) is the integral closure of \( A \) in \( L \). We have \( \zeta_m \in \mathcal{O}_{L,(p)} \). Let \( Q \in A[X] \) be the minimal polynomial of \( \zeta_m \) over \( K \) and let \( \overline{Q} \in \mathbb{F}_p[X] \) be the reduction of \( Q \) mod \( \pi \). As \( Q \mid X^m - 1 \) we have \( \overline{Q} \mid X^m - 1 \). Moreover \( p \nmid m \) so that \( \overline{Q} \) is separable in \( \mathbb{F}_p[X] \) and thus a product of distinct irreducible polynomial. It follows that the \( \mathbb{F}_p \)-algebra \( A[\zeta_m] / (\pi) \) is a product of extensions of \( \mathbb{F}_p \) (automatically separable since \( \mathbb{F}_p \) is finite thus perfect), this implies that the trace form on \( A[\zeta_m] / (\pi) \) is nondegenerate and then that the discriminant of an \( A \)-basis of \( A[\zeta_m] \) is not in \( (\pi) \) and is invertible in \( A \). Let \( (e_1, \ldots, e_d) \) be an \( A \)-basis of \( \mathcal{O}_{L,(p)} \) and \( (e'_1, \ldots, e'_d) \) be an \( A \)-basis of \( A[\zeta_m] \). Let \( P \) be the matrix of \( (e'_1, \ldots, e'_d) \) in \( (e_1, \ldots, e_d) \). We have \( P \in M_d(A) \) and

\[
\Delta(e'_1, \ldots, e'_d) = \det(P)^2 \Delta(e_1, \ldots, e_d)
\]

so that \( \det(P) \in A^\times \) and \( P \in \text{GL}_d(A) \), that it \( \mathcal{O}_{L,(p)} = A[\zeta_m] \). Finally we have proved that \( \mathcal{O}_{L,(p)} = A[\zeta_m] = \mathbb{Z}_p[\zeta_m] \). So we are done.

Note that if \( p \nmid n \), then \( m = n \) and \( A = \mathbb{Z}_p \), we have proved that \( \Delta \mathcal{O}_{L,(p)} / \mathbb{Z}_p \in \mathbb{Z}(p)^\times \) so that \( L / \mathbb{Q} \) is unramified at \( p \). \( \square \)
Let $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Then $\sigma(\zeta_n)$ is an element of order $n$ in $\mathbb{C}^\times$ so there exists $a = a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma(\zeta_n) = \zeta_n^a$. The element $a_\sigma$ determines completely $\sigma$ so that the map $\sigma \mapsto a_\sigma$ gives rise to an injective morphism of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

**Proposition 1.4.32.** Let $n \geq 1$ and let $p$ be a prime number such that $p \nmid n$. Then the image of the Frobenius element $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ is the class of $p$.

**Proof.** Let $\sigma := (p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ and let $a = a_\sigma$. Let $q$ be a maximal ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ dividing $(p)$. By definition, we have $\sigma(\zeta_n) \equiv \zeta_n^a \mod q$ and $\sigma(\zeta_n) = \zeta_n^a$. We have $\zeta_n^a \equiv \zeta_n^a$ in $\mathbb{Z}[\zeta_n]/q$. As the reduction mod $p$ of the polynomial $X^n - 1$ is separable, we must have $a \equiv p \mod n$.

**Corollary 1.4.33.** We have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ and the map $\sigma \mapsto a_\sigma$ is an isomorphism of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ onto $(\mathbb{Z}/n\mathbb{Z})^\times$.

**Proof.** As each element of $(\mathbb{Z}/n\mathbb{Z})^\times$ can be decomposed as a product of classes of prime number not dividing $n$, the images of the Frobenius elements generate $(\mathbb{Z}/n\mathbb{Z})^\times$ so that the map $a \mapsto a_\sigma$ is surjective.

**Proposition 1.4.34.** Let $p$ be an odd prime number and let $p^* = (-1)^{\frac{p-1}{2}}$. Then $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic extension contained in $\mathbb{Q}(\zeta_p)$.

**Proof.** As the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$, there is exactly one quadratic extension $\mathbb{Q}(\sqrt{d})$ contained in $\mathbb{Q}(\zeta_p)$. We can choose $d \in \mathbb{Z}$ without square divisor and in this case

$$
\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} 
\mathbb{Z}^{\frac{1+\sqrt{d}}{2}} & \text{if } d \equiv 1 \mod 4 \\
\mathbb{Z}^{\sqrt{d}} & \text{if } d \equiv 2 \text{ or } 3 \mod 4.
\end{cases}
$$

A direct computation shows that $\Delta_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathbb{Z}} = d$ if $d \equiv 1 \mod 4$ and $\Delta_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathbb{Z}} = 4d$ in the other cases. As $\mathbb{Q}(\zeta_p)$ is ramified only at $p$, the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is ramified at most at $p$. This shows that $d = \pm p$ and $d \equiv 1 \mod 4$, that is $d = p^*$.

**Theorem 1.4.35.** Let $p$ be an odd prime number and $q \neq p$ an other odd prime number. We have $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$ and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^*-1}{8}}$.

**Proof.** The prime number $q$ is unramified in $\mathbb{Q}(\zeta_p)$ and thus unramified in $\mathbb{Q}(\sqrt{p^*})$. Moreover it is split in $\mathbb{Q}(\sqrt{p^*})$ if and only if $(q, \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = 1$, that is, if and only if $(q, \mathbb{Q}(\zeta_p)/\mathbb{Q})$ is in the kernel of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$. This is still equivalent to the fact that $q$ is in the subgroup of index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, that to the fact that $q$ is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore $q$ is split in $\mathbb{Q}(\sqrt{p^*})$ if and only if $\left(\frac{q}{p}\right) = 1$. 


On the other hand, $q$ is split in $\mathbb{Q}(\sqrt{p^*})$ if and only if the $\mathbb{F}_q$-algebra $\mathbb{Z}[\frac{1+\sqrt{p^*}}{2}]/\langle q \rangle$ is a product of two fields isomorphic to $\mathbb{F}_q$, that is if and only if the minimal polynomial of $\frac{1+\sqrt{p^*}}{2}$ has a root in $\mathbb{F}_q$. If $q \neq 2$, this is equivalent to the fact that $p^*$ is a square in $\mathbb{F}_q$, that is $\left(\frac{p^*}{q}\right) = 1$. Consequently we have
\[
\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).
\]

Assume now that $q = 2$. Let's remark that the minimal polynomial of $\frac{1+\sqrt{p^*}}{2}$ is $X^2 - X + \frac{1-p^*}{4}$. As $X^2 - X$ takes the value 0 on $\mathbb{F}_2$, the polynomial $X^2 - X + \frac{1-p^*}{4}$ has a root in $\mathbb{F}_2$ if and only if $\frac{1-p^*}{4}$ is even, that is if and only if $p^* \equiv 1 \mod 8$, that is if and only if $p \equiv \pm 1 \mod 8$. \qed
Chapter 2

Adeles and ideles

2.1 Adeles

2.1.1 Topological groups and restricted products

Let $G$ be an locally compact group (i.e. Hausdorff and having a basis of compact neighborhoods) and let $H$ be a closed subgroup of $G$. Then the quotient space $G/H$ is locally compact (use the fact that $H$ is closed and that the quotient map $\pi : G \rightarrow G/H$ is open). If $H$ is moreover normal, this is a locally compact topological group.

Lemma 2.1.1. Let $G$ be a topological group. Let $\Gamma \subset G$ be a subgroup.

1) The subspace $\Gamma$ discrete in $G$ if and only if there exists a neighborhood $V$ of $e_G$ such that $V \cap \Gamma = \{e_G\}$.

2) If $\Gamma$ is a discrete subgroup of $G$, it is closed in $G$.

3) If $\Gamma$ is discrete, then the map $\pi : G \rightarrow G/H$ is a covering.

Proof. If $\Gamma$ is discrete, then $\{e_G\}$ is an open subset of $\Gamma$ for the induced topology so that there exists a neighborhood $V$ of $e_G$ in $G$ such that $V \cap \Gamma = \{e_G\}$. Conversely assume that there exists such a $V$ and let $\gamma \in \Gamma$. Then $\gamma V$ is a neighborhood of $\gamma$ and $\gamma V \cap \Gamma = \gamma(V \cap \Gamma) = \{\gamma\}$. Then $\Gamma$ is discrete. This proves 1).

Let $x \in G \setminus \Gamma$. Let $V$ be a neighborhood of $e_G$ such that $V \cap \Gamma = \{e_G\}$ and let $W$ be a neighborhood of $\{e_G\}$ such that $W \cdot W^{-1} \subset V$. If $\gamma_1, \gamma_2 \in Wx \cap \Gamma$, we have $\gamma_1 \gamma_2^{-1} \in W \cdot W^{-1} \cap \Gamma = \{e_G\}$. There is at most one element of $\Gamma$ in $Wx$. As $x \notin \Gamma$ and $G$ is Hausdorff, we can choose $W$ small enough so that $xW \cap \Gamma = \emptyset$. Then $G \setminus \Gamma$ is open and $\Gamma$ is a closed subgroup of $G$.

Let $W$ be a compact neighborhood of $e_G$ such that $W \cdot W^{-1} \cap \Gamma = \{e_G\}$. For $\gamma_1, \gamma_2 \in \Gamma$, we have $\gamma_1 W \cap \Gamma_2 W \neq \emptyset \Rightarrow \gamma_1 = \gamma_2$. Then, for $x \in G$, $\pi(Wx)$ is a
neighborhood of \( \pi(x) \) and \( pt^{-1}(\pi(Wx)) = \bigcup_{\gamma \in \mathcal{F}} \gamma Wx \) with \( \gamma Wx = (\gamma W^{-1})\gamma x \) a neighborhood of \( \gamma x \).

Let \( \Sigma \) be a set and let \( \Sigma_\infty \) be a finite subset of \( \Sigma \). For each \( v \in \Sigma \), we fix \( G_v \) a locally compact group and, if \( v \notin \Sigma_\infty \) an open and compact subgroup \( K_v \subset G_v \). In general the product \( \prod_{v \in \Sigma} G_v \) is not locally compact. That’s a reason to consider the following alternative construction.

**Definition 2.1.2.** The restricted product of the family \( (G_v)_{v \in \Sigma} \) with respect to the \( (K_v)_{v \notin \Sigma_\infty} \) is the set
\[
\prod_{v \in \Sigma} 'G_v := \{(g_v) \in \prod_{v \in \Sigma} | g_v \in K_v \text{ pp}(()v)\}
\]
where the notation \( \text{pp}(()v) \) means “for all except a finite number of \( v \)”.

We define a topology on \( G := \prod_{v \in \Sigma} G_v \). Let \( B \) be the set of all subsets
\[
U_S \times \prod_{v \notin S} K_v
\]
where \( S \) is a finite subset of \( \Sigma \) containing \( \Sigma_\infty \) and \( U_S \) is an open subset of \( \prod_{v \in S} G_v \). We can check that if \( U \) and \( V \) are in \( B \), for all \( x \in U \cap V \), there exists \( W \in B \) such that \( x \in X \subset U \cap V \), i.e. that \( B \) is a basis of open subset of \( G \). We can therefore define a topology on \( G \) whose open subsets are the \( U \subset G \) such that for all \( x \in U \) there exists \( V \in B \) such that \( x \in V \subset U \).

**Lemma 2.1.3.** With this topology, \( G \) is a locally compact topological group.

**Proof.** First of all \( G \) is a subgroup of the product \( \prod_{v \in \Sigma} G_v \).

For the topology, a system of neighborhoods of the neutral element is given by \( (U_S \times \prod_{v \notin S} K_v) \) for \( S \) finite and \( U_S \) a neighborhood of the neutral element in \( \prod_{v \in S} G_v \). This system of neighborhoods satisfy the properties \((GV_I),(GV_{II})\) and \((GV_{III})\) of [Bou71, Ch. III§1.2] \((GV_{III})\) needs some care when the groups are not commutative). As a system of neighborhoods of an element \( a \in G \) is just a translation by \( a \) of a system of neighborhoods of the neutral element, Prop. 1 of loc. cit. shows that the topology on \( G \) is compatible to the group structure.

Finally we have to check that \( G \) is locally compact. First of all, \( G_S := \prod_{v \in S} G_v \times \prod_{v \notin S} K_v \) is an open subset of \( G \) for each finite subset \( S \subset \Sigma \) containing \( \Sigma_\infty \). Moreover the topology of \( G \) induces the product topology on \( G_S \). As the \( K_v \) are compact, the product \( \prod_{v \notin S} K_v \) is compact. Thus \( G \) is a finite product of locally compact spaces ans is locally compact.

**Remark 2.1.4.** If all the topologies of the groups \( G_v \) are metric and \( \Sigma \) is countable, the topology of \( G \) is metric.
2.1.2 Adeles

Let $F$ be a global field and let $\Sigma$ be the set of its places. Let $\Sigma_\infty$ be the finite subset of archimedean places. If $v \in \Sigma$, we note $F_v$ the completion of $F$ at $v$ and, if $v \notin \Sigma_\infty$, $\mathcal{O}_v \subset F_v$ its valuation ring and $\mathfrak{p}_v \subset \mathcal{O}_v$ the maximal ideal. Moreover we denote $|\cdot|_v$ the normalized absolute value on $F$ associated to the place $v$.

**Definition 2.1.5.** The group of adeles is the restricted product of the additive groups $(F_v)_{v \in \Sigma}$ with respect to the family $(\mathcal{O}_v)_{v \notin \Sigma_\infty}$. We use the notation

$$\mathbb{A}_F := \prod_{v \in \Sigma} F_v.$$  

The group $\mathbb{A}_F$ is a locally compact abelian group. Moreover it has a natural structure of topological ring (see [Bou71, Ch. III §6.3]). There is a diagonal embedding of $F$ in $\mathbb{A}_F$ which is a ring homomorphism defined by $\xi \mapsto (\xi)_{v \in \Sigma}$. We use this embedding to identify $F$ to a subring of $\mathbb{A}_F$.

**Theorem 2.1.6.** The subring $F \subset \mathbb{A}_F$ is discrete and the quotient group $\mathbb{A}_F/F$ is compact.

**Proof.** Let’s show that $F$ is a discrete subset of $\mathbb{A}_F$. Let $v_0 \in \Sigma$ and define a neighborhood of $0$ by

$$V := \{(x_v)_v \in \mathbb{A}_F \mid |x_{v_0}|_{v_0} < r, |x_v|_v \leq 1 \text{ if } v \neq v_0\}.$$  

If $x \in F \cap V$, we have $\prod_v |x_v| < r < 1$ so that the product formula implies $x = 0$. Hence $F \cap V = \{0\}$ and $F$ is discrete in $\mathbb{A}_F$.

To prove the compactness of $\mathbb{A}_F/F$, we will separate the cases of number fields and function fields. Let $F_\infty := \prod_{v \notin \Sigma} F_v = F \otimes \mathbb{Q} \mathbb{R}$.

Assume that $F$ is a number field. We will use the following lemmas.

**Lemma 2.1.7.** Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be finitely many maximal ideals of $\mathcal{O}_F$, elements $x_i \in \mathcal{O}_{\mathfrak{p}_i}$ in the valuation rings of $F_{\mathfrak{p}_i}$ and $\varepsilon_i > 0$ some real numbers for $1 \leq i \leq r$. Then there exists $\xi \in \mathcal{O}_F$ such that $|\xi - x_i|_{\mathfrak{p}_i} < \varepsilon_i$ for $1 \leq i \leq r$.

**Proof.** Equivalently we have to prove that, for every choice of integral numbers $n_i \geq 1$, the diagonal map $\mathcal{O}_F \to \prod_{i=1}^r \mathcal{O}_F/\mathfrak{p}_i^{n_i}$ is surjective. This is a consequence of the fact that $\mathcal{O}_F = \mathfrak{p}_1^{n_1} + \prod_{j \neq i} \mathfrak{p}_j^{n_j}$ for all $1 \leq i \leq r$.  

**Lemma 2.1.8.** We have $\mathbb{A}_F = F + F_\infty \times \prod_{v \notin \Sigma} \mathcal{O}_v$.

**Proof.** Let $x = (x_v)_v \in \mathbb{A}_F$. There exists some natural number $m \geq 1$ such that $m x_v \in \mathcal{O}_v$ for all $v \nmid \infty$. Let’s choose $0 < \varepsilon_v < |m|_v^{-1}$ for each $v \nmid m$. By Lemma 2.1.7 there exists some $\xi \in \mathcal{O}_F$ such that $|m x_v - \xi| < \varepsilon_v$ for all $v \nmid m$. Then we have $|x_v - \frac{\xi}{m}| \leq 1$ for all $v \nmid \infty$ so that $x = \frac{\xi}{m} + y$ where $\frac{\xi}{m} \in F$ and $y \in F_\infty \times \prod_{v \nmid \infty} \mathcal{O}_v$.  

Lemma 2.1.9. We have \( F \cap F_\infty \times \prod_{v \mid \infty} \mathcal{O}_v = \mathcal{O}_F. \)

Proof. This is clear: if \( \xi \in F \) is such that \( |\xi|_p \leq 1 \) for all maximal ideals \( p \) of \( \mathcal{O}_F \), then \( \xi \in \mathcal{O}_F. \)

Then Lemmas 2.1.8 and 2.1.9 implies that the inclusion \( F_\infty \times \prod_{v \mid \infty} \mathcal{O}_v \subset \mathbb{A}_F \) induces a group isomorphism

\[
(F_\infty \times \prod_{v \mid \infty} \mathcal{O}_v)/\mathcal{O}_F \cong \mathbb{A}_F/F.
\]

The \( \mathbb{Z} \)-module \( \mathcal{O}_F \) is finite free and generates the \( \mathbb{Q} \)-vector space \( F \), therefore there exists a \( \mathbb{Z} \)-basis \( (e_1, \ldots, e_d) \) of \( \mathcal{O}_F \) which is also a \( \mathbb{Q} \)-basis of \( F \). This implies that

\[
(e_1 \otimes 1, \ldots, e_d \otimes 1)
\]

is an \( \mathbb{R} \)-basis of the \( \mathbb{R} \)-vector space \( F_\infty = F \otimes_{\mathbb{Q}} \mathbb{R} \). Let

\[
Q := \left\{ \sum_{i=1}^d t_i (e_i \otimes 1) \mid 0 \leq t_i \leq 1 \right\}.
\]

Then the inclusion \( Q \subset F_\infty \) induces a continuous a surjective map \( Q \to F_\infty/\mathcal{O}_F \). As \( \mathcal{O}_F \) acts freely on \( F_\infty \), the map \( Q \times \prod_{v \mid \infty} \mathcal{O}_v \to (F_\infty \times \prod_{v \mid \infty} \mathcal{O}_v)/\mathcal{O}_F \) is surjective. Finally the composite map \( Q \times \prod_{v \mid \infty} \mathcal{O}_v \to \mathbb{A}_F \to \mathbb{A}_F/F \) is surjective and continuous. As \( Q \times \prod_{v \mid \infty} \mathcal{O}_v \) is compact, so is \( \mathbb{A}_F/F \).

