Part 1

Basic number theory

CHAPTER 1

Algebraic numbers and adèles

1. Valuations of the field of rational numbers

We will begin by reviewing the construction of real numbers from rational numbers. Recall that the field of rational numbers $\mathbf{Q}$ is a totally ordered field by the semigroup $\mathbf{Q}_+$ of positive rational numbers. We will call the function $\mathbf{Q}^\times \to \mathbf{Q}_+$ mapping a nonzero rational number x to x or $-x$ depending on whether $x \in \mathbf{Q}_+$ or $-x \in \mathbf{Q}_+$ the **real valuation**. It defines a distance on $\mathbf{Q}$ with values in $\mathbf{Q}_+$ and thus a topology on $\mathbf{Q}$.

A real number is defined as an equivalence class of Cauchy sequences of rational numbers. We recall that a sequence $\{\alpha_i\}_{i\in\mathbf{N}}$ of rational numbers is Cauchy if for all $\epsilon \in \mathbf{Q}_+$, $|\alpha_i - \alpha_j| < \epsilon$ for all i, j large enough, and two Cauchy sequences are said to be equivalent if in shuffling them we get a new Cauchy sequence. The field of real numbers $\mathbf{R}$ constructed in this way is totally ordered by the semigroup $\mathbf{R}_+$ consisting of elements of $\mathbf{R}$ which can be represented by Cauchy sequences with only positive rational numbers. The real valuation can be extended to $\mathbf{R}^\times$ with range in the semigroup $\mathbf{R}_+$ of positive real numbers. The field of real numbers $\mathbf{R}$ is now complete with respect to the real valuation in the sense that every Cauchy sequences of real numbers is convergent. According to the Bolzano-Weierstrass theorem, every closed interval in $\mathbf{R}$ is compact and consequently, $\mathbf{R}$ is locally compact.

We will now review the construction of p-adic numbers in following the same pattern. For a given prime number p, the **p-adic valuation** of a nonzero rational number is defined by the formula

$$|m/n|_p = p^{-\mathrm{ord}_p(m)+\mathrm{ord}_p(n)}$$

where $m, n \in \mathbf{Z} - \{0\}$, and $\mathrm{ord}_p(m)$ and $\mathrm{ord}_p(n)$ are the exponents of the highest power of p dividing m and n respectively. The p-adic valuation is ultrametric in the sense that it satisfies the multiplicative property and the ultrametric inequality:

$$|\alpha\beta|_p = |\alpha|_p|\beta|_p \text{ and } |\alpha+\beta|_p \le \max\{|\alpha|_p, |\beta|_p\}. \tag{1.1}$$

The field $\mathbf{Q}_p$ of p-adic numbers is the completion of $\mathbf{Q}$ with respect to the p-adic valuation, its elements are equivalence classes of Cauchy

sequences of rational numbers with respect to the p-adic valuation. If $\{\alpha_i\}_{i\in\mathbf{N}}$ is a Cauchy sequence for the p-adic valuation, then $\{|\alpha_i|_p\}$ is a Cauchy sequence for the real valuation and therefore it has a limit in $\mathbf{R}_+$. This allows us to extend the p-adic valuation to $\mathbf{Q}_p$ as a function $|.|_p : \mathbf{Q}_p \to \mathbf{R}_+$ that satisfies (1.6). If $\alpha \in \mathbf{Q}_p - \{0\}$ and if $\alpha = \lim_{i\to\infty} \alpha_i$ then the ultrametric inequality (1.1) implies that $|\alpha|_p = |\alpha_i|_p$ for i large enough. In particular, the p-adic valuation ranges in $p^{\mathbf{Z}}$, and therefore in $\mathbf{Q}_+$.

A p-adic integer is defined to be a p-adic number of valuation no more than 1, the set of p-adic integers is denoted:

$$\mathbf{Z}_p = \{\alpha \in \mathbf{Q}_p \mid |\alpha|_p \leq 1\}. \tag{1.2}$$

LEMMA 1.1. *Every p-adic integer can be represented by a Cauchy sequence made only of integers.*

PROOF. We can suppose that $\alpha \neq 0$ because the statement is fairly obvious otherwise. Let $\alpha \in \mathbf{Z}_p - \{0\}$ be a p-adic integer represented by a Cauchy sequence $\alpha_i = p_i/q_i$ where p_i, q_i are relatively prime nonzero integers. As discussed above, for large i, we have $|\alpha|_p = |\alpha_i|_p \leq 1$ so that q_i is prime to p. It follows that one can find an integer q_i' so that $q_i q_i'$ is as p-adically close to 1 as we like, for example $|q_i q_i' - 1| \leq p^{-i}$. The sequence $\alpha_i' = p_i q_i'$, made only of integers, is Cauchy and equivalent to the Cauchy sequence α_i. □

One can reformulate the above lemma by asserting that the ring of p-adic integers $\mathbf{Z}_p$ is the completion of $\mathbf{Z}$ with respect to the p-adic valuation

$$\mathbf{Z}_p = \varprojlim_n \mathbf{Z}/p^n\mathbf{Z}. \tag{1.3}$$

It follows that $\mathbf{Z}_p$ is a local ring, its maximal ideal is $p\mathbf{Z}_p$ and its residue field is the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

It follows also from (1.3) that $\mathbf{Z}_p$ is compact. With the definition of $\mathbf{Z}_p$ as the valuation ring (1.2), it is a neighborhood of 0 in $\mathbf{Q}_p$, and in particular, $\mathbf{Q}_p$ is a locally compact field. This is probably the main property it shares with its cousin $\mathbf{R}$. In constrast with $\mathbf{R}$, the topology on $\mathbf{Q}_p$ is totally disconnected in the sense every p-adic number α admits a base of neighborhoods made of open and compact subsets of the form $\alpha + p^n\mathbf{Z}_p$ with $n \to \infty$.

It is straightforward to derive from the definition of the real and the p-adic valuations that for all $\alpha \in \mathbf{Q}$, $|\alpha|_p = 1$ for almost all primes p, and that the product formula

$$|\alpha|_\infty \prod_p |\alpha|_p = 1 \tag{1.4}$$

holds. In this formula the product runs the prime numbers, and from now on, we will have the product run over the prime numbers together with the sign ∞, which may be considered as the infinite prime of $\mathbf{Q}$.

There are essentially no other valuations of $\mathbf{Q}$ other than the ones we already know. We will define a **valuation** to be a homomorphism $|.| : \mathbf{Q}^\times \to \mathbf{R}_+$ such that the inequality

$$|\alpha + \beta| \leq (|\alpha| + |\beta|) \tag{1.5}$$

is satisfied for all $\alpha, \beta \in \mathbf{Q}^\times$.

For all prime numbers p and positive real numbers t, $|.|_p^t$ is a valuation in this sense. For all positive real numbers $t \leq 1$, $|.|_\infty^t$ is also a valuation. In these two cases, a valuation of the form $|.|_v^t$ will be said to be equivalent to $|.|_v$. Equivalent valuations define the same completion of $\mathbf{Q}$.

THEOREM 1.2 (Ostrowski). *Every valuation of* $\mathbf{Q}$ *is equivalent to either the real valuation or the* p*-adic valuation for some prime number* p.

PROOF. A valuation $|.| : \mathbf{Q}^\times \to \mathbf{R}_+$ is said to be nonarchimedean if it is bounded over $\mathbf{Z}$ and archimedean otherwise.

We claim that a valuation is nonarchimedean if and only if it satisfies the ultrametric inequality

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}. \tag{1.6}$$

If (1.6) is satisfied, then for all $n \in \mathbf{N}$, we have

$$|n| = |1 + \cdots + 1| \leq 1.$$

Conversely, suppose that for some positive real number A, the inequality $|\alpha| \leq A$ holds for all $\alpha \in \mathbf{Z}$. For $\alpha, \beta \in \mathbf{Q}$ with $|\alpha| \geq |\beta|$, the binomial formula and (1.5) together imply

$$|\alpha + \beta|^n \leq A(n+1)|\alpha|^n$$

for all $n \in \mathbf{N}$. By taking the n-th root and letting n go to ∞, we get $|\alpha + \beta| \leq |\alpha|$ as desired.