The case of function fields is left as an exercise. \( \square \)

2.1.3 Haar measures

Lemma 2.1.10. Let \( X \) be a locally compact topological space such that \( X \) can be written as a increasing union of open subset \( (X_n)_{n \in \mathbb{N}} \). Let \( (\mu_n)_{n \in \mathbb{N}} \) be a family where \( \mu_n \) is a Radon measure on \( X_n \) such that \( \mu_{n+1} |_{X_n} = \mu_n \) for all \( n \geq \mathbb{N} \). Then there exists a unique Radon measure \( \mu \) on \( X \) inducing \( \mu_n \) on each \( X_n \).

Let \( (G_v)_{v \in \Sigma} \) be family of locally compact groups and \( (K_v)_{v \in \Sigma - \Sigma_\infty} \) a family of compact open subgroups. Assume that for each \( v \in \Sigma \), \( \mu_v \) is a left Haar measure over \( G_v \) such that \( \mu_v(K_v) = 1 \) for all \( v \notin \Sigma_\infty \).

In order to describe a (left) Haar measure on \( G := \prod'_{v \in \Sigma} G_v \), it is sufficient to describe a Haar measure \( \mu_S \) on each \( G_S := \prod_{v \in S} G_v \times K_S \) where \( K_S := \prod_{v \in S} K_v \) for each finite subset \( S \subset \Sigma \subset T \), so that the restriction of \( \mu_T \) to \( G_S \) is \( \mu_S \) if \( S \subset T \).

Lemma 2.1.11. There is a unique Radon measure \( \mu^S \) on \( K_S \) such that, for each finite subset \( T \subset \Sigma \setminus S \) and \( (f_v)_{v \in T} \in \prod_{v \in T} C(G_v, \mathbb{R}) \),

\[
\int_{K^T} (f_T \otimes 1^T) \mu^S = \prod_{v \in T} \int_{G_v} f_T \otimes_{v \notin T} \mu_v.
\]
As a consequence, $\mu^S = \otimes_{v \in T} \mu_v \otimes \mu^{S \setminus T}$.

**Proof.** Let $I_T$ be the positive linear form on $C(\prod_{v \in T} K_v, \mathbb{R})$ associated to the product measure $\otimes_{v \in T} \mu_v$ over $\prod_{v \in T} K_v$. If $T \subset T'$, we can define an $\mathbb{R}$-linear injection $C(\prod_{v \in T} K_v, \mathbb{R}) \subset C(\prod_{v \in T'} K_v, \mathbb{R})$ induced by the projection $\prod_{v \in T} K_v \to \prod_{v \in T'} K_v$. Fubini Theorem and the fact that the total measures of the $\mu_v$ are 1 shows that the restriction of $I_{T'}$ to $C(\prod_{v \in T} K_v, \mathbb{R})$ is $I_T$. Therefore there exists a positive linear form $I_S$ on $\bigcup_{T \subset \Sigma \setminus \{v \in T \}} C(\prod_{v \not\in T} K_v, \mathbb{R})$. In order to prove the existence of the measure $\mu^S$ we just have to check that the left hand side is dense in the right hand side and that $I_S$ is continuous. The continuity is a consequence of the fact all the inclusions $C(\prod_{v \in T} K_v, \mathbb{R}) \subset C(\prod_{v \not\in S} K_v, \mathbb{R})$ are isometries for the sup norm and from

$$\left| \int_{\prod_{v \in T} K_v} f_T \mu_T \right| \leq \| f \|_{\infty}.$$  

Let’s prove the density. If $f \in C(\prod_{v \not\in S} K_v, \mathbb{R})$ and if $\varepsilon > 0$, for each point $x$, there exists a subset $T_x \subset T$, such that $f(U_{x,T_x} \times \prod_{v \not\in T_x} K_v) \subset f(x) - \varepsilon, f(x) + \varepsilon$, where $U_{x,T}$ is an open subset of $\prod_{v \in T_x} K_v$ containing $(x_v)_{v \in T_x}$. As $K^S$ is compact, there exists a finite covering of $K^S$ by some $U_{x,T_x}$ so that there exists some $T$ and $g \in C(\prod_{v \in T} O_v, \mathbb{R})$ such that $\| f - g \|_{\infty} < \varepsilon$. \hfill \Box

Now we can define $\mu_S = \prod_{v \in S} \mu_v \otimes \mu^S$. This is a Radon measure over $G_S$. As all the $\mu_v$ are left $G_v$-invariant, the measure $\mu_S$ is left $G^S$-invariant and is a Haar measure. If $S \subset S'$, we have $\mu_{S'}|_{G_S} = \mu_S$ so that they glue into a Haar measure $\mu$ over $G$.

We apply this general construction to the case $G = \mathbb{A}_F$ with $G_v = F_v$ and $K_v = O_v$. For each $v \in \Sigma$, we need to fix a normalization $dx_v$ of the Haar measure. We fix

- $\int_{O_v} dx_v = 1$ if $v$ is ultrametric;
- $dx_v$ is the Lebesgue measure if $F_v = \mathbb{R}$;
- $dx_v := 2 dx dy = dz d\bar{z}$ if $F_v = \mathbb{C}$.

**Proposition 2.1.12.** Let $G$ be a locally compact abelian group. Let $H$ be a closed subgroup of $G$ and $\pi : G \to G/H$ the quotient map. Let $dg$ be a Haar measure
over $G$ and $dh$ a Haar measure over $H$. Then there exists a unique Haar measure $d\overline{g}$ over $G/H$ such that

$$\forall f \in C_c(G, \mathbb{R}), \quad \int_{G/H} \overline{f}(\overline{g}) \, d\overline{g} = \int_{G} f(g) \, dg$$

where $\overline{f} \in C_c(G/H, \mathbb{R})$ is defined by $\overline{f}(\overline{g}) := \int_{H} f(g + h) \, dh$ for $g$ lifting $\overline{g}$.

If $H$ is a discrete subgroup of $G$, then we can choose for $dh$ to be the counting measure such that each singleton has measure 1. Then $f(g) = \sum_{\gamma \in \Gamma} f(g + \gamma)$.

**Proof.** The linear map $f \mapsto \overline{f}$ from $C_c(G, \mathbb{R})$ to $C_c(G/H, \mathbb{R})$ is surjective. Namely let $h \in C_c(G/H, \mathbb{R})$. The support of $h$ being compact and $\pi : G \to G/H$ being open, the support of $h$ can be covered by finitely many relatively compact open subsets $U_i$ of the form $\pi(V_i)$ with $V_i \subset G$ relatively compact. Then $C := \bigcup_i V_i$ is a compact subset of $G$ such that $\pi(C)$ contains the support of $h$. Let $F \in C_c(G, \mathbb{R})$ be a function such that $F > 0$ on $C$ (to show that $F$ exist, use the fact that a locally compact topological group is *normal* by [Bou71, Ch. III §4 Prop. 13] and [Bou74, Ch. IX §4 Prop 4]). Then the function $f$ on $G$ defined by

$$f(g) := \begin{cases} h(\pi(g))f(g)\overline{f}(g)^{-1} & \text{if } g \in C \\ 0 & \text{if } g \notin C \end{cases}$$

is in $C_c(G, \mathbb{R})$ and $\overline{f} = h$. We can define a Haar measure over $G/H$ by the formula

$$\int_{G/H} h \, d\overline{g} := \int_{G} f \, dg$$

where $h = \overline{f}$. To check that it is well defined, it is sufficient to check that $\int_{G} f \, dg = 0$ if $\overline{f} = 0$. Let $C$ be the support of $f$. Then there exists a positive function $\psi \in C_c(G, \mathbb{R})$ such that $\overline{\psi}$ is equal to 1 on $C$. We deduce that

$$0 = \int_{G} \psi(g) \int_{H} f(g + h) \, dh \, df = \int_{H} \int_{G} \psi(g) f(g + h) \, dg \, dh$$

$$= \int_{H} \int_{G} \psi(g - h)f(g) \, dg \, dh = \int_{G} \overline{\psi}(\pi(g))f(g) \, dg = \int_{G} f(g) \, dg. \quad \square$$

**Remark 2.1.13.** Assume that $G \simeq H_1 \times H_2$, with $G$, $H_1$ and $H_2$ locally compact abelian groups. Let $dg$ be a Haar measure on $G$ and $dh_1$ a Haar measure on $H_1$. It follows from Proposition 2.1.12 that there exists a unique Haar measure $dh_2$ on $H_2$ such that $dg = dh_1 \otimes dh_2$. 
Let $G$ be locally compact abelian group and $\Gamma$ a discrete subgroup of $G$. A \textit{fundamental domain} for the action of $\Gamma$ over $G$ is a measurable subset $D \subset G$ such that $G = \bigcup_{\gamma \in \Gamma} (\gamma + D)$ and $D \cap (\gamma + D)$ has measure 0 if $\gamma \neq 0$. A fundamental domain is \textit{strict} if we have moreover $D \cap (\gamma + D) = \emptyset$ when $\gamma \neq 0$.

**Lemma 2.1.14.** Assume that $\Gamma$ is a discrete countable subgroup of $G$. Let $D$ be a fundamental domain for the action of $\Gamma$ over $G$. Then

$$\forall f \in C_c(G/\Gamma, \mathbb{R}), \quad \int_{G/\Gamma} f(g) \, dg = \int_D (f \circ \pi)(g) \, dg.$$ 

**Proof.** Let $h \in C_c(G)$ such that $f = h$. Then

$$\int_{G/\Gamma} f = \int_G h = \sum_{\gamma \in \Gamma} \int_{D + \gamma} h = \int_D (\sum_{\gamma \in \Gamma} h(g - \gamma)) \, dg = \int_D f(\pi(g)) \, dg. \quad \square$$

**Corollary 2.1.15.** We have $\text{Vol}(G/\Gamma) = \text{Vol}(D)$.

We will now consider the case where $G = \mathbb{A}_F$ and $\Gamma = F$. We endow $\mathbb{A}_F$ with its normalized measure $dx$ and $F$ with the counting measure. We obtain a natural quotient measure on $\mathbb{A}_F/F$ and we want to compute its volume.

**Theorem 2.1.16.** If $F$ is a number field, we have $\text{Vol}(\mathbb{A}_F/F) = \sqrt{|\Delta_{\mathcal{O}_F/\mathbb{Z}}|}$.

**Proof.** We need to determine first a fundamental domain for the action of $F$. As seen in the proof of Theorem 2.1.6, it is equivalent to determine a fundamental domain for the action of $\mathcal{O}_F$ on $F_\infty \times \prod_{v \nmid \infty} \mathcal{O}_v$. As $\mathcal{O}_F$ acts freely on $F_\infty$, if $Q$ is a fundamental domain for $\mathcal{O}_F$ acting on $F_\infty$, then $Q \times \prod_{v \nmid \infty} \mathcal{O}_v$ is a fundamental domain for $F$ acting on $\mathbb{A}_F$. For the normalized measure over $\mathbb{A}_F$, we have

$$\text{Vol}(Q \times \prod_{v \nmid \infty} \mathcal{O}_v) = \text{Vol}(Q).$$

Therefore it is sufficient to compute $\text{Vol}(Q)$. Let’s recall that we can choose $Q$ of the form

$$Q := \left\{ \sum_{i=1}^d t_i (e_i \otimes 1) \mid 0 \leq t_i \leq 1 \right\},$$

Let $j_1, \ldots, j_{r_1}$ be the real embeddings of $F$ and $j_{r_1+1}, \overline{j_{r_1+1}}, \ldots, j_{r_1+r_2}, \overline{j_{r_1+r_2}}$ be the complex embeddings (recall that $d = [F : \mathbb{Q}] = r_1 + 2r_2$). We can identify $F_\infty$ to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ via $e \otimes 1 \mapsto (j_1(e), \ldots, j_{r_1+r_2}(e))$. We identify each $\mathbb{C}$ to $\mathbb{R}^2$ via $z \mapsto (\text{Re}(z), \text{Im}(z))$ and $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ to $\mathbb{R}^d$. The image of $Q$ is

$$\left\{ \sum_{i=1}^d t_i j_i (e_i) \mid 0 \leq t_i \leq 1 \right\}.$$
where \( j(e) = (j_1(e), \ldots, j_r(e), \text{Re} j_{r+1}(e), \text{Im} j_{r+1}, \ldots, \text{Im} j_{r+r}(e)) \). As the \( \mathbb{R} \)-isomorphism \( F_\infty \cong \mathbb{R}^d \) exchange the normalized Haar measure with \( 2^r \) times the Lebesgue measure over \( \mathbb{R}^d \), we have

\[
\text{Vol}(Q) = 2^{2r} \begin{vmatrix} j_1(e_1) & \cdots & \text{Im} j_1(e_d) \\ \vdots & \ddots & \vdots \\ \text{Re} j_{r+1}(e_1) & \cdots & \text{Re} j_{r+1}(e_d) \\ \text{Im} j_{r+1}(e_1) & \cdots & \text{Im} j_{r+1}(e_d) \end{vmatrix} = 2^{2r} 2^{-r_2} \begin{vmatrix} j_1(e_1) & \cdots & j_1(e_d) \\ \vdots & \ddots & \vdots \\ j_{r+1}(e_1) & \cdots & j_{r+1}(e_d) \\ j_{r+1}(e_1) & \cdots & j_{r+1}(e_d) \end{vmatrix} = \det((j(e_i))_{i \in \text{Hom}(F, \mathbb{C})})_{1 \leq i \leq d} = |\Delta_{O_F/\mathbb{Z}}|^\frac{1}{2}.
\]

\[\square\]

### 2.2 Ideles

#### 2.2.1 Definition and first properties

Let \( F \) be a global field. The idele group \( I_F \) of \( F \) is the restricted product of the locally compact groups \( (F_v^\times)_{v \in \Sigma} \) with respect to the compact open subgroups \( (\mathcal{O}_v^\times)_{v \notin \Sigma_\infty} \).

Recall that if \( R \) is a topological ring, the natural topology of \( R^\times \) is the topology induced by the inclusion \( i : R^\times \hookrightarrow R^2 \) defined by \( x \mapsto (x, x^{-1}) \). For this topology, \( R^\times \) is a topological group.

**Proposition 2.2.1.** 1. The topological group of ideles \( I_F \) is isomorphic to \( \mathbb{A}_F^\times \) with its natural topology.

2. The diagonal inclusion of \( F^\times \) into \( I_F \) has a discrete image.

**Proof.** First of all, we remark that if \( x = (x_v)_{v \in \Sigma} \in I_F \), then \( (x_v)_{v \in \Sigma} \in \mathbb{A}_F \) and \( (x_v^{-1})_{v \in \Sigma} \in \mathbb{A}_F \) so that \( (x_v)_{v \in \Sigma} \in \mathbb{A}_F^\times \). Conversely if \( x = (x_v)_{v \in \Sigma} \in \mathbb{A}_F^\times \), there exists \( y = (y_v)_{v \in \Sigma} \) such that \( xy = 1 \). Then \( |x_v| \leq 1 \) for almost all \( v \) and \( |y_v| = |x_v|^{-1} \leq 1 \) for almost all \( v \), this implies that \( (x_v)_{v \in \Sigma} \in I_F \). A basis of neighborhoods of 1 in \( \mathbb{A}_F^\times \) for the natural topology is given by

\[
i^{-1}(U_S \times \prod_{v \notin S} \mathcal{O}_v) \times (V_S \prod_{v \notin S} \mathcal{O}_v) = \{ (x_v)_{v \in \Sigma} \in I_F \mid (x_v)_{v \in S} \in U_S \cap V_S^{-1}, x_v \in \mathcal{O}_v^\times \text{ for } v \notin S \}.
\]

This is a basis of neighborhoods of 1 for the topology of \( I_F \).

In order to prove that \( F^\times \) is discrete in \( I_F \), we can remark that the inclusion \( I_F \hookrightarrow \mathbb{A}_F \) is continuous, so that the inverse image \( F \) is discrete. \( \square \)
2.2. IDELES

Remark 2.2.2. Even if the inclusion \( I_F \subset \mathbb{A}_F^\times \) is continuous, this is not an homeomorphism onto its image. Namely the topology of \( I_F \) is strictly finer than the topology induced by \( \mathbb{A}_F \). Namely we can check that \( \mathbb{A}_F^\times \) is not a topological group for the topology induced by \( \mathbb{A}_F \).

Soit \( x = (x_v)_{v \in \Sigma} \in I_F \) be an idele. We define its idele norm as the real number

\[
|x| := \prod_{v \in \Sigma} |x_v|_v
\]

where \(|·|_v\) is the normalized absolute value on \( F_v \) (note that when \( F_v = \mathbb{C} \), this is not really an absolute value...). This product is well defined since \(|x_v|_v = 1\) for almost all \( v \).

The idele norm defines a (continuous) group homomorphism \( I_F \to \mathbb{R}_{>0} \) whose kernel is denoted \( I_F^1 \).

Lemma 2.2.3. a) If \( F \) is a number field, there is an isomorphism of topological groups \( I_F \cong I_F^1 \times \mathbb{R}_{>0} \).

b) If \( F \) is a function field, there is an isomorphism of topological groups \( I_F \cong I_F^1 \times \mathbb{Z} \).

Proof. a) We just have to show that there exists a continuous section to \(|·|\).

Let \( v_0 \) be an archimedean place and define, for \( t \in \mathbb{R}_{>0} \), \( s(t) = (x_v)_v \) with \( x_{v_0} := t^{|t|_v} \) and \( x_v = 1 \) for \( v \neq v_0 \). Then \( s \) is a continuous section to \(|·|\).

b) Let \( q \) be the gcd of all \( q_v := |k_v| \). Then for each place \( v \), we have \( q_v = q^{f_v} \) for some integer \( f_v \geq 1 \). Moreover there is a family \( (m_v)_v \in \mathbb{Z}^\Sigma \) such that \( m_v = 0 \) for almost all \( v \) and \( \sum_v m_v f_v = 1 \). Then we have \(|I_F| \subset q^Z \subset \mathbb{R}_{>0} \) and we define a group homomorphism \( s : q^Z \to I_F \) by \( s(q^n) := (x_v) \) where \( x_v = \pi_v^{-nm_v} \). Then we have \(|s(q^n)| = q^n \) for all \( n \in \mathbb{Z} \). We easily derive the isomorphism.

Theorem 2.2.4. We have \( F^\times \subset I_F^1 \) and the quotient group \( I_F^1/F^\times \) is compact.

Proof. The inclusion \( F^\times \subset I_F^1 \) is a direct consequence of the product formula. Let’s prove the compactness of the quotient. For \( t > 0 \) we define

\[
I_F^t := \{ x \in I_F \mid |x| = t \}.
\]

Lemma 2.2.5. There exists a real number \( C > 0 \) such that if \( x = (x_v)_v \in I_F \) is such that \(|x| > C\), there exists \( \xi \in F^\times \) such that \(|\xi|_v \leq |x_v|_v \) for all \( v \in \Sigma \).

Proof. Let \( A_x := \{ y = (y_v)_v \in \mathbb{A}_F \mid |y_v|_v \leq \delta_v |x_v|_v \} \) where \( \delta_v = 1 \) excepted when \( v \) is archimedean where \( \delta_v = 1/4 \). Then \( \text{Vol}(A_x) = \alpha \prod_v |x_v|_v \) for some \( \alpha > 0 \) independent on \( x \). Let \( C > 0 \) be such that \( C\alpha > \text{Vol}(\mathbb{A}_F/F) \). Then if \(|x| > C\), there exist \( x_1 \) and \( x_2 \) in \( A_x \) such that \( x_1 - x_2 \in F^\times \). Then we have \(|\xi|_v \leq |x_v|_v \) for all \( v \in \Sigma \).
Lemma 2.2.6. There exists a real number $C > 0$ such that for all $t > C$ and $x = (x_v)_v \in I^1_F$, there exists $\xi \in F^\times$ such that $1 \leq |\xi x_v|_v \leq t$ for all $v \in \Sigma$.