Let $|.| : \mathbf{Q}^\times \to \mathbf{R}_+$ be a nonarchimedean valuation. It follows from the ultrametric inequality (1.6) that $|\alpha| \leq 1$ for all $\alpha \in \mathbf{Z}$. The subset $\mathfrak{p}$ of $\mathbf{Z}$ consisting of $\alpha \in \mathbf{Z}$ such that $|\alpha| < 1$ is then an ideal. If $|\alpha| = |\beta| = 1$, then $|\alpha\beta| = 1$; in other words $\alpha, \beta \notin \mathfrak{p}$, then $\alpha\beta \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is a prime ideal of $\mathbf{Z}$, and is therefore generated by a prime number p. If t is the positive real number such that $|p| = |p|_p^t$, then for all $\alpha \in \mathbf{Q}$ we have $|\alpha| = |\alpha|_p^t$.

We claim that a valuation $|.|$ is archimedean if for all integers $\beta > 1$, we have $|\beta| > 1$. We will argue by contradiction. Assume there is an integer

$\beta > 1$ with $|\beta| \leq 1$, then we will derive that for all integers α, we have $|\alpha| \leq 1$. One can write

$$\alpha = a_0 + a_1\beta + \cdots + a_r\beta^r$$

with integers a_i satisfying $0 \leq a_i \leq \beta - 1$ and $a_r > 0$. In particular $|a_i| \leq \beta$ and $r \leq \log\alpha / \log\beta$. It follows from (1.5) that

$$|\alpha| \leq (1 + \frac{\log\alpha}{\log\beta})\beta.$$

Replacing α by α^k in the above inequality, taking k-th roots on both sides, and letting k tend to ∞, we will get $|\alpha| \leq 1$.

We now claim that for every two natural numbers $\alpha, \beta > 1$ we have

$$|\alpha|^{1/\log\alpha} \leq |\beta|^{1/\log\beta}. \tag{1.7}$$

One can write

$$\alpha = a_0 + a_1\beta + \cdots + a_r\beta^r$$

with integers a_i satifying $0 \leq a_i \leq \beta - 1$ and $a_r > 0$. In particular $|a_i| < \beta$ and $r \leq \log\alpha / \log\beta$. It follows from (1.5) and $|\beta| > 1$ that

$$|\alpha| \leq \left(1 + \frac{\log\alpha}{\log\beta}\right)\beta|\beta|^{\frac{\log\alpha}{\log\beta}}.$$

Replacing α by α^k in the above inequality, taking k-th roots on both sides, and letting k tend to ∞, we will get (1.7). By symmetry, we then derive the equality

$$|\alpha|^{1/\log\alpha} = |\beta|^{1/\log\beta}, a \tag{1.8}$$

implying $|.|$ is equivalent to the real valuation $|.|_\infty$. □

2. Adèles and idèles for Q

We will denote by $\mathscr{P}$ the set of prime numbers. An **adèle** is a sequence

$$\left(x_\infty, x_p; p \in \mathscr{P}\right)$$

consisting of a real number $x_\infty \in \mathbf{R}$ and a p-adic number $x_p \in \mathbf{Q}_p$ for every $p \in \mathscr{P}$ such that $x_p \in \mathbf{Z}_p$ for almost all $p \in \mathscr{P}$. The purpose of the ring of adèles $\mathbf{A}$ is to simultaneously host analysis on the real numbers and ultrametric analysis on the p-adic numbers. However, it is fair to say this is no easy task since an adèle is somewhat cumbersome structure to imagine as a number. In order to get used to adèles, it may be of some use to unravel the structure of $\mathbf{A}$.

A finite adèle is a sequence

$$\left(x_p; p \in \mathscr{P}\right)$$

with $x_p \in \mathbf{Q}_p$ for all prime p and $x_p \in \mathbf{Z}_p$ for almost all p. If we denote by $\mathbf{A}_{\text{fin}}$ the ring of finite adèles, then $\mathbf{A} = \mathbf{R} \times \mathbf{A}_{\text{fin}}$.

We observe that the subring $\prod_{p\in\mathscr{P}} \mathbf{Z}_p$ of $\mathbf{A}_{\text{fin}}$ can be represented as the profinite completion $\hat{\mathbf{Z}}$ of $\mathbf{Z}$:

$$\prod_{p\in\mathscr{P}} \mathbf{Z}_p = \varprojlim_n \mathbf{Z}/n\mathbf{Z} = \hat{\mathbf{Z}}. \tag{2.1}$$

where the projective limit is taken over the set of nonzero integers ordered by the relation of divisibility. There is indeed a natural surjective map

$$\prod_{p\in\mathscr{P}} \mathbf{Z}_p \to \mathbf{Z}/n\mathbf{Z}$$

for all integers n that induces a surjective map $\prod_{p\in\mathscr{P}} \mathbf{Z}_p \to \hat{\mathbf{Z}}$. This map is also injective as it is easy to see.

On the other hand, $\mathbf{A}_{\text{fin}}$ contains $\mathbf{Q}$, for a rational number α can be represented diagonally as a finite adèle (α_p) with $\alpha_p = \alpha$. For all finite adèles $x \in \mathbf{A}_{\text{fin}}$, there exists an $n \in \mathbf{N}$ so that $nx \in \hat{\mathbf{Z}}$; in other words the relation

$$\mathbf{A}_{\text{fin}} = \bigcup_{n\in\mathbf{N}} n^{-1}\hat{\mathbf{Z}}$$

holds. It follows from this relation that the natural map

$$\hat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathbf{A}_{\text{fin}} \tag{2.2}$$

is surjective. But it is injective as the inclusion $\hat{\mathbf{Z}} \to \mathbf{A}_{\text{fin}}$ is, and therefore it is in fact an isomorphism of $\mathbf{Q}$-vector spaces.

Let us equip $\hat{\mathbf{Z}}$ with the profinite topology, which makes it a compact ring. This topology coincides with the product topology $\hat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$ whose compactness is asserted by the Tychonov theorem. We will equip $\mathbf{A}_{\text{fin}}$ with the finest topology such that the inclusion map $\hat{\mathbf{Z}} = n^{-1}\hat{\mathbf{Z}} \to \mathbf{A}_{\text{fin}}$ is continuous for all n. In other words, a subset U of $\mathbf{A}_{\text{fin}}$ is open if and only if $U \cap n^{-1}\hat{\mathbf{Z}}$ is open in $n^{-1}\hat{\mathbf{Z}}$ for all n. In particular, $\mathbf{A}_{\text{fin}}$ is a locally compact group, of which $\hat{\mathbf{Z}}$ is a compact open subgroup. The group of adèles $\mathbf{A} = \mathbf{A}_{\text{fin}} \times \mathbf{R}$ equipped with product topology is a **locally compact group** as each of the two factors is. It can be proved that a base of the topology of $\mathbf{A}$ consists of open subsets of the form $U = U_{S,\infty} \times \prod_{p\notin S} \mathbf{Z}_p$ where S is a finite set of primes and $U_{S,\infty}$ is an open subset of $\mathbf{R} \times \prod_{p\in S} \mathbf{Q}_p$.

Let us embed $\mathbf{Q}$ in $\mathbf{A}$ diagonally; in other words we map $\alpha \mapsto (\alpha_\infty, \alpha_p)$ with $\alpha_p = \alpha$ for all primes p and $\alpha_\infty = \alpha$.

PROPOSITION 2.1. *The diagonal embedding identifies* $\mathbf{Q}$ *with a discrete subgroup of* $\mathbf{A}$. *The quotient* $\mathbf{A}/\mathbf{Q}$ *can be identified with the prouniversal covering of* $\mathbf{R}/\mathbf{Z}$

$$\mathbf{A}/\mathbf{Q} = \varprojlim_n \mathbf{R}/n\mathbf{Z},$$

the projective limit being taken over the set of natural integers ordered by the divisibility order. In particular, $\mathbf{A}/\mathbf{Q}$ *is a compact group.*

PROOF. Take the neighborhood of 0 in $\mathbf{A}$ defined by $\hat{\mathbf{Z}} \times (-1,1)$ and its intersection with $\mathbf{Q}$. If $\alpha \in \mathbf{Q}$ lies in this intersection, then because the finite adèle part of α lies in $\hat{\mathbf{Z}}$, we must have $\alpha \in \mathbf{Z}$; but as a real number $\alpha \in (-1,1)$, so we must have $\alpha = 0$. This prove the discreteness of $\mathbf{Q}$ as subgroup of $\mathbf{A}$.