Proof. Let $C > 0$ be as in the previous lemma. For $x = (x_v)_v \in I^1_F$, we have $|x| > C$ so that there exists $\xi \in F^\times$ such that $|\xi^{-1}|_v \leq |x_v|_v$ for all $v \in \Sigma$. This gives us $|\xi x_v|_v \geq 1$ for all $v \in \Sigma$. Let $v \in \Sigma$, we have

$$|\xi x_v|_v = \frac{\xi x_v}{\prod_{w \neq v} |x_w|_w} \leq |\xi x| = |x| = t.$$ 

Lemma 2.2.7. Let $t > 1$. There exist only finitely many ultrametric places $v$ of $F$ such that $q_v := |k_v| \leq t$.

Proof. Left as an exercise.

We can finish the proof of the theorem. Let $C > 0$ be as in lemma 2.2.6 and let $t > \max\{C, 1\}$ such that $t \in |I^1_F|$. By Lemma 2.2.7, there is a finite set of places $S$ of $F$ containing $\Sigma_{\infty}$ such that $q_v > t$ if $v \notin S$. Let $x \in I^1_F$. By Lemma 2.2.6, there exists $\xi \in F^\times$ such that $1 \leq |\xi x_v|_v \leq t$ for all $v \in \Sigma$. As $|F_v| \cap [1, t[ \subset |F_v| \cap [1, q_v[ = \emptyset$, we have $|\xi x_v|_v = 1$ for $v \notin S$. Therefore

$$\xi x \in \prod_{v \in S} \{y_v \in F^\times_v | 1 |y_v|_v \leq t\} \times \prod_{v \notin \Sigma} \mathcal{O}_v^\times$$

and this subset is compact. We have proved that there exists a compact subset of $I^1_F$ which surjects onto $I^1_F / F^\times$. By translation by the inverse of an element of $I^1_F$, we obtain a compact subset of $I^1_F$ which surjects onto $I^1_F / F^\times$.

2.2.2 Ideles and ideals

The case of number fields

Let $F$ be a number field and let $x = (x_v)_v \in I_F$. We can associate to $x$ a fractional ideal $\mathfrak{a}(x)$ of $\mathcal{O}_F$. This is the ideal

$$\mathfrak{a}(x) := \prod_{v \in \Sigma \setminus \Sigma_{\infty}} \mathfrak{p}_v^{v(x_v)}$$

where $v(x_v) \in \mathbb{Z}$ is the $v$-adic valuation of $x_v$, that is $|x_v| = q_v^{-v(x_v)}$.

Example 2.2.8. If $v \in \Sigma \setminus \Sigma_{\infty}$ and $\pi_v$ is an uniformizer of $F_v$, if $x^{(v)} := (x_w)_w$ with $x_v = \pi_v$ and $x_w = 1$ when $w \neq v$, then $\mathfrak{a}(x^{(v)})$ is just the prime ideal $\mathfrak{p}_v$. 
Let’s remark that $a(x) = \mathcal{O}_F$ if and only if $|x_v|_v = 1$ for all $v \in \Sigma \setminus \Sigma_{\infty}$. Therefore we obtain a group homomorphism toward the group of nonzero fractional ideals of $\mathcal{O}_F$

$$a : I_F \to \mathcal{I}_{\mathcal{O}_F}. $$

It is clearly surjective and its kernel is $F_{\infty}^\times \times \prod_{v \mid \infty} \mathcal{O}_v^\times$. In other words, we have an exact sequence of topological groups

$$1 \to F_{\infty}^\times \times \prod_{v \mid \infty} \mathcal{O}_v^\times \to I_F \to \mathcal{I}_{\mathcal{O}_F} \to 1. $$

Let $\mathcal{P}_{\mathcal{O}_F} \subset \mathcal{I}_{\mathcal{O}_F}$ be the subgroup of principal ideals. Let’s remark that $a(F^\times) \subset \mathcal{P}_{\mathcal{O}_F}$ so that we obtain a surjective group homomorphism

$$\overline{a} : I_F/(F_{\infty}^\times F_{\infty}^\times \times \prod_{v \mid \infty} \mathcal{O}_v^\times) \to \text{Cl}(\mathcal{O}_F) = \mathcal{I}_{\mathcal{O}_F}/\mathcal{P}_{\mathcal{O}_F}. $$

**Proposition 2.2.9.** The map $\overline{a}$ is an isomorphism.

**Proof.** We just need to prove that it is injective. Assume that $\overline{a}(x) = 0$. This means that $a(x) = (\xi)$ for some $\xi \in F^\times$. Therefore $a(\xi^{-1}x) = 0$ so that $\xi^{-1}x \in F_{\infty}^\times \times \prod_{v \mid \infty} \mathcal{O}_v^\times$. $\square$

**Corollary 2.2.10.** The class group $\text{Cl}(\mathcal{O}_F)$ is a finite group.

**Proof.** Let $G := I_F/F_{\infty}^\times F_{\infty}^\times \times \prod_{v \mid \infty} \mathcal{O}_v^\times$ and $G^1 := I_F^1/F^\times$. As $|F_{\infty}^\times| = \mathbb{R}_{>0}$, the natural continuous map $G^1 \to G$ is surjective. As $G^1$ is compact by Theorem 2.2.4, the group $G$ is compact. Moreover $F_{\infty}^\times \times \prod_{v \mid \infty} \mathcal{O}_v^\times$ is an open subgroup $I_F$, it follows that the quotient of $I_F$ by $F_{\infty}^\times \times \prod_{v \mid \infty} \mathcal{O}_v^\times$ is discrete and so is $G$. Finally $G$ is compact and discrete, hence finite. $\square$

**The case of function fields**

Let $k$ be a finite field and let $F$ be a finite extension of $k(T)$. The algebraic closure of $k$ in $F$ is finite, so that up to replacing $k$ by its algebraic closure in $F$, we can assume that $k$ is algebraically closed in $F$. It is called the field of constants of $F$.

Recall that we denote by $\Sigma$ the set of places of $F$ (and recall that they are ultrametric). A **divisor** of $F$ is map with finite support

$$d : \begin{cases} \Sigma & \longrightarrow \mathbb{Z} \\ v & \longmapsto d(v) \end{cases} $$

We use the notation $\sum d(v)v$ for such a map. The **degree** of a divisor $d$ is the integer $\sum_v f_v d(v)$ where $f_v := [k_v : k]$. The set $\text{Div}(F)$ of divisors of $F$ has a
natural group structure, this is the free abelian group generated by the places of $F$. The degree defines a group homomorphism $\text{Div}(F) \to 0$. Its kernel $\text{Div}^0(F)$ is the subgroup of divisors of degree 0.

We can define a group homomorphism $\text{div} : I_F \to \text{Div}(F)$ by the formula

$$\text{div}((x_v)_v) := \sum_v d(v)v$$

where $|x_v|_v = q_v^{-d(v)}$ where $q_v$ is the cardinal of the residue field $k_v$ at $v$ and $|\cdot|_v$ is the normalized absolute value over $F_v$. The map $\text{div}$ is clearly surjective. Moreover we have $\text{div}(x) \in \text{Div}^0(F)$ if and only if $x \in I_F^1$ so that $\text{div}(I_F^1) = \text{Div}^0(F)$.

It follows from the product formula that $\text{div}(F^\times) \subset \text{Div}^0(F)$. We define the Picard groups of $F$ as

$$\text{Pic}(F) := \text{Div}(F)/\text{div}(F^\times), \quad \text{Pic}^0(F) := \text{Div}^0(F)/F^\times.$$  

**Theorem 2.2.11.** The Picard group of degree 0 $\text{Pic}^0(F)$ is a finite group.

**Proof.** This is a quotient of $I_F^1/F^\times$, so that it is a compact group. Moreover, as $\prod_v \mathcal{O}_v^\times$ is open in $I_F$, the group $\text{Pic}(F)$ is discrete as a topological group. The map $I_F^1/F^\times \to \text{Pic}^0(F)$ where $\text{Pic}^0(F)$ has the topology induced by the one of $\text{Pic}(F)$ is continuous and, since $I_F^1/F^\times$ is compact, it coincides with the quotient topology from $I_F^1/F^\times \to \text{Pic}^0(F)$. Therefore $\text{Pic}^0(F)$ is both discrete and compact and so is finite.  

**Remark 2.2.12.**  1) We have a group exact sequence

$$1 \to k^\times \to F^\times \to \text{Div}^0(F) \to \text{Pic}^0(F) \to 1.$$  

Namely we just need to check that an element $\xi \in F^\times$ such that $\text{div}(\xi) = 0$ is in $k$. But this is an element of the group $F^\times \cap \prod_v \mathcal{O}_v^\times$ which is both discrete and compact, hence finite. Therefore $\xi$ is a root of unity, thus algebraic over $k$ and so is in $k$.

2) We can prove that there exists a geometrically connected projective smooth curve $C$ defined over $k$ such that $F$ is the fraction field of $C$. Then $\text{Pic}(F)$ is isomorphic to the group of isomorphism classes of invertible sheaves over $C$ and $\text{Pic}^0(C)$ to the subgroup of invertible sheaves of degree 0.

### 2.2.3 Fundamental domain of $I_F/F^\times$ and Dirichlet unit Theorem

**Case of a number field**

Let $h$ be the cardinal of the class group $\text{Cl}(\mathcal{O}_F)$. We have constructed a surjective homomorphism $I_F^1/F^\times \to \text{Cl}(\mathcal{O}_F)$. Let $a_1, \ldots, a_h$ be some lifts in $I_F^1$ of the
elements of \( \text{Cl}(\mathcal{O}_F) \). We have

\[
I_F^1 = \prod_{i=1}^{h} a_i \left(F_\infty^1 \prod_{v|\infty} \mathcal{O}_v^x \right) F^x
\]

where \( F_\infty^1 \) is the subgroup of \( F_\infty^x \) consisting of elements \( (x_v)_{v|\infty} \) such that \( \prod_v |x_v| = 1 \). We are consequently reduced to find a fundamental domain for

\[
(F_\infty^1 \prod_{v|\infty} \mathcal{O}_v^x) F^x / F^x \simeq (F_\infty^1 \prod_{v|\infty} \mathcal{O}_v^x) / \mathcal{O}_F^x
\]

since \( F^x \cap (F_\infty^1 \prod_{v|\infty} \mathcal{O}_v^x) = \mathcal{O}_F^x \).

**Lemma 2.2.13.** Let \( A \) and \( B \) be two set and \( \Gamma \) a group acting on \( A \) and \( B \). If \( D \) is a strict fundamental domain for the action of \( \Gamma \) on \( A \), then \( D \times B \) is a fundamental domain for the action of \( \Gamma \) on the product \( A \times B \).

**Proof.** Exercise.

Therefore we are reduced to find a fundamental domain \( D_\infty \) for the action of \( \mathcal{O}_F^x \) on \( F_\infty^1 \).

Let \( L : F_\infty^x \to \mathbb{R}^{r_1+r_2} \) be the group homomorphism defined by

\[
L(x) := (\log |x_v|_v)_v, \quad x = (x_v)_{v|\infty}.
\]

The product formula implies that \( L(\mathcal{O}_F^x) \) is included in the hyperplane \( H \) of \( \mathbb{R}^{r_1+r_2} \) of equation \( \sum_v X_v = 0 \).

We have \( L(F_\infty^x) \) and the preimage of \( H \) by \( L \) is exactly the subgroup \( F_\infty^1 \subset F_\infty^x \). Therefore we obtain an isomorphism

\[
F_\infty^1 / \mathcal{O}_F^x \simeq H / L(\mathcal{O}_F^x).
\]

**Proposition 2.2.14.** The subgroup \( L(\mathcal{O}_F^x) \) is a lattice of \( H \).

**Proof.** The morphism \( L : F_\infty^x \to \mathbb{R}^{r_1+r_2} \) is open (this is the case of each \( |\cdot|_v : F_v^x \to \mathbb{R}_{>0} \) if \( v \mid \infty \) and so the case of each \( \log |\cdot|_v \)). Therefore \( L \) induces an homeomorphism \( F_\infty^x / \text{Ker} L \simeq \mathbb{R}^{r_1+r_2} \). As moreover the kernel of \( L \) is compact, the map \( L \) is closed. As \( \mathcal{O}_F^x \subset F_\infty^1 \) is closed, so is \( L(\mathcal{O}_F^x) \) in \( H \) and the quotient \( H / L(\mathcal{O}_F^x) \) is separated. As \( H / L(\mathcal{O}_F^x) \) is moreover a quotient of \( F_\infty^1 / \mathcal{O}_F^x \), this is a compact group. This implies that \( L(\mathcal{O}_F^x) \) is a lattice of \( H \). \( \Box \)

We have used:

**Lemma 2.2.15.** Let \( H \subset G \) be a compact subgroup of locally compact group. The quotient map \( \pi : G \to G / H \) is closed.
Let $F$ be a closed subset of $G$. By definition of the quotient topology, $\pi(F)$ is closed in $G/H$ if and only if $\pi^{-1}(\pi(F))$ is closed in $G$. But $\pi^{-1}(\pi(F)) = F \cdot H$. If $x \notin F \cdot H$, for each $h \in H$, $Fh$ is closed in $G$ and there exists an open neighborhood $V_h$ of $e_G$ such that $xV_h \notin Fh$, ie $x \notin FhV_h^{-1}$. We have $H \subset \bigcap_{h \in H} hV_h^{-1}$. As $H$ is compact there exists finitely many $h_i$ such that $H \subset \bigcap_i h_i V_{h_i}^{-1}$. Then $\bigcap_i xV_{h_i}$ is an open subset containing $x$ and disjoint from $F \cdot H$.

**Theorem 2.2.16** (Dirichlet). The group $\mathcal{O}_F^\times$ is finitely generated and isomorphic to $\mu_F \times \mathbb{Z}^{r_1+r_2-1}$ where $\mu_F$ is the finite group of roots of unity in $F$.

**Proof.** As $L(\mathcal{O}_F^\times)$ is a lattice in $H$, it is free of rank $r_1 + r_2 - 1$. The kernel of $L$ is the set of elements of $\xi \in F^\times$ such that $|\xi|_v = 1$ for all $v \in \Sigma$. This is a compact and discrete subspace of $I_F$, thus a finite group. Its elements are therefore the roots of unity in $F$.

Let $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ be elements of $\mathcal{O}_F^\times$ such that the $L(\varepsilon_i)$ form a basis of $L(\mathcal{O}_F^\times)$. Fix $v_0 \in \Sigma_\infty$ and consider $L' : F_\infty^1 \to \mathbb{R}^{r_1+r_2-1}$ the composite of $L$ with the projection of $\mathbb{R}^{r_1+r_2}$ on $\mathbb{R}^{\Sigma_\infty \setminus \{v_0\}}$ obtained by forgetting $v_0$. Then $L'$ is surjective and $L'(\mathcal{O}_F^\times)$ is a lattice of $\mathbb{R}^{\Sigma_\infty \setminus \{v_0\}}$. Set

$$Q := \sum_{v \in \Sigma_\infty \setminus \{v_0\}} \{0, 1[L'(\varepsilon_i)] \}$$

so that we have

$$\mathbb{R}^{\Sigma_\infty \setminus \{v_0\}} = Q + L'(\mathcal{O}_F^\times).$$

Let $w$ be the cardinal of the finite group $\mu_F$. Then

$$D_\infty := \{x = (x_v)_{v \in \Sigma_\infty} \in F_\infty^1 \mid L'(x) \in Q \text{ and } \text{Arg}(x_{v_0}) \in [0, \frac{2\pi}{w}]\}$$

is fundamental domain for the action of $\mathcal{O}_F^\times$ on $F_\infty^1$. Namely the kernel of $L'$ is $\{x \in F_\infty^\times \mid |x|_{v_0} = 1\}$ and the set of numbers in this kernel with argument in $[0, \frac{2\pi}{w}]$ is a fundamental domain for the action of $\mu_F$.

**Proposition 2.2.17.** The set $\prod_{i=1}^h a_i(D_\infty \times \prod_{v|\infty} \mathcal{O}_v^\times)$ is a strict fundamental domain for the action of $F^\times$ on $I_F^1$.

### 2.2.4 Haar measures

As $I_F$ is the direct product of the $F_v^\times$ with respect to the $\mathcal{O}_v^\times$, it is possible to construct a Haar measure on $I_F$ from a family of Haar measures $d^x x_v$ on the $F_v^\times$ if $\int_{\mathcal{O}_v^\times} d^x x_v = 1$ for almost all $v$.

Let $dx_v$ be a Haar measure on $F_v$. As $F_v^\times$ is an open subset of $F_v$, the restriction of $dx_v$ to $F_v^\times$ is a Radon measure on $F_v^\times$. Moreover, by definition of the normalized
2.2. IDELES

absolute value, the measure $|x_v|^{-1} dx_v$ is a Haar measure over $F_v^\times$. Let’s compute the volume of $O_v^\times$ for this measure when $v$ is ultrametric. If $\pi_v$ is a uniformizer of $F_v$, we have $O_v^\times = O_v \setminus \pi_v O_v$ so that

$$\int_{O_v^\times} |x_v|^{-1} dx_v = \int_{O_v^\times} |x_v|^{-1} dx_v = \int_{O_v} dx_v - \int_{\pi_v O_v} dx_v = \text{Vol}(O_v)(1 - q_v^{-1}).$$

Therefore we can make the following choice of a Haar measure over $F_v^\times$ at ultrametric places. Let $dx_v$ be the normalized Haar measure over $F_v$ and define

$$d^\times x_v := \frac{1}{1 - q_v^{-1}} |x_v|^{-1} dx_v.$$

If $v | \infty$, we define $d^\times x_v$ as $|x_v|^{-1} dx_v$. As almost all these measures have integral equal to 1 on $O_v^\times$ for almost all $v$, we can define a Haar measure over $I_F$ by taking their product:

$$d^\times x := \prod_v d^\times x_v.$$

Note that we have a short exact sequence of topological groups:

$$1 \longrightarrow I_F^0 \longrightarrow I_F \longrightarrow |I_F| \longrightarrow 1.$$ 

Where the group $|I_F|$ is $\mathbb{R}_{>0}$ if $F$ is a number field and $\mathbb{Z}$ if $F$ is a function field. We can define a Haar measure over $|I_F|$ as being $t^{-1} dt$ in the first case and the counting measure in the second case. Then there exists a unique Haar measure $d^\times x_1$ on $I_F^0$ such that, for all $f \in C_c(I_F)$, we have

$$\int_{I_F} f(x) d^\times x = \int_{|I_F|} \int_{I_F} f(\omega x_1) d^\times x_1 d\omega.$$

The existence of the measure $d^\times x_1$ follows immediately of the splitting of the exact sequence and from Remark 2.1.13.

We will now compute the volume of the compact group $I_F^0/F^\times$ for the measure we just defined. Assume that $F$ is a number field. Let $\varepsilon_1, \ldots, \varepsilon_{r_1 + r_2 - 1}$ be a fundamental family of units of $O_F^\times$, that is a family such that

$$O_F^\times \simeq \mu_F \times \varepsilon_1^Z \cdots \varepsilon_{r_1 + r_2 - 1}^Z.$$

The regulator of $F$ is the positive real number

$$R_F := |\det((\log(|\varepsilon_i|_v))_{1 \leq i \leq r_1 + r_2 - 1})|_{v \neq v_0}$$

where $v_0$ is a fixed archimedean place of $F$. Let’s remark that the product formula implies that it doesn’t depend on the choice of $v_0$. 
Theorem 2.2.18. We have \( \text{Vol}(I_F^1/F^\times) = 2^r (2\pi)^r h R_F w^{-1} \).