There is an exact sequence

$$0 \to \mathbf{R} \times \hat{\mathbf{Z}} \to \mathbf{A} \to \bigoplus_p \mathbf{Q}_p/\mathbf{Z}_p \to 0$$

where $\bigoplus_p \mathbf{Q}_p/\mathbf{Z}_p$ is the subgroup of $\prod_p \mathbf{Q}_p/\mathbf{Z}_p$ consisting of sequences (x_p) whose members $x_p \in \mathbf{Q}_p/\mathbf{Z}_p$ vanish for almost all p. Consider now the homomorphism between two exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathbf{Q} & \longrightarrow & \mathbf{Q} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \hat{\mathbf{Z}} \times \mathbf{R} & \longrightarrow & \mathbf{A} & \longrightarrow & \bigoplus_p \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & 0 \end{array} \tag{2.3}$$

Since the middle vertical arrow is injective and the right vertical arrow is surjective with kernel $\mathbf{Z}$, the snake lemma induces an exact sequence

$$0 \to \mathbf{Z} \to \hat{\mathbf{Z}} \times \mathbf{R} \to \mathbf{A}/\mathbf{Q} \to 0 \tag{2.4}$$

$\mathbf{Z}$ being diagonally embedded in $\hat{\mathbf{Z}} \times \mathbf{R}$. In other words, there is a canonical isomorphism

$$\mathbf{A}/\mathbf{Q} \to \left(\hat{\mathbf{Z}} \times \mathbf{R}\right)/\mathbf{Z}. \tag{2.5}$$

Dividing both sides by $\hat{\mathbf{Z}}$, one gets an isomorphism

$$\mathbf{A}/(\mathbf{Q} + \hat{\mathbf{Z}}) \to \mathbf{R}/\mathbf{Z}. \tag{2.6}$$

With the same argument, for every $n \in \mathbf{N}$ one can identify the covering $\mathbf{A}/(\mathbf{Q} + n\hat{\mathbf{Z}})$ of $\mathbf{A}/(\mathbf{Q} + \hat{\mathbf{Z}})$ with the covering $\mathbf{R}/n\mathbf{Z}$ of $\mathbf{R}/\mathbf{Z}$. It follows that $\mathbf{A}/\mathbf{Q}$ is the prouniversal covering of $\mathbf{R}/\mathbf{Z}$.

For the compactness of the quotient $\mathbf{A}/\mathbf{Q}$, one can also argue as follows. Let B denote the compact subset of $\mathbf{A}$ which is defined as follows

$$B = \{(x_\infty, x_p)_{p \in \bar{\mathcal{P}}}; |x_\infty|_\infty \leq 1 \text{ and } |x_p|_p \leq 1\}. \tag{2.7}$$

With help of the exact sequence (2.4), we see that the map $B \to \mathbf{A}/\mathbf{Q}$ is surjective. Since B is compact, its image in $\mathbf{A}/\mathbf{Q}$ is also compact, and therefore $\mathbf{A}/\mathbf{Q}$ is compact. □

Let us recall that for every prime number p, we have the p-adic absolute value $|.|_p : \mathbf{Q}_p^\times \to \mathbf{R}_+$, whose image is the discrete subgroup $p^{\mathbf{Z}}$ of $\mathbf{R}_+$. The kernel

$$\{\alpha \in \mathbf{Q}_p^\times; |\alpha|_p = 1\}$$

is the complement in $\mathbf{Z}_p$ of the maximal ideal $p\mathbf{Z}_p$, and as $\mathbf{Z}_p$ is a local ring, this kernel is the group $\mathbf{Z}_p^\times$ of invertible elements in $\mathbf{Z}_p$. We have an exact sequence

$$0 \to \mathbf{Z}_p^\times \to \mathbf{Q}_p^\times \to \mathbf{Z} \to 0 \tag{2.8}$$

where $\mathrm{val}_p : \mathbf{Q}_p^\times \to \mathbf{Z}$ is defined such that $|\alpha|_p = p^{-\mathrm{val}_p(\alpha)}$. In particular, $\mathbf{Z}_p^\times$ is the set of p-adic numbers of valuation zero, and $\mathbf{Z}_p$ is the set of p-adic numbers of non-negative valuation.

An **idèle** is a sequence $(x_p; x_\infty)$ consisting of a nonzero p-adic number $x_p \in \mathbf{Q}_p^\times$ for each prime p such that $x_p \in \mathbf{Z}_p^\times$ for almost all p, and $x_\infty \in \mathbf{R}^\times$. The group of idèles $\mathbf{A}^\times$ is in fact the group of invertible elements in ring of adèles $\mathbf{A}$.

We will equip $\mathbf{A}^\times$ with the coarsest topology such that the inclusion map $\mathbf{A}^\times \to \mathbf{A}$ as well as the inversion map $\mathbf{A}^\times \to \mathbf{A}$ given by $x \mapsto x^{-1}$ are continuous. It can be proved that a base of the topology of $\mathbf{A}^\times$ consists of open subsets of the form $U = U_{S,\infty} \times \prod_{p \notin S} \mathbf{Z}_p^\times$ where S is a finite set of primes and $U_{S,\infty}$ is an open subset of $\prod_{p \in S} \mathbf{Q}_p^\times \times \mathbf{R}^\times$.

We also have $\mathbf{A}^\times = \mathbf{A}_{\mathrm{fin}}^\times \times \mathbf{R}^\times$. The subgroup

$$\prod_p \mathbf{Z}_p^\times = \hat{\mathbf{Z}}^\times = \varprojlim_n (\mathbf{Z}/n\mathbf{Z})^\times,$$

where the projective limit is taken over the set of nonzero integers ordered by the divisibility order, is a compact open subgroup of $\mathbf{A}_{\mathrm{fin}}^\times$. It follows that $\mathbf{A}_{\mathrm{fin}}^\times$ is locally compact, and so is the group of idèles $\mathbf{A}^\times = \mathbf{A}_{\mathrm{fin}}^\times \times \mathbf{R}^\times$.

LEMMA 2.2. *The group of invertible rational numbers $\mathbf{Q}^\times$ embeds diagonally in $\mathbf{A}^\times$ as a discrete subgroup.*

PROOF. If $\alpha \in \mathbf{Q}^\times$ such that $\alpha \in \mathbf{Z}_p^\times$ for all prime p then $\alpha \in \mathbf{Z}^\times = \{\pm 1\}$. This implies that $\mathbf{Q}^\times \cap (\hat{\mathbf{Z}}^\times \times \mathbf{R}^\times) = \{\pm 1\}$ which shows that $\mathbf{Q}^\times$ is a discrete subgroup of $\mathbf{A}^\times$. □

We define the absolute value of every idèle $x = (x_\infty, x_p) \in \mathbf{A}^\times$ as

$$|x| = \prod_p |x_p|_p |x_\infty|_\infty,$$

this infinite product being well defined since $|x_p|_p = 1$ for almost all prime p. Let us denote by $\mathbf{A}^1$ the kernel of the absolute value

$$0 \to \mathbf{A}^1 \to \mathbf{A}^\times \to \mathbf{R}_+ \to 0 \tag{2.9}$$

The product formula (7.3) implies that the discrete subgroup $\mathbf{Q}^\times$ is contained in $\mathbf{A}^1$. Let us consider $\hat{\mathbf{Z}}^\times = \prod_p \mathbf{Z}_p^\times$ as a compact subgroup of $\mathbf{A}$ consisting of elements $(x_p; x_\infty)$ with $x_p \in \mathbf{Z}_p^\times$ and $x_\infty = 1$. Let us consider $\mathbf{R}_+$ as the subgroup of $\mathbf{A}^\times$ consisting of elements of the form $(x_p; x_\infty)$ with $x_p = 1$ and $x_\infty \in \mathbf{R}_+$ a positive real number.

PROPOSITION 2.3. *The homomorphism $\mathbf{Q}^\times \times \hat{\mathbf{Z}}^\times \times \mathbf{R}_+ \to \mathbf{A}^\times$ that maps $\alpha \in \mathbf{Q}^\times, u \in \hat{\mathbf{Z}}^\times, t \in \mathbf{R}_+$ on $x = \alpha u t \in \mathbf{A}^\times$ is an isomorphism. Via this isomorphism, the subgroup $\mathbf{A}^1$ of $\mathbf{A}^\times$ correspond to the subgroup $\mathbf{Q}^\times \times \hat{\mathbf{Z}}^\times$ of $\mathbf{Q}^\times \times \hat{\mathbf{Z}}^\times \times \mathbf{R}_+$.*