Proof. We have \( I_F^1 = \prod a_i(F_\infty^1 \prod_{\psi|\infty} \mathcal{O}_e^\times) F^\times \), so that \( \text{Vol}(I_F^1/F^\times) = h \text{Vol}(F_\infty^1/\mathcal{O}_F^\times) \) (recall that \( \text{Vol}(\mathcal{O}_e^\times) = 1 \)). Let \( D_\infty \) be the fundamental domain constructed previously and let \( D'_\infty := \{ x \in F_\infty^1 \mid L'(x) \in Q \} \) where we remind that \( Q = \sum_{i=1}^{r_1+r_2-1} [0,1] L'(\varepsilon_i) \). We have \( D'_\infty = \prod_{\zeta \in \mu_F} \zeta D_\infty \) so that \( \text{Vol}(D'_\infty) = w \text{Vol}(D_\infty) \).

Let

\[
E_\infty := \{ x \in F_\infty \mid x = (t, \ldots, t, \frac{t^2}{r_1}, \ldots, \frac{t^2}{r_2}) d \mid t \in [1, \varepsilon], d \in D'_\infty \}.
\]

Then we have

\[
\text{Vol}(E_\infty) = \int_{E_\infty} d^x x = \int_{1}^{e^{r_1+r_2}} \text{Vol}(D'_\infty) \frac{dt}{t} = \text{Vol}(D'_\infty)(r_1 + r_2).
\]

We can now use the decomposition \( F_\infty^\times \simeq (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \) to compute the volume of \( E_\infty \) in polar coordinates. We consider the quotient map \( \rho : F_\infty^\times \to (\mathbb{R}_>0)^{r_1+r_2} \) defined by \( \rho(x) = (|x_\varepsilon|_v) \). We obtain

\[
\int_{E_\infty} d^x x_1 \cdots d^x x_{r_1+r_2} = \int_{\rho(E_\infty)} \frac{dp_1}{\rho_1} \cdots \frac{dp_{r_1+r_2}}{\rho_{r_1+r_2}} = 2^r (2\pi)^r \int_{\rho(E_\infty)} \frac{dp_1}{\rho_1} \cdots \frac{dp_{r_1+r_2}}{\rho_{r_1+r_2}}.
\]

Namely if \( v \) is a complex place, we have \( d^x x_v = \frac{dp_v}{\rho_v} d\theta \). Using the variables \( X_i = \log \rho_i \), the integral \( \int_{\rho(E_\infty)} \frac{dp_1}{\rho_1} \cdots \frac{dp_{r_1+r_2}}{\rho_{r_1+r_2}} \) is the volume of the set

\[
P = \sum_{i=1}^{r_1+r_2-1} [0,1[L(\varepsilon_i) + [0,1[(1, \ldots, 1)]
\]

in \( \mathbb{R}^{r_1+r_2} \). We have

\[
\text{Vol}(P) = \begin{vmatrix} \log|\varepsilon_1| & \cdots & 1 \\ \vdots & \ddots & \vdots \\ \log|\varepsilon_{r_1+r_2}| & \cdots & 1 \\ \log|\varepsilon_1| & \cdots & \log|\varepsilon_{r_1+r_2-1}| \\ \vdots & \ddots & \vdots \\ \log|\varepsilon_{r_1+r_2-1}| & \cdots & \log|\varepsilon_{r_1+r_2-1}| \\ 0 & \cdots & 0 \end{vmatrix} = (r_1 + r_2) R_F. \quad \square
\]
Chapter 3
Zêta functions

3.1 Duality in locally compact abelian groups

3.1.1 Dual of a locally compact abelian group

Let $S^1 := \{ z \in \mathbb{C}^\times \mid |z| = 1 \}$ be the locally compact group of unit complex numbers. If $G$ is locally compact abelian group, we define its dual as the set $\hat{G}$ of continuous group homomorphisms $\chi : G \to S^1$. An element of $\hat{G}$ is also called a unitary character (or sometime just a character). The set $\hat{G}$ is a group for the multiplication law $(\chi_1 \cdot \chi_2)(g) := \chi_1(g)\chi_2(g)$.

We endow the set $\hat{G}$ with the compact open topology. This is the topology generated by the sets of the form

$$W(K,V) = \{ \chi \in \hat{G} \mid \chi(K) \subset V \}$$

for $K$ compact in $G$ and $V$ open in $S^1$. For this topology, $\hat{G}$ is a topological group.

**Theorem 3.1.1.**

1. If $G$ is compact, the topological group $\hat{G}$ is discrete.

2. If $G$ is discrete, the topological group $\hat{G}$ is compact.

3. More generally if $G$ is locally compact, the topological group $\hat{G}$ is locally compact.

**Proof.**

1. We will use the following lemma.

**Lemma 3.1.2** (No small subgroup Lemma). In $\mathbb{C}^\times$ the only subgroup contained in the open ball $B(1, \sqrt{3})$ is the trivial subgroup $\{1\}$.

**Proof.** Let $H$ be a subgroup of $\mathbb{C}^\times$ contained in $B(1, \sqrt{3})$. Then $H$ is bounded, this implies that all its element have absolute value 1 and that $H \subset S^1 \cap B(1, \sqrt{3})$.
CHAPTER 3. ZÉTA FUNCTIONS

As $\mathbb{S}^1 \cap B(1, \sqrt{3})$ is not dense in $\mathbb{S}^1$, then it is a discrete subgroup of $\mathbb{S}^1$, thus a finite subgroup. All the elements of $H$ are roots of unity. Assume that there exists $z = e^{2\pi i \theta} \in H \setminus \{1\}$. Then $\theta = 2\pi i \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $a \wedge b = 1$ and $1 \leq a < b$. If $\frac{a}{b} \notin \left[\frac{1}{3}, \frac{2}{3}\right]$, then either $2\frac{a}{b}$ or $-2\frac{a}{b}$ is in $\left[\frac{1}{3}, \frac{2}{3}\right]$. In all cases we have $z \in H$ such that $\arg(z) \in [2\pi i \frac{1}{3}, 2\pi i \frac{2}{3}]$, which implies $|z - 1| \geq \sqrt{3}$. This is a contradiction.

Assume that $G$ is compact. Then $W(G, B(1, \sqrt{3}))$ is a neighborhood of the trivial character in $\hat{G}$. Moreover if $\chi \in W(G, B(1, \sqrt{3}))$, then $\chi(G)$ is a subgroup of $\mathbb{C}^\times$ which is contained in $B(1, \sqrt{3})$. It follows from the lemma that $\chi$ is the trivial character. This proves that $\hat{G}$ is discrete.

2. Assume that $G$ is discrete. The compact subset of $G$ are the finite sets and the compact open topology on $\hat{G}$ is the topology of pointwise convergence, that is the topology induced by the product topology on $(\mathbb{S}^1)^G$. It is easy to check that the $\hat{G}$ is a closed subset of $(\mathbb{S}^1)^G$. As the latter is compact by Tychonoff Theorem, so is $\hat{G}$.

3. This is [CG47, III.7].

Let $G$ be locally compact abelian group. There is a continuous group homomorphism $G \to \hat{\hat{G}}$ defined by $g \mapsto (\hat{g} \mapsto \hat{g}(\cdot))$ and called biduality homomorphism. We will admit the following result.

**Theorem 3.1.3 (Pontriagin Duality).** The biduality homomorphism is an isomorphism of topological groups.

*Proof.* See Théorème 5 in [CG47, VI.16].

**Corollary 3.1.4.** Let $G$ be a locally compact abelian group. Then $G$ is discrete if and only if $G$ is compact and $G$ is compact if and only if $\hat{G}$ is discrete.

**Corollary 3.1.5.** If $g \in G$. We have $g = 1$ if and only if $\chi(g) = 1$ for all $\chi \in \hat{G}$.

Let $G$ be a locally compact abelian group and let $H$ be a closed subgroup of $G$. Let $H^\perp$ be the subgroup $\{\chi \in \hat{G} \mid \chi|_H = 1\}$. This is a closed subgroup of $\hat{G}$ and there is a topological isomorphism $G/H \simeq H^\perp$ induced by the precomposition of a character with the quotient map $G \to G/H$.

**Proposition 3.1.6.** The restriction from $G$ to $H$ induces a short exact sequence of topological groups

\[ 1 \to \hat{G}/H \to \hat{G} \to \hat{H} \to 1. \]

*Proof.* (...)
3.1.2 Duality in local fields

Let \( F \) be an ultrametric local field. Let \( \mathcal{O} \) be its valuation ring and \( p \) the maximal ideal of \( \mathcal{O} \).

**Proposition 3.1.7.** Let \( \chi \) be a continuous character \( F \to \mathbb{C}^\times \), then \( \chi \) is a locally constant function over \( F \). Moreover \( \chi \) is unitary, i.e. \( \chi(F) \subset \mathbb{S}^1 \). Let \( \chi \) be a continuous character \( F^\times \to \mathbb{C}^\times \), then \( \chi \) is a locally constant function over \( F^\times \) (but this time \( \chi \) can be non unitary).

**Proof.** We observe that \( F \) and \( F^\times \) have “small subgroups” that is they have a basis of their neutral element made of subgroups. The local constancy of a character is then a direct consequence of the “No small subgroups” in \( \mathbb{C}^\times \).

Let \( \chi \) be a character of \( F \). By local constancy, there is an open neighborhood of 0 in \( F \) on which \( \chi \) is equal to 1, thus there exists \( n \geq 0 \) such that \( \chi(p^n) = 1 \). Then \( \chi \) can be considered as a character of \( F/p^n \). Now \( F/p^n \) is the union of the finite subgroups \( p^{-N}/p^n \) for \( N \geq 0 \). As the elements of \( \chi(p^{-N}/p^n) \) are roots of unity, all the elements of \( \chi(F) \) are roots of unity and \( \chi \) is unitary.

We give some example of characters of \( F \). We consider the case where \( F = \mathbb{Q}_p \) for a prime number \( p \). We have \( \mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p] \) and \( \mathbb{Z}_p \cap \mathbb{Z}[1/p] = \mathbb{Z} \). If \( x \in \mathbb{Q}_p \), we write \( x = u + x' \) with \( u \in \mathbb{Z}_p \) and \( x' \in \mathbb{Z}[1/p] \) and we set \( \psi_{\mathbb{Q}_p}(x) := e^{2\pi i x'} \). Then \( \psi_{\mathbb{Q}_p} \) is a group homomorphism of \( \mathbb{Q}_p \) into \( \mathbb{C}^\times \). Its kernel is exactly the subgroup \( \mathbb{Z}_p \) so it is a locally constant function on \( \mathbb{Q}_p \) and thus continuous. This is a nontrivial character of \( \mathbb{Q}_p \). More generally if \( F \) is a finite extension of \( \mathbb{Q}_p \), then \( \psi_{\mathbb{Q}_p} \circ \text{Tr}_{F/\mathbb{Q}_p} \) is a nontrivial character of \( F \).

If \( F \) is of characteristic \( p \), then \( F \) is isomorphic to the field \( k((T)) \) where \( k \) is a finite field of characteristic \( p \). We can define a nontrivial character of \( k((T)) \) by the formula

\[
\psi_{k((T))} \left( \sum_{n \gg -\infty} a_n T^n \right) = e^{\frac{2\pi i}{p} \text{Tr}_{k/F}(a_{-1})}.
\]

If \( \psi \) is a character the local field \( F \), we define its conducteur as the largest ideal \( f_\psi \) of \( F \) such that \( \psi|_{f_\psi} \) is trivial. In other words we have \( x \in f_\psi \iff \forall y \in \mathcal{O}_F, \; \psi(xy) = 1 \).

**Remark 3.1.8.** We should not confuse the conductor of a character with its kernel. The kernel contains the conductor but can be strictly bigger.

**Example 3.1.9.** The conductor of \( \psi_{\mathbb{Q}_p} \) is \( \mathbb{Z}_p \). The conductor of \( \psi_{k((T))} \) is \( k[[T]] \).

**Lemma 3.1.10.** Let \( E/F \) be a finite separable extension of ultrametric local fields. Let \( \psi \) be a nontrivial character of \( F \). Then we have

\[
\mathfrak{f}_\psi \circ \text{Tr}_{E/F} = \mathfrak{f}_\psi D_{E/F}^{-1}.
\]
Proof. Namely we have
\[ x \in f_{\psi \circ \text{Tr}_{E/F}} \iff \forall y \in \mathcal{O}_E, \quad \psi(\text{Tr}_{E/F}(yx)) = 1 \]
\[ \iff \forall z \in \mathcal{O}_F, \forall y \in \mathcal{O}_E, \quad \psi(\text{Tr}_{E/F}(zyx)) = 1 \]
\[ \iff \forall z \in \mathcal{O}_F, \forall y \in \mathcal{O}_E, \quad \psi(z \text{Tr}_{E/F}(yx)) = 1 \]
\[ \iff \forall y \in \mathcal{O}_E, \quad \text{Tr}_{E/F}(yx) \in f_{\psi} \]
\[ \iff x \in f_{\psi} D_{E/F}^{-1} \]

**Proposition 3.1.11.** Let \( F \) be a local field. Let \( \psi \) be a nontrivial unitary character of \( F \). For \( x \in F \), we note \( \psi_x \) the character of \( F \) defined by \( y \mapsto \psi(xy) \). Then the map \( x \mapsto \psi_x \) is an isomorphism of topological groups.

Proof. Assume that \( F \) is ultrametric. Let \( \pi \) be a uniformizer of \( F \). The map \( x \mapsto \psi_x \) is an injective group homomorphism. A system of neighborhoods of the unity in \( \hat{F} \) is given by the subsets \( W(\pi^n \mathcal{O}_F, B(1, \sqrt{3})) = W(\pi^n \mathcal{O}_F, \{1\}) \) where the equality comes from the “no small subgroup Lemma”. Let \( \overline{\psi} \) be the map \( x \mapsto \psi_x \). We have \( \overline{\psi}(\pi^{-n} f_{\psi}) = W(\pi^n \mathcal{O}_F, \{1\}) \cap \text{Im} \overline{\psi} \) so that \( \overline{\psi} \) is a homeomorphism onto its image. It is sufficient to check that the image of \( \overline{\psi} \) is dense in \( \hat{F} \) to conclude. By biduality Theorem, it is sufficient to check that if \( z \in F \) is such that \( \psi_x(z) = 1 \) for all \( x \in F \), then \( z = 0 \). Namely we have \( \psi(xz) = 1 \) for all \( x \in F \), for instance \( z \in \bigcap_{n \geq 1} \pi^n f_{\psi} = \{0\} \).

The cases of \( \mathbb{R} \) and \( \mathbb{C} \) are left as an exercise.

---

### 3.1.3 Dualité dans les adèles

Let \( F \) be a global field and let \( A = \mathbb{A}_F \). If \( \psi : A \to \mathbb{C}^\times \) is a character, we note \( \psi_v \) the character of \( F_v \) obtained by precomposition with the inclusion of \( F_v \) in \( A \). The continuity of \( \psi \) implies that \( \psi_v(\mathcal{O}_v) = 1 \) for almost all places \( v \) of \( F \). Conversely, if \( (\psi_v)_v \) is a family of characters, \( \psi_v \) being a character of \( F_v \) such that \( \psi_v(\mathcal{O}_v) = 1 \), we can define a character of \( A \) by the formula
\[
(x_v)_v \mapsto \prod_v \psi_v(x_v).
\]

We obtain a natural bijection between characters of \( A \) and families \( (\psi_v)_v \) such that \( \psi_v(\mathcal{O}_v) = 1 \) for almost all \( v \).

**Proposition 3.1.12.** There exists a nontrivial unitary character \( \psi : A \to S^1 \) such that \( \psi(F) = 1 \) and \( f_{\psi_v} = \mathcal{O}_v \) for almost all \( v \).

Proof. We define \( \psi \) explicitly. In a first time we construct it when \( F = \mathbb{Q} \). Let \( \psi_{\mathbb{Q}} \) be the character of \( \mathbb{A}_{\mathbb{Q}} \) corresponding to the family \( (\psi_v)_v \) where \( \psi_v = \psi_{\mathbb{Q}_p} \) if
Remark 3.1.13. Let 

\[ v = p \text{ and } \psi_{\infty} \text{ is the character of } \mathbb{R} \text{ defined by } x \mapsto e^{-2\pi i x}. \] 

We have \( f_{\psi_p} = \mathbb{Z}_p \) for all prime numbers \( p \), so that the second property is clear. Moreover, if \( \xi \in \mathbb{Q} \), we can write \( \xi \) as a finite sum \( \sum_p \xi_p + m \) with \( m \in \mathbb{Z} \) and \( \xi_p \in \mathbb{Z}[1/p] \). By the definition of \( \psi_{\mathbb{Q}} \) we have \( \psi_{\mathbb{Q}}(m) = 1 \) and, for a prime number \( p \), we have

\[ \psi_{\mathbb{Q}}(\xi_p) = \psi_{\mathbb{Q}_p}(\xi_i)\psi_{\infty}(\xi_p) = e^{2\pi i \xi_p} e^{-2\pi i \xi_p} = 1 \]

so that \( \psi_{\mathbb{Q}}(\mathbb{Q}) = 1 \).

Now we construct it when \( F = \mathbb{F}_p(T) \). We have a decomposition

\[ \mathbb{A} = \mathbb{F}_p(T) + \mathbb{F}_{\infty} \times \prod_p \mathcal{O}_{F_p} \]

where \( \infty \) is the place of \( \mathbb{F}_p(T) \) corresponding to the valuation \( v_{T-1} \). A character of \( \mathbb{A}/\mathbb{F}_p(T) \) is thus equivalent to character of \( (\mathbb{F}_{\infty} \times \prod_p \mathcal{O}_{F_p})/\mathbb{F}_p[T] \), i.e. a character of \( \mathbb{F}_{\infty} \times \prod_p \mathcal{O}_{F_p} \), which is trivial over \( \mathbb{F}_p[T] \). We can define

\[ \psi_{\mathbb{F}_p(T)}(a_\infty, (a_p)) := \psi_{\infty}(a_\infty) \]

where \( \psi_{\infty} \left( \sum_{n< \infty} a_n T_n \right) = a_{-1} \). It is clear that \( \psi_{\mathbb{F}_p(T)} \) is continuous since \( \psi_{\infty} \) is via \( \psi_{\infty}(T^{-2}F_p[[T^{-1}]])) = 1 \).

In general, there exists a finite separable extension \( F/F_0 \) with \( F_0 \) isomorphic to \( \mathbb{Q} \) or \( \mathbb{F}_p(T) \) and we can choose \( \psi = \psi_{F_0} \circ \text{Tr}_{F/F_0} \). The character \( \psi \) corresponds to a family of characters \( \psi_v \) with \( f_{\psi_v} = \mathcal{O}_v \) for almost all \( v \) since the extension \( F/F_0 \) is unramified at almost all places of \( F_0 \).

\[ \square \]

Remark 3.1.13. Let \( \psi \) be a non trivial unitary character of \( \mathbb{A}_F \) such that \( \psi(F) = 1 \). The strong approximation theorem implies that \( \psi_v \) is non trivial for all \( v \). Namely if \( \psi_v = 1 \), as \( FF_v \) is dense in \( \mathbb{A}_F \), this would imply \( \psi = 1 \).