PROOF. Let us construct the inverse homomorphism. Let $x = (x_\infty, x_p)$ be an idèle. For every prime p there is a unique way to write x_p under the form $x_p = p^{r_p} y_p$ where $y_p \in \mathbf{Z}_p^\times$ and $r_p \in \mathbf{Z}$; note that $r_p = 0$ for almost all p. We can also write $x_\infty = \epsilon |x_\infty|$ where $\epsilon \in \{\pm 1\}$ and $|x_\infty| \in \mathbf{R}_+$. Then we set $\alpha = \epsilon \prod_p p^{r_p} \in \mathbf{Q}^\times$, $y = (y_p, 1) \in \hat{\mathbf{Z}}^\times$ and $t = |x|$. This defines a homomorphism from $\mathbf{A}^\times$ to $\mathbf{Q}^\times \times \hat{\mathbf{Z}}^\times \times \mathbf{R}_+$ which is an inverse to the multiplication map $(\alpha, u, t) \mapsto \alpha u t$ from $\mathbf{Q}^\times \times \hat{\mathbf{Z}}^\times \times \mathbf{R}_+$ to $\mathbf{A}^\times$. □

3. Integers in number fields

Number fields are finite extensions of the field of rational numbers. For every irreducible polynomial $P \in \mathbf{Q}[x]$ of degree n, the quotient ring $\mathbf{Q}[x]/(P)$ is a finite extension of degree n of $\mathbf{Q}$. The irreducibility of P implies that $\mathbf{Q}[x]/(P)$ is a domain, in other words the multiplication with every nonzero element $y \in \mathbf{Q}[x]/P$ is an injective $\mathbf{Q}$-linear map in $\mathbf{Q}[x]/P$. As $\mathbf{Q}$-vector space $\mathbf{Q}[x]/P$ is finite dimensional, all injective endomorphisms are necessarily bijective. It follows that $\mathbf{Q}[x]/(P)$ is a field, finite extension of $\mathbf{Q}$. All finite extensions of $\mathbf{Q}$ are of this form since it is known that all finite extensions of a field in characteristic zero can be generated by a single element [**?**, V,4.6].

Let L be a finite extension of degree n of $\mathbf{Q}$. For every element $\alpha \in L$, the multiplication by α in L can be seen as $\mathbf{Q}$-linear transformation of L as a $\mathbf{Q}$-vector space. We define $\mathrm{Tr}_{L/\mathbf{Q}}(\alpha)$ as the trace of this transformation and $\mathrm{Nm}_{L/\mathbf{Q}}(\alpha)$ as its determinant, the subscript $L/\mathbf{Q}$ can be dropped if no confusion is possible. The $\mathbf{Q}$-linear transformation induces by the multiplication by α in L has a characteristic polynomial

$$\mathrm{ch}(\alpha) = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n$$

with $c_1 = \mathrm{Tr}(\alpha)$ and $c_n = \mathrm{Nm}(\alpha)$. If $\alpha_1, \ldots, \alpha_n$ are the zeroes of $\mathrm{ch}(\alpha)$ in an algebraic closed field containing $\mathbf{Q}$, for instant $\mathbf{C}$, then $\mathrm{Tr}(\alpha) = \alpha_1 + \cdots + \alpha_n$.

PROPOSITION 3.1. *Let L be a finite extension of $\mathbf{Q}$ and $\alpha \in L$. The following assertion are equivalent:*

(1) *The ring* $\mathbf{Z}[\alpha]$ *generated by* α *is a finitely generated* $\mathbf{Z}$*-module.*
(2) *The coefficients* $c_1, \dots, c_n$ *of the characteristic polynomial* $\mathrm{ch}(\alpha)$ *are integers.*

PROOF. Assume that $\mathbf{Z}[\alpha]$ is $\mathbf{Z}$-module of finite type. It is contained in the subfield $E = \mathbf{Q}[\alpha]$. Choose a $\mathbf{Z}$-basis of $\mathbf{Z}[\alpha]$. The multiplication by α preserves $\mathbf{Z}[\alpha]$ thus can be expressed as an integral matrix in this basis. It follows that $\mathrm{ch}_{E/\mathbf{Q}}(\alpha)$ is a polynomial with integral coefficient. Now L is a E-vector space of some dimension r, the polynomial $\mathrm{ch}_{L/\mathbf{Q}}(\alpha) = \mathrm{ch}_{E/\mathbf{Q}}(\alpha)^r$ also has integral coefficients.