Theorem 3.1.14. Let \( \psi : \mathbb{A}_F \to \mathbb{S}^1 \) be a unitary character of \( \mathbb{A}_F \) such that \( \psi(F) = 1 \) and \( f_{\psi_v} = \mathcal{O}_v \) for almost all \( v \). Then the map \( x \mapsto \psi_x \), with \( \psi_x(y) = \psi(xy) \) is an isomorphism of topological groups from \( \mathbb{A}_F \) onto \( \mathbb{A}_F \).

**Proof.** Let \( x = (x_v)_v \in \mathbb{A}_F \). For \( y = (y_v)_v \in \mathbb{A}_F \), we have

\[ \psi_x(y) = \prod_v \psi_{x_v}(y_v). \]

Then \( \psi_x(x_v O_v) = 1 \) for almost all \( v \) so that \( \psi_x \) is a continuous character of \( \mathbb{A}_F \). We can check that the map \( x \mapsto \psi_x \) is a continuous homomorphism from \( \mathbb{A}_F \) to \( \mathbb{A}_F \). Let’s show that it is surjective. If \( \varphi \in \mathbb{A}_F \), the character \( \varphi \) corresponds to a family \( (\varphi_v) \) of unitary characters of \( F_v \) such that \( \varphi(O_v) = 1 \) for almost all \( v \). As \( \psi_v \neq 1 \) for all \( v \), there exists \( x_v \in F_v \) such that \( \varphi_v = \psi_{x_v} \). As \( f_{\psi_v} = \mathcal{O}_v \) for almost
all \( v \), we must have \( x_v \in \mathcal{O}_v \) for almost all \( v \), that is \( x_v \in \mathcal{O}_v \) for almost all \( v \) and \( (x_v) \in \mathcal{A}_F \). This implies that \( \varphi = \psi_x \) for \( x = (x_v)_v \). Finally the map \( x \mapsto \psi_x \) is a continuous bijection homomorphism between locally compact abelian group, thus an topological isomorphism.

\[ \square \]

**Corollary 3.1.15.** Let \( \psi \) be a unitary nontrivial character of \( \mathcal{A}_F \) such \( \psi_v = \mathcal{O}_v \) for almost all \( v \). The the map \( x \mapsto \psi_x \) induces an isomorphism from \( F \) onto \( \mathcal{A}_F/\mathcal{F} \).

**Proof.** The dual group \( \mathcal{A}_F/\mathcal{F} \) is identified to \( F \). Using the identification \( \mathcal{A}_F \cong \mathcal{A}_F \), we can see \( F \) as a discrete subgroup of \( \mathcal{A}_F \). Since \( \psi(F) = 1 \), we have \( F \subset F \). Moreover it is easy to check that \( F \) is an \( F \)-vector subspace of \( \mathcal{A}_F \). The quotient \( F/F \) is therefore a discrete subgroup of the compact group \( \mathcal{A}_F/\mathcal{F} \) and so is a finite group. As \( F/F \) is moreover an \( F \)-vector space and \( F \) is infinite, we must have \( F = F \).

\[ \square \]

**Corollary 3.1.16.** Let \( \psi \) be a unitary nontrivial character of \( \mathcal{A}_F \) such that \( \psi(F) = 1 \). Then \( f \psi_v = \mathcal{O}_v \) for almost all \( v \).

### 3.1.4 Fourier transform

Let \( G \) be a locally compact abelian group and let \( dg \) be a Haar measure on \( G \). For \( f \in L^1(G) \), the Fourier transform of \( f \) is the function \( \hat{f} \) on \( \widehat{G} \) defined by

\[
\forall \hat{g} \in \widehat{G}, \quad \hat{f}(\hat{g}) := \int_G f(g) \hat{g}(g)^{-1} \, dg.
\]

We have the Fourier inverse theorem.

**Theorem 3.1.17** (Inversion Theorem). There exists a unique Haar measure \( d\hat{g} \) on \( \widehat{G} \) such that for all \( f \in L^1(G) \) such that \( \hat{f} \in L^1(\widehat{G}) \) we have

\[
\forall g \in G, \quad f(g) = \int_{\widehat{G}} \hat{f}(\hat{g}) \hat{g}(g) \, d\hat{g}.
\]

The measure \( d\hat{g} \) is called the dual measure of \( dg \).

**Remark 3.1.18.** The theorem can also be written \( \hat{\hat{f}} = \hat{f} \) where \( \hat{f}(g) := f(g^{-1}) \).

Assume that \( G \) is isomorphic to its dual \( \widehat{G} \) and fix such an isomorphism. For example, if \( G = F \) with \( F \) a local field, this is equivalent to fix a nontrivial unitary character of \( F \). In this case, we can use this isomorphism to consider the Fourier transform \( \hat{f} \) of a function \( f \) as a function over \( G \) and the measure \( d\hat{g} \) as a Haar measure over \( G \). If \( c \in \mathbb{R}_{>0} \), we can easily check that the dual measure of \( cdg \) is \( c^{-1} d\hat{g} \). Therefore there exists a unique Haar measure \( dg \) on \( G \) which is autodual, i.e. \( d\hat{g} = dg \). We call it the autodual measure. Note that the autodual measure depends on the chosen isomorphism between \( G \) and \( \widehat{G} \).
3.1.5 Fourier transform on a local field

Let $F$ be a local field. Let’s assume in a first time that $F$ is ultrametric. Let $\mathcal{O}_F$ be its valuation ring, $p_F$ the maximal ideal of $\mathcal{O}_F$, $\pi_F$ a uniformizer of $F$ and $q_F$ the cardinal of the residue field $\mathcal{O}_F/p_F$. Let $\psi$ be a nontrivial character of $F$. The choice of $\psi$ gives us an isomorphism $F \simeq \hat{F}$. Let $f_\psi$ be the conductor of $\psi$ and let $d \in \mathbb{Z}$ be such that $f_\psi = p_F^d (\pi_F^d)$ (where $\pi_F$ is a uniformizer of $F$). Let $dx$ be the unique Haar measure on $F$ such that $\text{Vol}(\mathcal{O}_F) = \int_{\mathcal{O}_F} dx = q_F^d$. We will check that $dx$ is the autodual measure over $F$ (with respect to $\psi$). The Fourier transform of a function $f$ over $G$ is the function $\hat{f}$ over $G$ defined by

$$\hat{f}(y) = \int_G f(x) \psi(xy) \, dx.$$ 

We will be more interested in some special functions over $F$. Let $S(F)$ be the $\mathbb{C}$-vector space of locally constant functions with compact support over $F$. This space is called the Schwartz-Bruhat space.

**Theorem 3.1.19.** Let $f \in S(F)$. Then $\hat{f} \in S(F)$ and $\hat{\hat{f}} = f$.

**Proof.** A function $f \in S(F)$ is a finite $\mathbb{C}$-linear combination of functions of the form $\mathbbm{1}_{a+p_F^n}$ for $a \in F$ and $n \in \mathbb{Z}$. Therefore it is sufficient to check the particular case $f = \mathbbm{1}_{a+p_F^n}$. A direct computation shows that

$$\mathbbm{1}_{a+p_F^n} \hat{f}(y) = q_F^{-n} \psi(-ay) \mathbbm{1}_{p_F^{-n}a}^F(y).$$

The result follows. □

**Example 3.1.20.** If $F$ is a finite extension of $\mathbb{Q}_p$ and $\psi = \psi_{\mathbb{Q}_p} \circ \text{Tr}_{F/\mathbb{Q}_p}$, then $f_\psi = D_{F/\mathbb{Q}_p}^{-1}$. For this choice of character, the autodual measure over $F$ is $q_F^{-\frac{m}{2}} dx$ where $dx$ is the normalized Haar measure and $D_{F/\mathbb{Q}_p} = p^m$, with $m \in \mathbb{N}$.

**Exercice 3.1.1.** We consider the case where $F = \mathbb{R}$. Define a nontrivial unitary character of $\mathbb{R}$ by $\psi_{\mathbb{R}}(x) := e^{-2\pi i x}$. Check that the autodual measure over $\mathbb{R}$ is the Lebesgue measure $dx$ (such that $\int_0^1 dx = 1$). Moreover let $S(\mathbb{R})$ be the Schwartz space of infinitely derivable functions $f : \mathbb{R} \to \mathbb{C}$ such that for all $(m,n) \in \mathbb{N}^2$

$$\lim_{|x| \to +\infty} |x|^m |f^{(n)}(x)| = 0.$$ 

Check that $f \in S(\mathbb{R})$ implies $\hat{f} \in S(\mathbb{R})$ and that $\hat{\hat{f}} = f$. 

Exercice 3.1.2. We consider the case where $F = \mathbb{C}$. Define a nontrivial unitary character of $\mathbb{C}$ by $\psi_C(z) := \psi_R(\text{Tr}_{\mathbb{C}/\mathbb{R}}(z)) = e^{-4\pi i \text{Re}(z)}$. Check that the autodual measure over $\mathbb{C}$ is the measure $2 \, dx \, dy$ (such that the measure of $[0, 1]^2$ is 2). Moreover let $\mathcal{S}(\mathbb{C})$ be the Schwartz space of $\mathbb{C}^\infty$ functions $f : \mathbb{C} \simeq \mathbb{R}^2 \to \mathbb{C}$ such that for all $(p, q, n) \in \mathbb{N}^3$

$$\lim_{|z| \to +\infty} |z|^{|n|} \left| \frac{\partial^p+q f}{\partial x^p \partial y^q}(z) \right| = 0.$$ 

Check that $f \in \mathcal{S}(\mathbb{C})$ implies $\hat{f} \in \mathcal{S}(\mathbb{C})$ and that $\hat{\hat{f}} = \check{f}$.

3.1.6 Fourier transform on adeles

Let $\psi$ be a nontrivial unitary character of $\mathbb{A}_F$ such that $\psi(F) = 1$. We know that $f_{\psi_v} = O_v$ for almost all $v$. Let $\mathbb{A}_f$ be the ring of finite adeles, i.e. the restricted tensor product of the $F_v$ for $v$ ultrametric place, with respect to the $O_v$. We define the space of Schwartz-Bruhat functions over $\mathbb{A}_F$ as

$$\mathcal{S}(\mathbb{A}_F) := \mathcal{S}(F_\infty) \otimes_{\mathbb{C}} \mathcal{S}(\mathbb{A}_f)$$

where $\mathcal{S}(F_\infty) := \bigotimes_{v | \infty} \mathcal{S}(F_v)$ and $\mathcal{S}(\mathbb{A}_f)$ is the space of locally constant functions with compact support on $\mathbb{A}_f$. Any element of $\mathcal{S}(\mathbb{A}_F)$ is a finite sum of functions of the form $\bigotimes_{v \in S} f_v \otimes 1 \prod_{v \not\in S} O_v$ where $S$ is a finite set of places containing $\Sigma_\infty$ and $f_v \in \mathcal{S}(F_v)$.

Note that, as $f_{\psi_v} = O_v$ for almost all $v$, the autodual measure on $F_v$ with respect to $\psi_v$ is such that $\int_{O_v} dx_v = 1$. Let $dx$ be the measure on $\mathbb{A}_F$ defined as the product of the autodual measure over the $F_v$ with respect to the $\psi_v$.

Proposition 3.1.21. If $f \in \mathcal{S}(\mathbb{A}_F)$, then $\hat{f} \in \mathcal{S}(\mathbb{A}_F)$ and $\hat{\hat{f}} = \check{f}$.

Proof. By linearity, it is sufficient to check the result for a function $f$ of the form $\bigotimes_{v \in S} f_v \otimes 1 \prod_{v \not\in S} O_v$. We can enlarge $S$ so that $S$ contains all the places $v$ for which $f_{\psi_v} \neq O_v$. Then we have

$$\hat{f}(y) = \int_{\mathbb{A}_F} f(x) \psi(-xy) \, dx = \prod_{v \in S} \int_{F_v} f_v(x) \psi_v(-x_v y_v) \, dx_v \prod_{v \not\in S} \int_{O_v} dx_v = \prod_{v \in S} \hat{f}_v(y_v).$$

We deduce that $\hat{f} \in \mathcal{S}(\mathbb{A}_F)$ and the desired formula. \qed

Proposition 3.1.21 shows in particular that the measure $dx$ is autodual with respect to the character $\psi$. Moreover by Theorem 3.1.14 any other unitary character $\psi$ of $\mathbb{A}_F$ satisfying $\psi(F)$ is of the form $\psi(\xi - )$ for some $\xi$. The product formula
shows that the autodual measure on $A_F$ with respect to $\psi(\xi-)$ is $dx$. Therefore this measure doesn’t depend on the choice of the character $\psi$. The quotient of this autodual measure on $A_F$ by the counting measure on $F$ is a measure on $A_F/F$ called the Tamagawa measure on $A_F$.

**Proposition 3.1.22.** For the Tamagawa measure, the volume of $A_F/F$ is equal to one.

**Proof.** We do only the case of number fields. Let $dx = \prod_v dx_v$ be the measure over $A_F$ such that $dx_v$ is the normalized measure for all $v$. We have already proved that, for the quotient of $dx$ by the counting measure over $F$, we have $\int_{A_F/F} dx = |\Delta_F/Q|^{\frac{1}{2}}$ where $\Delta_F/Q$ is the discriminant of $O_F$ over $\mathbb{Z}$. Let $\psi$ be a nontrivial unitary character of $A_F$. As the autodual measure over $A_F$ does not depend on the choice of the character, we can choose it of the form $\psi_Q \circ \text{Tr}_{F/Q}$.

Then $f_{\psi_v} = D_{F_v/Q_v}^{-1}$ for all $v$ ultrametric (and $p = v|Q$) whereas $dx_v$ is already autodual if $v \mid \infty$. Thus the autodual measure over $A_F$ is $c dx$ where $c = \prod_{v|\infty} c_v$ with $c_v = |\pi_v|^{-\frac{d_v}{2}}$ where $D_{F_v/Q_v}^{-1} = (\pi_v^{d_v})$. By the product formula we have

$$\prod_v c_v = \prod_v |\pi_v|^{-\frac{d_v}{2}} = \prod_p \prod_{v|p} |N_{F_v/Q_v}(\pi_v)|^{-\frac{d_v}{2}} = \prod_p |\Delta_{F/Q}|^{-\frac{1}{2}} = |\Delta_{F/Q}|^{-\frac{1}{2}}.$$

This gives us the result. 

\[\square\]

### 3.2 Local zeta functions

#### 3.2.1 Multiplicative characters

Let $F$ be a local ultrametric field. A **character** of $F^\times$ is a continuous group homomorphism $\omega : F^\times \to \mathbb{C}^\times$. A character is said to be **unramified** is $\omega(O_F^\times) = 1$. In this case it is determined by its value on a uniformizer $\pi_F$ of $F$ and is of the form $|\cdot|_F^s$ for some complex number $s \in \mathbb{C}$. More generally a character $\omega$ of $F^\times$ can be written as $\omega_0|\cdot|_F^s$ where $\omega_0$ is unitary and $s \in \mathbb{C}$. Note that such a decomposition is not unique. We say that two characters $|\cdot|_1$ and $|\cdot|_2$ are **equivalent** if there exists $s \in \mathbb{C}$ such that $|\cdot|_2 = |\cdot|_1^{-1} = |\cdot|^{-s}$. The equivalence class of a character is in bijection with $\mathbb{C}/\mathbb{Z}_{\log q_F} \simeq \mathbb{C}^\times$ and can be considered as a Riemann surface. This allows us to speak about holomorphy or meromorphy of a complex function defined over the set of all characters.

If $\omega$ is a character of $F^\times$, we set $\sigma(\omega) := \text{Re}(s)$ where $\omega = \omega_0|\cdot|_F^s$ with $\omega_0$ unitary. This definition does not depend on the choice of the decomposition. Namely if $\omega_0|\cdot|_F^s = \omega'_0|\cdot|_F^{s'}$, then $s - s' \in i\mathbb{R}$. 
From now we fix \( \psi \) a nontrivial character of \( F \) and let \( dx \) be the autodual measure over \( F \) with respect to \( \psi \). We also fix \( d^x x \) a Haar measure over \( F^\times \) (the choice of \( d^x x \) will have no consequence in what follows).

If \( f \in S(F) \) and \( \omega \) is a character of \( F^\times \), the zeta integral associated to \( f \) and \( \omega \) is the number
\[
Z(f, \omega) := \int_{F^\times} f(x)\omega(x) \, d^x x
\]
(when it exists).

**Lemma 3.2.1.** The integral \( Z(f, \omega) \) converges absolutely for \( \sigma(\omega) > 0 \).

**Proof.** We can write \( f = f(0)1_{\mathcal{O}_F} + g \) with \( g \) locally constant with compact support in \( F^\times \). The integral \( \int_{F^\times} g(x)\omega(x) \, d^x x \) converges absolutely for any \( \omega \). Moreover, if \( \sigma := \sigma(\omega) > 0 \),
\[
\int_{F^\times} |1_{\mathcal{O}_F}(x)\omega(x)| \, dx = \int_{\mathcal{O}_F} |x|^\sigma \, d^x x = \sum_{n=0}^{\infty} \int_{\pi_F^n\mathcal{O}_F} |x|^\sigma \, d^x x
\]
\[
= \sum_{n=0}^{\infty} q_F^{-n\sigma} \text{Vol}(O_F^\times) = \text{Vol}(O_F^\times) \frac{1}{1 - q_F^{-\sigma}}. \quad \Box
\]

**Remark 3.2.2.** The proof of the previous lemma shows that, for any \( s \in \mathbb{C} \) with \( \text{Re } s > 0 \), we have
\[
Z(1_{\mathcal{O}_F}, |\cdot|^s_F) = \text{Vol}(O_F^\times) \frac{1}{1 - q_F^{-s}}.
\]

### 3.2.2 Functional equation

Let \( f \in S(F) \). By remark 3.2.2, we have, for \( \text{Re } s > 0 \),
\[
Z(f, |\cdot|^s) = f(0) \text{Vol}(O_F^\times) \frac{1}{1 - q_F^{-s}} + Z(g, |\cdot|^s)
\]
where \( g = f - f(0)1_{\mathcal{O}_F} \). As \( g \) is a function with compact support in \( F^\times \), the integral \( Z(g, |\cdot|^s) \) converges absolutely for any value of \( s \in \mathbb{C} \) and the map \( s \mapsto Z(g, |\cdot|^s) \) is holomorphic on \( \mathbb{C} \). Therefore we have proved that the map \( s \mapsto Z(f, |\cdot|^s) \) can be (uniquely) extended to a meromorphic function over \( \mathbb{C} \).

Let’s consider now the ramified case. Let \( \omega_0 \) be a unitary character of \( F^\times \) and assume that \( \omega_0 \) is ramified, this is equivalent to ask that \( \omega_0 \) is not of the form \( |\cdot|^t \) with \( t \in \mathbb{R} \). We define the conductor of \( \omega_0 \) as the largest ideal \( \mathfrak{p} \) in \( c\mathcal{O}_F \) such that \( \omega_0 \) is trivial on \( 1 + \mathfrak{p} \). The conductor is of the form \( \mathfrak{p}_F^m = (\pi_F^m)^c \) for some \( m \geq 1 \).
Note that, as \( \omega_0 \) is ramified, the restriction of \( \omega_0 \) to \( \mathcal{O}_F^\times \) is non trivial. A standard argument implies that
\[
\int_{\mathcal{O}_F^\times} \omega_0(x) \, d^\times x = 0.
\]
We conclude that, for any \( n \geq 0 \), we have
\[
\int_{\pi^n \mathcal{O}_F^\times} \omega_0(x) \, d^\times x = 0.
\]
Let \( f \in \mathcal{S} \) and let \( n \geq 1 \) such that \( f \) is constant on \( \pi^n \mathcal{O}_F \). For \( s \in \mathbb{C} \) such that \( \text{Re } s > 0 \), we have
\[
\int_{\pi^n \mathcal{O}_F^\times \setminus \{0\}} f(x) \omega_0(x) |x|^s \, d^\times x = \sum_{k \geq n} \int_{\pi^k \mathcal{O}_F^\times} f(x) \omega_0(x) |x|^s \, d^\times x = 0.
\]
We have prove that
\[
Z(f, \omega_0 |\cdot|^s) = \int_{F \setminus \pi^n \mathcal{O}_F} \omega_0(x) |x|^s \, d^\times x
\]
for any \( s \in \mathbb{C} \) with \( \text{Re } s > 0 \). However the latter integral converges absolutely for any \( s \in \mathbb{C} \) and gives rise to a holomorphic function over \( \mathbb{C} \). Therefore we have proved that the function \( s \mapsto Z(f, \omega_0 |\cdot|^s) \) extends to a holomorphic function over \( \mathbb{C} \).

To conclude we have proved that the function \( \omega \mapsto Z(f, \omega) \) has a unique extension to a meromorphic function in \( \omega \). This meromorphic extension is holomorphic on equivalence classes of unramified characters. We will now check that this meromorphic extension satisfies a functional equation.

If \( \omega \) is a character of \( F^\times \), we define \( \tilde{\omega} := |\cdot| \omega^{-1} \). If we write \( \omega = \omega_0 |\cdot|^s \) with \( \omega_0 \) unitary, then \( \tilde{\omega} = \omega_0^{-1} |\cdot|^{1-s} = \overline{\omega_0} |\cdot|^{1-s} \).

**Proposition 3.2.3.** Let \( \omega \) be a character of \( F^\times \) with \( 0 < \sigma(\omega) < 1 \). Let \( f \) and \( g \) be two elements of \( \mathcal{S}(F) \). Then we have
\[
Z(f, \omega)Z(\hat{g}, \tilde{\omega}) = Z(g, \omega)Z(\hat{f}, \tilde{\omega}).
\]

**Proof.** We have to prove that the quantity \( Z(f, \omega)Z(\hat{g}, \tilde{\omega}) \) doesn’t change when we
exchange $f$ and $g$.

$$Z(f, \omega)Z(\hat{g}, \tilde{\omega}) = \int \int_{F^\times \times F^\times} f(x)\hat{g}(y)|y|\omega(xy^{-1})d^x x d^x y$$

$$= \int \int_{F^\times \times F^\times} f(yz)\hat{g}(y)|y|\omega(z) d^x y d^x z$$

$$= \int_{F^\times} \omega(z) \left( \int_{F^\times} f(yz)\hat{g}(y)|y|d^x y \right) d^x z$$

$$= \int_{F^\times} \omega(z) \int_{F^\times} f(yz)|y| \int_{F^\times} g(u)\psi(-uy) du d^x y d^x z$$

$$= \int_{F^\times} \int_{F^\times} \int_{F^\times} f(v)\psi(vz^{-1})|g(u)\psi(-uvz^{-1}) du d^x y d^x z$$

$$= \int_{F^\times} \int_{F^\times} \int_{F^\times} f(v)g(u)\psi(-uvz^{-1}) du d^x v d^x z$$

$$= C \int_{F^\times} \int_{F^\times} f(v)g(u)\psi(-uvz^{-1}) du d^x v d^x z$$

As $|v|d^x v$ is, up to nonzero factor $C > 0$, the Haar measure $dv$ on $F$, we see that the quantity is symmetric in $f$ and $g$. 

Eventually we have proved the following result.

**Theorem 3.2.4 (Tate).** For all $f \in S(F)$, the function $\omega \mapsto Z(f, \omega)$ has a meromorphic extension to the space of all characters of $F^\times$. Moreover there exists an invertible meromorphic function $\omega \mapsto \gamma(\psi, \omega)$ such that

$$Z(f, \omega) = \gamma(\psi, \omega)Z(\hat{f}, \tilde{\omega})$$

for all $\omega$.

**Proof.** It is sufficient to prove that for any unitary character $\omega_0$ of $F^\times$, there exists a function $g \in S(F)$ such that $Z(\hat{g}, \omega_0^{-1}|.|^{1-s})$ and $Z(g, \omega_0|.|^s)$ are meromorphic in $s \in \mathbb{C}$ and nonzero. Namely we will have $\gamma(\psi, \omega_0|.|^s) = \frac{Z(\hat{g}, \omega_0^{-1}|.|^{1-s})}{Z(g, \omega_0|.|^s)}$. Note that it is sufficient to find $g$ such that the function $s \mapsto Z(\hat{g}, \omega_0^{-1}|.|^{1-s})$ is nonzero. Namely if $Z(g, \omega_0|.|^s)$ where zero, we would have

$$Z(\hat{g}, \omega_0^{-1}|.|^{1-s})Z(\hat{g}, \omega_0|.|^s) = Z(g, \omega_0^{-1}|.|^{1-s})Z(\hat{g}, \omega_0|.|^s) = \omega_0(-1)Z(g, \omega_0|.|^{1-s})Z(\omega_0|.|^{1-s})$$

and so would be $s \mapsto Z(\hat{g}, \omega_0^{-1}|.|^{1-s})$.

In order to do this, we consider separately the cases where $\omega_0$ is unramified and where $\omega_0$ is ramified.
3.2. LOCAL ZETA FUNCTIONS

Assume that $\omega_0$ is unramified, we can suppose then that $\omega_0 = 1$. We can choose $g$ such that $\hat{g} = 1_{O_F}$. Namely we have already computed that

$$Z(1_{O_F}, |·|^{1-s}) = \frac{1}{1 - q_F^{-1}}$$

which is nonzero.

Assume that $\omega_0$ is ramified and choose $g$ such that $\hat{g} = 1 + p^m_F$ where $p^m_F$ is the conductor of $\omega_0$ (and of $\omega_0^{-1}$). Then we have

$$Z(\hat{g}, \omega_0^{-1}|·|^{1-s}) = \text{Vol}(1 + p^m_F) \neq 0.$$ 

If $\omega$ is a character of $F^\times$, we define its local $L$-function by the following formula

$$L(\omega) := \begin{cases} \frac{1}{1 - q_F^{-1}} & \text{if } \omega \text{ is unramified} \\ 1 & \text{if } \omega \text{ is ramified.} \end{cases}$$

We have checked that, for any $f \in S$, the function $\omega \mapsto L(\omega)^{-1}Z(f, \omega)$ is holomorphic in $\omega$. In other words, for any unitary character $\omega_0$ of $F^\times$, the function $s \mapsto L(\omega_0|·|^s)^{-1}Z(f, \omega_0|·|^s)$ is holomorphic in $s$.

We define the epsilon factor of $\omega$ as

$$\varepsilon(\psi, \omega) := \gamma(s, \omega) \frac{L(\tilde{\omega})}{L(\omega)}.$$ 

The local functional equation can also be written as

$$\forall f \in S(F), \ \forall \omega, \ \frac{Z(f, \omega)}{L(\omega)} = \varepsilon(\psi, \omega) \frac{Z(\hat{f}, \tilde{\omega})}{L(\tilde{\omega})}.$$ 

Moreover the function $\omega \mapsto \varepsilon(\psi, \omega)$ is holomorphic and invertible.

**Proposition 3.2.5.** Let $\omega$ be a character of $F^\times$, we have the following formulas.

(i) $\gamma(\psi, \omega)\gamma(\psi, \tilde{\omega}) = \omega(-1)$.

(ii) $\gamma(\psi, \tilde{\omega}) = \omega(-1)\gamma(\psi, \omega)$.

(iii) If $\sigma(\omega) = \frac{1}{2}$, then $|\gamma(\psi, \omega)| = 1$.

**Proof.** Exercise with the functional equation. 

\qed
Remark 3.2.6. The $\gamma$ and $\varepsilon$ can be computed explicitly. Let $(\pi_F^d)$ be the character of $\psi$. We have

$$\varepsilon(\psi, \cdot|s) = q_F^{d(\frac{1}{2} - s)}$$

and, if $\omega_0$ is a ramified unitary character of conductor $p_F^m$,

$$\varepsilon(\psi, \omega_0 \cdot|s) = q_F^{(d - m)(\frac{1}{2} - s) - \frac{m}{2}} G(\psi, \omega_0)$$

where $G(\psi, \omega_0)$ is the “Gauss sum”

$$G(\psi, \omega_0) = \sum_{a \in (O_F / p_F^m)^*} \omega_0(a) \psi(\pi^{-m - d} a).$$

From Proposition 3.2.5 we deduce that $|G(\psi, \omega_0)| = q_F^{\frac{n}{2}}$. When $n = 1$, we recover the classical result concerning Gauss sums of the finite field $k_F$.

### 3.2.3 Archimedean local fields

The statement of Theorem 3.2.4 stays true if we replace $F$ by $\mathbb{R}$ or $\mathbb{C}$. We give here the results and leave the computations behind their proof in exercise.

If $F = \mathbb{R}$, we set

$$L(|\cdot|^s) := \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right), \quad L(\text{sgn}|\cdot|^s) := L(|\cdot|^{s+1}).$$

Then we have

$$\varepsilon(\psi_\mathbb{R}, \cdot|s) = 1, \quad \varepsilon(\psi_\mathbb{R}, \text{sgn}|\cdot|^s) = -i$$

(we recall that $\psi_\mathbb{R}$ is the character $x \mapsto e^{-2\pi ix}$.

If $F = \mathbb{C}$ and $n \in \mathbb{Z}$, we define $\theta_n$ by $z \mapsto (z \bar{z}^{-1})^\frac{n}{2}$. This is a unitary character of $\mathbb{C}^\times$ and every character of $\mathbb{C}^\times$ is equivalent to $\theta_n$ for a unique $n \in \mathbb{Z}$. We set

$$L(\theta_n|_{\mathbb{C}}|s) := (2\pi)^{1-s+\frac{|n|}{2}} \Gamma\left(s + \frac{|n|}{2}\right).$$

Then we have

$$\varepsilon(\psi_\mathbb{C}, \theta_n|_{\mathbb{C}}|s) = i^{-|n|}.$$  

We recall that $\psi_\mathbb{C}$ is the character $\psi_\mathbb{R} \circ \text{Tr}_{\mathbb{C}/\mathbb{R}}$ of $\mathbb{C}$ and that $|\cdot|_{\mathbb{C}} = |\cdot|_R \circ N_{\mathbb{C}/\mathbb{R}} = |\cdot|^2$. 

3.3 Global zeta functions

3.3.1 Poisson formula

**Lemma 3.3.1.** Let $V$ be a finite dimensional real vector space. Let $\Lambda \subset V$ be a lattice. Let $f \in \mathcal{S}(V)$ be a Schwartz function. Then the series

$$\sum_{\lambda \in \Lambda} f(\omega(x + \lambda)), \quad (\omega, x) \in \Omega \times K$$

is uniformly convergent on each compact subset $\Omega \times K \subset \text{GL}(V) \times V$.

**Lemma 3.3.2.** Let $f \in \mathcal{S}(\mathbb{A}_F)$. Then the series

$$\sum_{\xi \in F} f(a(x + \xi)), \quad (a, x) \in \Omega \times K$$

is uniformly convergent on each compact subset $\Omega \times K \subset I_F \times \mathbb{A}_F$.

**Theorem 3.3.3** (Poisson formula). Let $f \in \mathcal{S}(\mathbb{A}_F)$. Then we have

(i) $\sum_{\xi \in F} f(\xi) = \sum_{\xi \in \hat{F}} \hat{f}(\xi)$.

(ii) for all $a \in I_F$, $|a| \sum_{\xi \in F} f(a\xi) = \sum_{\xi \in \hat{F}} \hat{f}(a^{-1}\xi)$.

**Proof.** The second formula can be easily deduced from the first formula applied to the function $x \mapsto f(ax)$. We prove only the first formula. As $\sum_{\xi} f(x + \xi)$ is uniformly convergent on each compact subset of $\mathbb{A}_F$, the function $x \mapsto g(x) := \sum_{\xi \in F} f(x + u) \psi(-\xi x)$ is continuous on $\mathbb{A}_F/F$. As $\mathbb{A}_F/F$ is compact, this is a $L^1$-function.

Let’s compute its Fourier coefficients: we identify $\mathbb{A}_F/F$ with $F$ according to $\xi \mapsto \psi(-\xi)$. Let $D \subset \mathbb{A}_F$ be a compact fundamental domain for $\mathbb{A}_F/F$. For $\xi \in F$, we have

$$\hat{g}(\xi) = \int_{\mathbb{A}_F/F} g(x) \psi(-\xi x) \, dx = \int_{\mathbb{A}_F/F} \sum_{u \in F} f(x + u) \psi(-\xi x) \, dx$$

$$= \sum_{u \in F} \int_{D} f(x + u) \psi(-\xi x) \, dx = \sum_{u \in D} \int_{D} f(x + u) \psi(-\xi x) \, dx$$

$$= \sum_{u \in F} \int_{D+u} f(x) \psi(-\xi x) \, dx = \int_{\mathbb{A}_F} f(x) \psi(-\xi x) \, dx$$

$$= \hat{f}(\xi).$$
As \( \hat{f} \in S(\mathbb{A}_F) \), the series \( \sum_{\xi \in F} \hat{g}(\xi) \) is absolutely convergent and by the Fourier inversion formula we have

\[
\forall x \in \mathbb{A}_F/F, \quad g(x) = \sum_{\xi \in F} \hat{f}(\xi) \psi(\xi x).
\]

We obtain the desired formula after evaluation at \( x = 0 \).

3.3.2 Integrals on \( I_F \)

Let \( (x_v)_{v \in \Sigma} \) be a family of non-zero complex numbers indexed by a countable set \( \Sigma \). We say that the product \( \prod_{v \in \Sigma} x_v \) is absolutely convergent if the series \( \sum_{v \in \Sigma} |x_v - 1| \) is convergent. In this case the infinite product \( \prod_{v \in \Sigma} x_v \) makes sense as an element of \( \mathbb{C}^\times \). Moreover \( |x_v - 1| < 1 \) for any \( v \), we have

\[
\log \left( \prod_{v \in \Sigma} x_v \right) = \sum_{v \in \Sigma} \log(x_v).
\]

For each place \( v \) of \( F \) we fix a Haar measure \( d_{x_v} \) on \( F_v^\times \) so that \( \int_{F_v^\times} d_{x_v} = 1 \) for almost all \( v \). Let \( d^\times x \) be the product measure on \( I_F \).

**Lemma 3.3.4.** For each \( v \in \Sigma_F \) let \( f_v \) be a continuous and integrable function over \( F_v^\times \) so that \( \int_{F_v^\times} d^\times x_v = 1 \) for almost all \( v \). Let \( d^\times x \) be the product measure on \( I_F \) and

\[
\int_{I_F} f(x) d^\times x = \prod_v \int_{F_v^\times} f_v(x_v) d^\times x_v.
\]

3.3.3 Hecke characters, global zeta functions

A Hecke character is a continuous group homomorphism \( \chi : I_F/F^\times \to \mathbb{C}^\times \). If \( \chi \) is a Hecke character, for any place \( v \) of \( F \), the precomposition of \( \chi \) with the inclusion \( F_v^\times \hookrightarrow I_F \) gives rise to a character \( \chi_v \) of \( F_v^\times \). From the continuity of \( \chi \) we deduce that \( \chi_v \) is unramified for almost all \( v \). Conversely if \( (\chi_v)_{v \in \Sigma} \) is a family of characters of \( F_v^\times \) such that almost all of them are unramified. We can define a character of \( I_F \) by the formula

\[
\chi((x_v)_{v \in \Sigma}) := \prod_{v \in \Sigma_F} \chi_v(x_v).
\]

However this character is a Hecke character only if \( \chi(F^\times) = 1 \).
Proposition 3.3.5. Let $\chi$ be a Hecke character. Then there exists $\sigma_\chi \in \mathbb{R}$ such that
\[
\forall x \in I_F, \quad |\chi(x)| = |x|^{\sigma_\chi}.
\]
Proof. This is a direct consequence of the compacity of $I_F/\mathbb{F}^\times$. Namely $\chi(I_F/\mathbb{F}^\times) \subset S^4$ so that $|\chi|$ can be factored through the idele norm.

A consequence of this proposition is that if $\chi$ is a Hecke character of local components $\chi_v$, the real number $\sigma_{\chi_v}$ does not depend on $v$.

Now we fix a Haar measure $d^\times x$ on $I_F$. If $f \in \mathcal{S}(\mathbb{A}_F)$ and $\chi$ is a Hecke character, we define the global zeta integral $Z(f, \chi)$ by the formula
\[
Z(f, \chi) := \int_{I_F} f(x)\chi(x) \, d^\times x.
\]

Proposition 3.3.6. If $\sigma_\chi > 1$, the integral $Z(f, \chi)$ is absolutely convergent.
Proof. We can assume that $f$ has the form $\bigotimes_v f_v$ with $f_v \in \mathcal{S}(F_v)$ and $f_v = 1_{\mathcal{O}_v}$ for all $v \notin S$ where $S$ is a finite set of places of $F$. We can assume $S$ big enough so that $\chi_v$ is unramified for $v \notin S$. For all $v$, the local integral $\int_{F_v} f_v(x)\chi_v(x) \, d^\times x_v$ is absolutely convergent since $\sigma_{\chi_v} = \sigma_\chi > 1 > 0$. It is therefore sufficient to check the absolute convergence of the product
\[
\prod_{v \notin S} \int_{F_v} |f_v(x_v)\chi_v(x_v)| \, d^\times x_v = \prod_{v \notin S} \int_{\mathcal{O}_v} |\chi_v(x_v)| \, d^\times x_v.
\]
As $\chi_v$ is unramified for $v \notin S$, we have $|\chi_v| = |\|_v^{\sigma_\chi}$ and $\int_{\mathcal{O}_v} |\chi_v(x_v)| \, d^\times x_v = \frac{1}{1-q_v^{-\sigma_\chi}}$. The result follows from the following lemma.

Lemma 3.3.7. The product $\prod_{v \notin S} \frac{1}{1-q_v^{-\sigma}}$ is absolutely convergent when $\sigma > 1$.
Proof. If $F = \mathbb{Q}$, we have $\frac{1}{1-p^{-\sigma}} - 1 = p^{-\sigma} < 2p^{-\sigma}$ and we know that $\sum_p p^{-\sigma} < +\infty$ if $\sigma > 1$. If $F$ is a finite extension of $\mathbb{Q}$, we have for any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_F$, $\frac{1}{1-N_{F/\mathbb{Q}}p^{-\sigma}} - 1 \leq 2Np^{-\sigma}$ and $|\{\mathfrak{p} \mid p\}| \leq [F : \mathbb{Q}]$ for any prime number $p$. Therefore $\sum_p Np^{-\sigma} \leq [F : \mathbb{Q}] \sum_p p^{-\sigma} < +\infty$ if $\sigma > 1$ and we are done. The case of function fields is left as an exercise.

The absolute convergence of the zeta integrals for $\sigma_\chi > 1$ shows that the function $\chi \mapsto Z(f, \chi)$ is holomorphic on the domain of Hecke characters such that $\sigma_\chi > 1$. More precisely, if $\chi_0$ is a unitary Hecke character, the function $s \mapsto Z(f, \chi_0|s|)$ is well defined and holomorphic on the set $\{s \in \mathbb{C} \mid \text{Re}(s) > 1\}$. 
Theorem 3.3.8.  
(1) The function \( \chi \mapsto Z(f, \chi) \) has a meromorphic extension to the domain of all Hecke characters and satisfies the functional equation

\[
Z(f, \chi) = Z(\hat{f}, \tilde{\chi})
\]

where \( \tilde{\chi} := |\cdot| \chi^{-1} \) and the Fourier transform \( \hat{f} \) is understood for the autodual measure on \( \mathbb{A}_F \).

(2) If \( \chi_0 \) is a Hecke character not of the form \( |\cdot|^{s_0} \) for some \( s_0 \in \mathbb{C} \), then the meromorphic function \( s \mapsto Z(f, \chi_0 |\cdot|^s) \) is holomorphic.

(3) The function \( s \mapsto Z(f, |\cdot|^s) \) is holomorphic over \( \mathbb{C} \setminus \{0, 1\} \). Moreover it has at most simple poles in 0 and 1 of respective residues \( -\kappa f(0) \) and \( \kappa \hat{f}(0) \) where \( \kappa := \int_{I_{p/F}^\times} d^\times x \).

3.3.4 L’equation fonctionnelle globale

Let \( \chi \) be a unitary Hecke character. We define its \( L \)-function by the formula

\[
L(\chi, s) = \prod_{v \mid \infty} L(\chi_v |\cdot|^s_v).
\]

We easily check (as before) that this product is absolutely convergent for \( \Re s > 1 \) and gives rise to an holomorphic function on \( \{ s \in \mathbb{C} \mid \Re s > 1 \} \).

Remark 3.3.9. Let \( S \) be the set of finite places of \( F \) such that \( \chi_v \) is ramified. If \( v \in S \) then \( L(\chi_v |\cdot|^s_v) = 1 \). Whereas if \( v \notin S \) then \( \chi_v(\varpi_v) \) does not depend on the choice of an uniformizer \( \varpi_v \) of \( F_v \) and we denote it \( \chi_v(p_v) \). Then \( L(\chi_v |\cdot|^s_v) = \frac{1}{1-\chi_v(p_v)Np_v^{-s}} \).

If \( a \) is a nonzero fractional ideal of \( \mathcal{O}_F \) which is prime to all the \( p_v \) with \( v \in S \), we can define \( \chi(a) := \prod_v \chi_v(p_v)^{v_{p_v}(a)} \). The map \( a \mapsto \chi(a) \) is a character of the group of fractional ideals of \( \mathcal{O}_F \) which are prime to \( S \). The unique factorization property gives us the following formula

\[
\forall s \in \mathbb{C}, \Re s > 1, \quad L(\chi, s) = \sum_{a \in \mathcal{O}_F} \frac{\chi(a)}{Na^s} \text{ for } v \in S
\]

The completed \( L \) function of the character \( \chi \) is defined as

\[
\Lambda(\chi, s) = L(\chi, s) \prod_{v \mid \infty} L(\chi_v |\cdot|^s_v).
\]
3.3. GLOBAL ZETA FUNCTIONS

Let \( \psi \) be a non trivial unitary character of \( \mathbb{A}_F / F \). We also define the epsilon factor of \( \chi \) by the formula:

\[
\varepsilon(\chi, s) = \prod_v \varepsilon(\chi_v, |\cdot|^s_v, \psi_v).
\]

This product is well defined since it is finite: \( \varepsilon(\chi_v, |\cdot|^s_v) = 1 \) if \( \chi_v \) is unramified and conductor of \( \psi_v \) is \( \mathcal{O}_v \). We will also see that the product doesn’t depend on the choice of \( \psi \).

**Theorem 3.3.10** (Hecke, Tate). The function \( s \mapsto \Lambda(\chi, s) \) can be extended into a meromorphic function over \( \mathbb{C} \) and satisfies the functional equation

\[
\Lambda(1 - s, \chi^{-1}) = \varepsilon(\chi, s) \Lambda(\chi, s).
\]

If the character \( \chi \) is not of the form \( |\cdot|^t \) for some \( t \in \mathbb{R} \), the function \( s \mapsto \Lambda(\chi, s) \) is holomorphic on \( \mathbb{C} \).

The function \( s \mapsto \Lambda(1, s) \) has simple poles in 0 and 1. There residues are respectively

\[
\frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F|\Delta_{F/Q}|^{\frac{1}{2}}} \text{ and } \frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F|\Delta_{F/Q}|^{\frac{1}{2}}}
\]

where \( h_F \) is the cardinal of the class field of \( \mathcal{O}_F \), \( R_F \) is the regulator of \( F \) and \( w_F \) is the number of roots of unity contained in \( F \).

If we choose for \( \chi \) the trivial character, the \( L \) function \( L(\chi, s) \) is also called the Dedekind zeta function of \( F \) and is denoted \( \zeta_F(s) \). We have, for \( \text{Re} \ s > 1 \),

\[
\zeta(s) = \sum_{a \subset \mathcal{O}_F} 1 = \prod_p \frac{1}{1 - Np^{-s}}
\]

the sum being taken over all nonzero ideals of \( \mathcal{O}_F \) and the product over all nonzero prime ideals of \( \mathcal{O}_F \).

**Corollary 3.3.11.** The Dedekind zeta function of \( F \) is holomorphic outside of 1 and we have

\[
\zeta_F(s) \sim_{s \to 1} \frac{2^{r_1}(2\pi)^{r_2}h_F R_F}{w_F|\Delta_{F/Q}|^{\frac{1}{2}}}(s - 1)^{-1}.
\]

Moreover the function \( \Lambda(s) = (\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2}))^{r_1}((2\pi)^{1-s}\Gamma(s))^{r_2}\zeta_F(s) \) satisfies the following functional equation

\[
\Lambda(1 - s) = |\Delta_{F/Q}|^{s-\frac{3}{2}}\Lambda(s).
\]

**Remark 3.3.12.** The zeta function of the field \( F \) has a zero of order \( r_1 + r_2 - 1 \) at 0.
CHAPTER 3. ZÉTA FUNCTIONS
Chapter 4

Class field Theory

4.1 Abelian extensions of $p$-adic fields

Let $p$ be a prime number. Let $F$ be a finite extension of $\mathbb{Q}_p$. We use the notation $\mathcal{O}_F$ for its valuation ring, $p_F$ for the maximal ideal of $\mathcal{O}_F$ and $k_F := \mathcal{O}_F / p_F$ for the residue field. Let $q_F$ be the cardinal of $k_F$. We fix $\pi_F$ a uniformizer of $F$. Let $U_F := \mathcal{O}_F^\times$ and, for $i \geq 0$,

$$U_F^i := \begin{cases} U_F & \text{if } i = 0 \\ 1 + p_F^i & \text{if } i \geq 1. \end{cases}$$

We also note $|\cdot|_F$ the normalized absolute value of $F$, i.e. such that $|\pi_F|_F = q_F^{-1}$.

We recall that if $E/F$ is a finite extension of residual degree $f(E/F)$ and inertia index $e(E/F)$, then $[E : F] = e(E/F) f(E/F)$, $[k_E : k_F] = f(E/F)$ and $p_E^{e(E/F)} = p_F \mathcal{O}_F$.

4.1.1 Unramified extensions

Let $E$ be a finite extension of $F$.

**Proposition 4.1.1.** There exists a unique unramified subextension $E/F$ of degree $f(E/F)$. It contains all unramified subextensions of $E/F$ and it is Galois over $F$.

**Proof.** As $k_E$ and $k_F$ are finite fields, the extension $k_E/k_F$ is separable. It follows from the primitive element theorem that there exists a unitary irreducible separable $P \in k_F[X]$ such that $k_E \simeq k_F[X]/(P)$. Let $\widetilde{P} \in \mathcal{O}_F[X]$ a lift of $P$. If $\alpha \in k_E$ is a root of $P$, then $\widetilde{P}(\alpha) = 0$ and it follows from Hensel Lemma that there exists a unique root $\tilde{\alpha} \in \mathcal{O}_F$ of $\widetilde{P}$ lifting $\alpha$. Let $E' := F(\alpha)$. Then $[E' : F] = \deg(\widetilde{P}) = \deg(P) = [k_E : k_F]$. Moreover the map $\mathcal{O}_F E' \subset \mathcal{O}_E \to k_E$ is surjective so that
$k_{E'} = k_F$ and $E'/F$ is unramified. The extension $k_E/k_F$ is Galois so that $P$ is split in $k_E[X]$. Hensel Lemma implies that $\tilde{P}$ is split in $E'$, which proves that $E'$ is a Galois extension of $F$.

Finally let $E'' \subset E$ be an unramified extension of $F$. The residue field of $E''$ is isomorphic to a subfield of $k_E$ containing $k_F$. Let $Q \in k_F[X]$ be such that $k_{E''} \cong k_F[X]/(Q)$. We conclude as before that $E''$ is the decomposition field of any lift $\tilde{Q}$ of $Q$ in $O_F[X]$. Using Hensel Lemma we can prove that $\tilde{Q}$ is also split in $E'$ which implies that $E'' \subset E'$.

**Remark 4.1.2.** If $E/F$ is a Galois extension, the maximal unramified extension of $E/F$ is the fixed subfield of the kernel of the map $\text{Gal}(E/F) \to \text{Gal}(k_E/k_F)$.

**Proposition 4.1.3.** Let $d \geq 1$. Then there exists, up to isomorphism, a unique unramified extension of $F$ of degree $d$.

**Proof.** Let $P \in k_F[X]$ be an irreducible polynomial of degree $d$ and let $\tilde{P} \in O_F[X]$ be a lift of $P$. Then the decomposition field of $\tilde{P}$ over $F$ is an unramified extension of degree $d$. The unicity follows from Hensel Lemma as usual.

If $E/F$ is an unramified extension of degree $d$, then we have a group isomorphism $\text{Gal}(E/F) \cong \text{Gal}(k_E/k_F) \cong \mathbb{Z}/d\mathbb{Z}$. Let $\text{Frob}_{E/F}$ be the Frobenius automorphism of $E$ over $F$ which is the unique $F$-automorphism such that

$$\forall x \in O_E, \quad \text{Frob}_{E/F}(x) \equiv x^{q^d} \mod p_E.$$

**Proposition 4.1.4.** Let $E/F$ be a finite unramified extension of degree $d$. We have $N_{E/F}(U_F) = U_F$. As a consequence $N_{E/F}(E^\times) = \pi_F^{d\times}U_F$.

**Proof.** The extension $E/F$ is Galois so that $N_{E/F}(x) = \prod_{\sigma \in \text{Gal}(E/F)} \sigma(x)$. Moreover we have $N_{E/F}(U_E) \subset U_F$ and, if $i \geq 1$, $\sigma(U_F^i) = U_F^i$ for any $\sigma \in \text{Gal}(E/F)$ so that $N_{E/F}(U_F^i) \subset U_E^i \cap U_F = (1 + \pi_F^iO_E) \cap O_F = 1 + \pi_F^iO_F = U_F^i$ (we use that $\pi_F$ is an uniformizer of $E$ since $E/F$ is unramified). We have two commutative diagrams, where $i \geq 1$,

\[
\begin{array}{c}
U_E/U_F^i \xrightarrow{N_{E/F}} U_F/U_F^i \\
\downarrow \quad \downarrow \\
k_E^i \xrightarrow{N_{k_E/k_F}} k_F^i
\end{array}
\quad \quad \quad \begin{array}{c}
U_E/U_F^{i+1} \xrightarrow{N_{E/F}} U_F/U_F^{i+1} \\
\downarrow \quad \downarrow \\
k_E \xrightarrow{\text{Tr}_{k_E/k_F}} k_F
\end{array}
\]

Namely, if $x \in O_E$, we have, for $i \geq 1$,

$$N_{E/F}(1 + \pi_F^i x) = \prod_{\sigma \in \text{Gal}(E/F)} (1 + \pi_F^i \sigma(x)) \equiv 1 + \pi_F^i \sum_{\sigma \in \text{Gal}(E/F)} \sigma(x) \mod p_F^{i+1}.$$
4.1. ABELIAN EXTENSIONS OF P-ADIC FIELDS

As $k_E/k_F$ is separable, the map $\text{Tr}_{k_E/k_F} : k_E \to k_F$ is surjective and so is $N_{E/F} : U_E/U_F^i \to U_F/U_F^i$ for any $i \geq 1$. Similarly, if $x \in k_E^\times$, we have

$$N_{k_E/k_F}(x) = x^{1+q_F + \cdots + q_F^{d-1}}$$

so that $N_{k_E/k_F}$ is surjective (exercise) and so is $N_{E/F} : U_E/U_F^i \to U_F/U_F^i$. We deduce from this result that the map $N_{E/F} : U_E/U_F^i \to U_F/U_F^i$ is surjective for any $i$. If $x \in U_F$, we can find, for each $n \geq 1$, an element $y_n \in U_E$ such that $x - N_{E/F}(y_n) \in \pi_F^n \mathcal{O}_F$. We deduce that there exists $y \in \mathcal{O}_E$ such that $x = N_{E/F}(y)$. □

**Corollary 4.1.5.** If $E/F$ is unramified, the quotient $F^\times/N_{E/F}(E^\times)$ is a cyclic group of order $[E : F]$ generated by an uniformizer of $F$.

There exists an isomorphism $F^\times/N_{E/F}(E^\times) \simeq \text{Gal}(E/F)$ such that $\pi_F \mapsto \text{Frob}_{E/F}$.

### 4.1.2 Local statements

If $G$ is a group, let $G'$ be its derived subgroup, that is the subgroup generated by all the commutators $[g, h] = ghg^{-1}h^{-1}$ with $g, h \in G$. This a normal subgroup and the quotient $G/G'$ is the largest abelian quotient of $G$. This is the abelianization $G^{ab}$ of $G$.

**Theorem 4.1.6** (Local reciprocity law). For any $E/F$ finite Galois extension, the subgroup $N_{E/F}(E^\times)$ is open in $F^\times$ and there exists a group isomorphism

$$r_{E/F} : F^\times/N_{E/F}(E^\times) \cong \text{Gal}(E/F)^{ab}$$

such that the following properties are satisfied.

a) If $E/F$ is unramified, then $r_{E/F}(\pi_F) = \text{Frob}_{E/F}$.

b) If $E'/F'$ is a finite Galois extension with $F \subset F'$ and $E \subset E'$, the following diagram commutes

$$
\begin{array}{ccc}
F'^\times/N_{E'/F'}(E'^\times) & \xrightarrow{N_{E'/F}} & F^\times/N_{E/F}(E^\times) \\
\downarrow r_{E'/F'} & & \downarrow r_{E/F} \\
\text{Gal}(E'/F')^{ab} & \longrightarrow & \text{Gal}(E/F)^{ab}
\end{array}
$$

where the bottom horizontal arrow is the morphism induced by the restriction map $\text{Gal}(E'/F') \to \text{Gal}(E/F)$.
c) If $\tau : E \xrightarrow{\sim} E'$ is an automorphism of valued fields and if $F' := \tau(F)$, we have a commutative diagram

$$
\begin{array}{ccc}
F^\times / N_{E/F}(E^\times) & \xrightarrow{\tau} & F'^\times / N_{E'/F'}(E'^\times) \\
\downarrow r_{E/F} & & \downarrow r_{E'/F'} \\
\text{Gal}(E/F)^{\text{ab}} & \xrightarrow{\tau} & \text{Gal}(E'/F')^{\text{ab}}
\end{array}
$$

where the bottom horizontal arrow is the isomorphism of groups induced by $\sigma \mapsto \tau \sigma \tau^{-1}$.

Moreover there is at most one family of isomorphisms $(r_{E/F})_{E/F}$ satisfies to a) and b).

**Theorem 4.1.7** (Local existence theorem). Let $N \subset F^\times$ be an open subgroup of finite index. Then there exists a unique up to isomorphism abelian extension $E/F$ such that $N = N_{E/F}(E^\times)$.

Let’s consider some particular cases of the property b) of functoriality.

If $F' = F$, we have a commutative diagram

$$
\begin{array}{ccc}
F^\times / N_{E/F}(E^\times) & \xrightarrow{r_{E/F}} & F^\times / N_{E/F}(E^\times) \\
\downarrow r_{E/F} & & \downarrow r_{E/F} \\
\text{Gal}(E/F)^{\text{ab}} & \xrightarrow{r_{E/F}} & \text{Gal}(E/F)^{\text{ab}}
\end{array}
$$

The upper horizontal arrow is the quotient map and the bottom horizontal arrow is the restriction to $E$.

If $E = E'$, we have a commutative diagram

$$
\begin{array}{ccc}
F'^\times / N_{E'/F'}(E'^\times) & \xrightarrow{N_{E'/F'}^{-1}} & F^\times / N_{E/F}(E^\times) \\
\downarrow r_{E'/F'} & & \downarrow r_{E/F} \\
\text{Gal}(E/F)^{\text{ab}} & \xrightarrow{\bar{\sigma}} & \text{Gal}(E/F)^{\text{ab}}
\end{array}
$$

The bottom horizontal arrow is induced by the inclusion $\text{Gal}(E/F') \subset \text{Gal}(E/F)$.

### 4.1.3 Proof of the unicity

Here we prove the unicity of the reciprocity law. We will need the following lemma.

**Lemma 4.1.8.** Let $E/F$ be a finite Galois extension. Let $\sigma \in \text{Gal}(E/F)$. Then there exists a finite extension $E'/E$ such that $E'/F$ is Galois and $\tilde{\sigma} \in \text{Gal}(E'/F)$ a lift of $\sigma$ such that $E'/(E')^{\tilde{\sigma}}$ is unramified.
4.2. ABELIAN EXTENSIONS OF NUMBER FIELDS

Let’s check that the lemma implies the unicity of the reciprocity law. Namely let \( F' := (E')^\tilde{\sigma} \), the functoriality diagram tells us that \( r_{E/F}^{-1}(\sigma) = N_{F'/F}(r_{E'/F'}(\tilde{\sigma}) = N_{F'/F}(\pi_{F'})^m \) where \( \tilde{\sigma} = \text{Frob}_{E'/F'}^m \).

**Proof.** Let \( K \subset E \) be the maximal unramified subextension and let \( r \geq 0 \) be such that \( \sigma|_K = \text{Frob}_K^r \). Let \( N \geq 1 \) be an integer which is divided by the order of \( \sigma \) in Gal\((E/F)\). Let \( E_1 \) be the unramified extension of \( E \) of degree \( rN \) and let \( F_1 \subset E_1 \) be the maximal unramified extension of \( F \) contained in \( E_1 \). We have

\[
[F_1 : F] = [k_{E_1} : k_F] = rN[k_E : k_F]
\]

and \( [K : F] = [k_E : k_F] \) so that \( [F_1 : K] = rN \). Moreover we have \( F_1 \cap E = K \) so that, by comparison of degrees \( E_1 = F_1E \) and so \( E_1 \) is a Galois extension of \( F \). Let \( \tilde{\sigma} \in \text{Gal}(E_1/F) \) be the element such that \( \tilde{\sigma}|_E = \sigma \) and \( \tilde{\sigma}|_{F_1} = \text{Frob}_{F_1/F}^r \) (such an element exists since \( \text{Frob}_{F_1/F}|_K = \text{Frob}_{K/F}^r = \sigma|_K \)). We need to show that the extension \( E_1/E_1^\tilde{\sigma} \) is unramified. The morphism of groups induces by the restriction to \( F_1 \) is surjective:

\[
\text{Gal}(E_1/E_1^\tilde{\sigma}) \rightarrow \text{Gal}(F_1/F_1^\tilde{\sigma}).
\] (4.1)

Namely both groups are cyclic generated by \( \tilde{\sigma} \) and \( \tilde{\sigma}|_{F_1} \). Moreover the right hand side is a cyclic subgroup of \( \text{Gal}(F_1/F) \) which is cyclic of order \( rN[k_E : k_F] \). As \( \tilde{\sigma}|_{F_1} = \text{Frob}_{F_1/F}^r \), we deduce that \( \text{Gal}(F_1/F) \) is cyclic of order \( N[k_E : k_F] \). On the other side we have \( \sigma^N = 1 \) so that \( \tilde{\sigma}^N|_E = 1 \) and \( \tilde{\sigma}|_{F_1}^{N[k_E : k_F]} = 1 \) so that \( \tilde{\sigma}^{N[k_E : k_F]} = 1 \). It follows that the morphism (4.1) is an isomorphism, which implies that \( E_1 = E_1^\tilde{\sigma}F_1 \) and that \( E_1/E_1^\tilde{\sigma} \) is unramified. \( \square \)

### 4.2 Abelian extensions of number fields

#### 4.2.1 Statements

Let \( E/F \) be a finite extension of number fields. There is a natural inclusion of topological rings

\[
A_E \hookrightarrow A_E
\]
defined by \((x_v)_v \mapsto (y_w)_w \) where \( y_w := x_v \) if \( w \mid v \). We have also multiplicative and additive homomorphisms of topological groups

- the norm

\[
N_{E/F} : (y_w)_w \mapsto (\prod_{w \mid v} N_{E_w/F_v}(y_w))_v
\]

\[
N_{E/F} : (y_w)_w \mapsto (\prod_{w \mid v} N_{E_w/F_v}(y_w))_v
\]
and the trace

$$\text{Tr}_{E/F} : \mathbb{A}_E \rightarrow \mathbb{A}_F$$

$$(y_w)_w \mapsto \left( \sum_{w|v} \text{Tr}_{E_w/F_v}(y_w) \right)_v.$$

We have obvious compatibilities with the norm and trace from $E$ to $F$:

$$\mathbb{E}^\times \xrightarrow{N_{E/F}} \mathbb{F}^\times \xrightarrow{\text{Tr}_{E/F}} \mathbb{F}.$$ 

Now we assume that the finite extension $E/F$ is moreover abelian. Let $v$ be a place of $F$ and $w | v$ a place of $E$. The local reciprocity law allows us to define a group homomorphism $F_v^\times \rightarrow \text{Gal}(E/F)$, $x_v \mapsto (x_v, E/F)$ which is the composite of the following chain of homomorphisms

$$F_v^\times \rightarrow F_v^\times / N_{E_w/F_v}(E_w^\times) \xrightarrow{r_{E_w/F_v}} \text{Gal}(E_w/F_v) \simeq D_w \hookrightarrow \text{Gal}(E/F).$$

We note that this application does not depend on the choice of $w | v$ since $\text{Gal}(E/F)$ is abelian. Moreover if $v$ is unramified in $E$, we have $(x_v, E/F) = 1$ for $x_v \in U_v := U_{F_v}$.

We can therefore define a group homomorphism

$$\text{Art}_{E/F} : \mathbb{A}_F^\times \rightarrow \text{Gal}(E/F) \quad (x_v)_v \mapsto \prod_v (x_v, E/F).$$

This map is called the Artin reciprocity map.

We can state the Artin reciprocity law.

**Theorem 4.2.1** (Artin reciprocity law). We have $\text{Art}_{E/F}(F^\times) = 1$. Moreover $\text{Art}_{E/F}$ is surjective and its kernel is generated by $F^\times$ and $N_{E/F}(\mathbb{A}_E^\times)$. In other words, $\text{Art}_{E/F}$ induces a group isomorphism

$$\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times) \xrightarrow{\sim} \text{Gal}(E/F).$$

Moreover $\text{Art}_{E/F}$ is the unique continuous group homomorphism from $\mathbb{A}_F^\times$ to $\text{Gal}(E/F)$ such that, for all $v$ unramified in $E$, we have

$$\text{Art}_{E/F}(\varpi_v) = \text{Frob}_{E/F}(v)$$

where $\varpi_v = (1, \ldots, 1, \pi_v, 1, \ldots) \in \mathbb{A}_F^\times$ is the idele whose all coordinates are 1 excepted the coordinate at $v$ which is a uniformizer.

**Theorem 4.2.2** (Existence theorem (Takagi, Chevalley)). The map $E \mapsto N_E := F^\times N_{E/F}(\mathbb{A}_E^\times)$ induces a decreasing bijection between isomorphism classes of finite abelian extensions of $F$ and open subgroup of finite index containing $F^\times$ in $\mathbb{A}_F^\times$. 
4.2.2 Reformulation with ideals

Let $E/F$ be a finite abelian extension of number fields. A modulus is a function

$$m : \Sigma_F \rightarrow \mathbb{N}$$

such that

- the support $\text{Supp} \ m := \{v \in \Sigma_F \mid m(v) > 0\}$ of $m$ is finite;
- if $F_v \simeq \mathbb{C}$, then $m(v) = 0$;
- if $F_v \simeq \mathbb{R}$, then $m(v) \in \{0, 1\}$.

We define an order relation on modulus, we say that $m_1 \leq m_2$ if $m_1(v) \leq m_2(v)$ for all $v$.

If $m$ is a modulus, we define an open subgroup of $\mathbb{A}_F^\times$ by the formula

$$V_m := \prod_{v \mid \infty, m(v)=0} F_v^\times \prod_{v \mid \infty, m(v)=1} \mathbb{R}_>^\times \prod_{v \not\mid \infty} U_v^{m_v}.$$

Note that the $V_m$ form a basis of open subgroups of $\mathbb{A}_F^\times$: if $H$ is an open subgroup of $\mathbb{A}_F^\times$, then there exists a modulus $m$ such that $V_m \subset H$.

**Remark 4.2.3.** Be careful that even if $(V_m)_m$ form a basis of open subgroups in $\mathbb{A}_F^\times$ they don’t form a basis of neighborhoods in $\mathbb{A}_F^\times$!

Let $J_F^m$ be the subgroup of $\mathbb{A}_F^\times$ which is the restricted product of the $F_v^\times$ for $v \not\in m$ and $v \nmid \infty$ and let $I_F^m$ be the group of fractional ideals of $\mathcal{O}_F$ which are prime to (the support of) $m$. We have a surjective map

$$J_F^m \twoheadrightarrow I_F^m$$

defined by $\varpi_v = (1, \ldots, 1, \pi_v, 1, \ldots) \mapsto \mathfrak{p}_v$ whose kernel is $\prod_{v \not\in \text{Supp} \ m} U_v$.

**Lemma 4.2.4.** Let $S$ be a finite set of places of $F$. Then the diagonal map $F^\times \to \prod_{v \in S} F_v^\times$ has a dense image.

**Proof.** Let $(x_v) \in \prod_{v \in S} F_v^\times$ and let $\varepsilon > 0$ small enough so that $\varepsilon < |x_v|$ for at least one $v \in S$. By the approximation theorem, there exists $\xi \in F$ such that $|\xi - x_v| < \varepsilon$ for all $v \in S$. By our assumption on $\varepsilon$, we have $\xi \not= 0$ and so $\xi \in F^\times$. \qed

Let $m$ be a modulus of $F$. We define $F_m^\times := F^\times \cap J_F^m V_m$, the intersection being in $\mathbb{A}_F^\times$. More explicitly this is the subgroup of elements of $F^\times$ such that
• if \( m(v) > 0 \) and \( v \nmid \infty, \xi \in U_v^{m(v)}; \)
• if \( m(v) = 1 \) and \( v | \infty \), then \( \xi \in F_v^{\times} > 0 \) (note that \( F_v \simeq \mathbb{R} \) in this case).

Then we define \( P_m \) as the subgroup of \( I_m^F \) of principal fractional ideals generated by an element of \( F_v^{\times} \):

\[
P_m := \{ (a) \mid a \in F_v^{\times} \}.
\]

**Proposition 4.2.5.** The inclusion \( J_m^F \rightarrow \mathbb{A}_F^{\times}/F^{\times}V_m \) factors through \( I_m^F \) and induces an isomorphism

\[
I_m^F/P_m \xrightarrow{\sim} \mathbb{A}_F^{\times}/F^{\times}V_m.
\]

**Proof.** If \( v \notin \text{Supp} \, m \), we have \( U_v \subset V_m \), this implies that the map \( J_v^F \rightarrow \mathbb{A}_v^{\times}/F_v^{\times}V_m \) factors through \( I_v^F \). To prove the surjectivity, it is sufficient to check that \( \mathbb{A}_F^{\times} = J_m^F V_m F^{\times} \). This is a consequence of lemma 4.2.4 since \( \mathbb{A}_F^{\times}/J_m^F = \prod_{v \in \text{Supp} \, m} F_v^{\times} \). Finally if \( (x_v) \in J_v^F \) is in the kernel of the map, there exists \( \xi \in F_v^{\times} \) such that \( (x_v) \in \xi V_m \). Therefore \( v_p(x_v) = v_p(\xi) \) for all maximal ideal \( p_v \) of \( \mathcal{O}_F \) so that the ideal of \( \mathcal{O}_F \) defined by \( (x_v) \) is \( (\xi) \). Moreover \( \xi \in J_v^m V_m \cap F^{\times} = F_m^{\times} \) so that \( (\xi) \in P_m \). \( \square \)

Artin reciprocity law can thus be stated in terms of ideals. Let \( m \) be a modulus such that \( \text{Supp} \, m \) contains all finite places of \( F \) which ramify in \( E \) and all infinite places of \( F \) which are real for \( F \) but becomes complex in \( E \). Then we can define a group homomorphism

\[
\text{Art}_{E/F}^m : I_m^F \rightarrow \text{Gal}(E/F)
\]

by the formula \( \text{Art}_{E/F}^m(p) = \text{Frob}_{E/F}(p) \). This is well defined since \( p \) is unramified in \( E \) if \( p \notin \text{Supp} \, m \).

**Theorem 4.2.6.** Let \( S \) be a finite set of places of \( F \) containing all finite places of \( F \) which ramify in \( E \) and all infinite places of \( F \) which are real for \( F \) but becomes complex in \( E \). Then there exists a modulus \( m \) of support \( S \) such that the map \( \text{Art}_{E/F}^m \) induces an isomorphism

\[
\text{Art}_{E/F}^m : I_m^F/P_m \xrightarrow{\sim} \text{Gal}(E/F).
\]

There is some important particular case. Let \( m = 0 \) be the zero modulus. Then we have

\[
\mathbb{A}_F^{\times}/F^{\times}V_0 \simeq I_0^F/P_0 \simeq \text{Cl}(\mathcal{O}_F).
\]

By the existence theorem, there exists an extension \( H/F \) such that \( N_H = F^{\times}V_0 \) and Artin reciprocity law induces an isomorphism

\[
\text{Art}_{H/F} : \text{Cl}(\mathcal{O}_F) \xrightarrow{\sim} \text{Gal}(H/F).
\]
For any place \( v \) of \( F \), and \( w \mid v \) in \( E \), the local reciprocity map induces an isomorphism
\[
F_v^\times / N_{E_w/F_v}(E_w^\times) \simto \Gal(E_w/F_v)
\]
so that \( U_v \subset N_{E_w/F_v}(E_w^\times) \). As a consequence the extension \( E_w/F_v \) is unramified (if \( v \mid \infty \), this means that \( E_w = F_v \)). The \( H \) is a finite abelian extension which is unramified at all places of \( F \) and this is the largest such extension. Moreover the Artin map is defined by \( \Art_{E/F}(p) = \Frob_{H/F}(p) \) so that the decomposition type of \( p \) in \( H \) depends only on its class in \( \Cl(O_F) \). The field \( H \) is called the Hilbert class field of \( F \).

**Example 4.2.7.** If \( F = \Q(i\sqrt{5}) \), we know that \( \Cl(O_F) \) has order 2 so that the Hilbert class field of \( F \) is a quadratic extension. We can check that the extension \( F(\sqrt{5}) \) is unramified and of degree 2 so that it is the Hilbert class field of \( F \).

**Remark 4.2.8.** 1. In the proof of proposition 4.2.5, we have shown that if \( S \) is a finite set of places containing the ramified places of \( F \) in \( E \), then the map \( J^S_F \to \A_F^\times / \F^\times V \) is surjective for any open subgroup \( V \) of \( \A_F^\times \). It follows that the Artin map \( \Art_{E/F} \) is uniquely defined by its values on elements \( \varpi_v = (1, \ldots, 1, \pi_v, 1, \ldots) \) with \( v \notin S \). Therefore this is the unique continuous group homomorphism sending \( \varpi_v \) on \( \Frob_{E/F}(p_v) \) for \( v \) finite place of \( F \) unramified in \( E \).

2. Using the remark above, it is easy to check the following compatibility for the Artin maps: if \( E'/F' \) is a finite Galois extension with \( F \subset F' \) and \( E \subset E' \), the following diagram commutes
\[
\begin{array}{ccc}
\A_F^\times & \xrightarrow{N_{F'/F}} & \A_F^\times \\
\downarrow{\Art_{E'/F'}} & & \downarrow{\Art_{E/F}} \\
\Gal(E'/F') & \longrightarrow & \Gal(E/F)
\end{array}
\]
where the bottom horizontal arrow is induced by the restriction map.

If \( \tau : E \simto E' \) is an automorphism and if \( F' := \tau(F) \), we have a commutative diagram
\[
\begin{array}{ccc}
\A_F^\times & \xrightarrow{\tau} & \A_F^\times \\
\downarrow{\Art_{E/F}} & & \downarrow{\tau_{E'/F'}} \\
\Gal(E/F) & \xrightarrow{\tau \tau^{-1}} & \Gal(E'/F')
\end{array}
\]
where the bottom horizontal arrow is the isomorphism of groups induced by \( \sigma \mapsto \tau \sigma \tau^{-1} \).
4.3 First inequality

4.3.1 Dirichlet density

Let $F$ be a number field and let $\mathcal{P}_F$ be the set of maximal ideals of $O_F$. A subset $\mathcal{P}$ of $\mathcal{P}_F$ has a Dirichlet density $\delta \in [0,1]$ if

$$\frac{\sum_{p \in \mathcal{P}} Np^{-s}}{\sum_{p \in \mathcal{P}_F} Np^{-s}} \rightarrow_{s \to 1} \delta.$$ 

We remind that if $\text{Re} \ s > 1$, the sum $\sum_{p \in \mathcal{P}_F} Np^{-s}$ is absolutely convergent.

Let $\log$ be the unique branch of the logarithm, defined over $\mathbb{C} \setminus \mathbb{R}_{\leq 0}$ which is equal to

$$\log s = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} \frac{1}{s-1}$$

when $|s-1| < 1$.

**Proposition 4.3.1.** We have

$$\sum_{p \in \mathcal{P}_F} Np^{-s} \sim_{s \to 1} \log \frac{1}{s-1}.$$ 

**Proof.** We have proved that

$$\zeta_F(s) = \prod_{p \in \mathcal{P}_F} \frac{1}{1 - Np^{-s}} \sim_{s \to 1} \frac{a}{s-1}$$

for some $a > 0$ so that

$$\log(\zeta_F(s)) \sim_{s \to 1} \log \frac{1}{s-1}.$$ 

Moreover if $\text{Re} \ s > 1$, we have

$$\log \zeta_F(s) = - \sum_{p \in \mathcal{P}_F} \log(1 - Np^{-s}) = \sum_{p \in \mathcal{P}_F} \sum_{n \geq 1} \frac{1}{n} Np^{-ns}$$

$$= \sum_{n \geq 1} \frac{1}{n} \sum_{p \in \mathcal{P}_F} Np^{-ns}$$

$$= \sum_{p \in \mathcal{P}_F} Np^{-s} + \sum_{n \geq 2} \frac{1}{n} \sum_{p \in \mathcal{P}_F} Npp^{-sn}$$

$$= \sum_{p \in \mathcal{P}_F} Np^{-s} + g(s).$$
We have
\[ |g(s)| \leq [F : \mathbb{Q}] \sum_p \sum_{n \geq 1} \frac{1}{n^2} p^{-n \text{Re}s} \leq \frac{1}{2[F : \mathbb{Q}]} \sum_p p^{-2 \text{Re}s} \frac{1}{1 - p^{-s}} \]
which is uniformly convergent on every compact subset of \([\frac{1}{2}, +\infty[\), so that \(g\) is holomorphic on \([\frac{1}{2}, +\infty[\). We deduce the result.

**Corollary 4.3.2.** If \(\mathcal{P}\) is a finite subset of \(\mathcal{P}_F\), then \(\mathcal{P}\) has Dirichlet density 0.

We say that a maximal ideal of \(O_F\) is **completely decomposed** in a finite extension \(E/F\) for all \(q \mid p\) in \(O_E\), we have \(f(q \mid p) = e(q \mid p) = 1\). Equivalently, \(pO_E\) is a product of \([E : F]\) different maximal ideals of \(O_E\). If the extension \(E/F\) is Galois, a maximal ideal of \(O_F\) is completely decomposed in \(E\) if and only if it is unramified in \(E\) and \(\text{Frob}_{E/F}(q \mid p) = 1\) for one (resp. all) maximal ideal \(q\) of \(O_E\) dividing \(p\).

**Theorem 4.3.3.** Let \(E/F\) be a finite Galois extension of number fields. The set of maximal ideals of \(O_F\) which are completely decomposed in \(E\) has a Dirichlet density equal to \([E : F]^{-1}\).

### 4.3.2 The first inequality

**Theorem 4.3.4.** Let \(E/F\) be a finite Galois extension. Then we have
\[ |\mathbb{A}_F^\times / F^\times N_{E/F}(\mathbb{A}_E^\times)| \leq [E : F]. \]

### 4.3.3 Other consequences

**Theorem 4.3.5.** Let \(E_1/F\) and \(E_2/F\) be two finite Galois extensions of a number field \(F\). For \(i \in \{1, 2\}\), let \(\mathcal{P}_i\) be the set of maximal ideals of \(O_F\) which are completely decomposed in \(E_i\). If \(\mathcal{P}_2 \setminus \mathcal{P}_1\) has Dirichlet density 0 (for example if \(\mathcal{P}_2 \subset \mathcal{P}_1\)), then \(E_1 \subset E_2\).

**Proposition 4.3.6.** Let \(E/F\) be a finite Galois extension of number fields. Then there are infinitely many maximal ideals of \(O_F\) which are not completely decomposed in \(E\).

**Corollary 4.3.7.** Let \(E/F\) be a cyclic extension of number fields of degree \(p^r\) for some prime number \(p\). Then there are infinitely many maximal ideals of \(O_F\) which are inert in \(E\), i.e. such that \(pO_E\) is prime.
Bibliography