Assume that the coefficients $c_1, \dots, c_n$ are integers. Since α is annihilated by its characteristic polynomial according to the Cayley-Hamilton theorem, $\mathbf{Z}[\alpha]$ is a quotient of $\mathbf{Z}[x]/\mathrm{ch}_{L/\mathbf{Q}}(\alpha)$. Since $\mathbf{Z}[x]/\mathrm{ch}_{L/\mathbf{Q}}(\alpha)$ is a $\mathbf{Z}$-module of finite type generated by the classes of $1, x, \dots, x^{n-1}$, so is its quotient $\mathbf{Z}[\alpha]$. □

An element α of number field is called integral if it satisfies one of the above conditions. If α, β are integral then so are $\alpha + \beta$ and $\alpha\beta$ since $\mathbf{Z}[\alpha, \beta]$ is a finitely generated $\mathbf{Z}$-module as long as $\mathbf{Z}[\alpha]$ and $\mathbf{Z}[\beta]$ are. It follows that the set $\mathbf{Z}_L$ of integral elements in L is a subring of L which will be called the ring of integers of L.

PROPOSITION 3.2. *Let* L *be a finite extension of* $\mathbf{Q}$*. The symmetric bilinear form on* L *as* $\mathbf{Q}$*-vector space given by*

$$(\alpha, \beta) \mapsto \mathrm{Tr}_{L/\mathbf{Q}}(\alpha\beta). \tag{3.1}$$

is nondegenerate.

PROOF. We recall that all finite extension of field of characteristic 0 can be generated by one element. Let α be a generator of L as $\mathbf{Q}$-algebra and $P \in \mathbf{Q}[x]$ the minimal polynomial of α which is a monic polynomial of degree $n = \deg(L/\mathbf{Q})$, then $\{1, \alpha, \dots, \alpha^{n-1}\}$ form a basis of L as $\mathbf{Q}$-vector space. Since P is an irreducible polynomial in $\mathbf{Q}[x]$, it has no multiple roots and in particular $P'(\alpha) \neq 0$.

We also recall the Euler formula

$$\mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{\alpha^i}{P'(\alpha)}\right) = \begin{cases} 0 & \text{if } i = 0, \dots, n-2 \\ 1 & \text{if } i = n-1 \end{cases} \tag{3.2}$$

This derives from the expansion of $1/P$ for all separable polynomial $P \in \mathbf{Q}[x]$ as linear combination of simple fractions $1/(x - \alpha_j)$ where $\alpha_1, \dots, \alpha_n$ are the zeroes of P in an algebraic closed field containing $\mathbf{Q}$

$$\frac{1}{P} = \sum_{j=1}^{n} \frac{1}{P'(\alpha_j)(x - \alpha_j)}$$

Let us develop the left and right hand side as power series in variable $y = x^{-1}$

$$\frac{1}{P} = y^n Q$$

where $Q \in \mathbf{Q}[[y]]^\times$ is an invertible power series and

$$\frac{1}{x - \alpha_j} = y \sum_{i=0}^{\infty} \alpha_j^i y^i.$$

By equating coefficients in low degrees, we obtain the formulas

$$\mathrm{Tr}_{L/\mathbf{Q}}\left(\frac{\alpha^i}{P'(\alpha)}\right) = \sum_{j=1}^{n} \frac{\alpha_j^i}{P'(\alpha_j)} = \begin{cases} 0 & \text{if } i = 0, \ldots, n-2 \\ 1 & \text{if } i = n-1 \end{cases}$$

and hence the Euler formula (3.2).

The matrix of the bilinear form (3.1) expressed in the two basis

$$\{1, \alpha, \ldots, \alpha^{n-1}\} \text{ and } \left\{\frac{\alpha^{n-1}}{P'(\alpha)}, \frac{\alpha^{n-2}}{P'(\alpha)}, \ldots, \frac{1}{P'(\alpha)}\right\}$$

is unipotent upper triangle and therefore invertible. □

PROPOSITION 3.3. *The ring of integers of any finite extension L of $\mathbf{Q}$ is a finitely generated $\mathbf{Z}$-module.*

PROOF. The bilinear form (3.1) induces a $\mathbf{Z}$-bilinear form $\mathbf{Z}_L \times \mathbf{Z}_L \to \mathbf{Z}$ as for all $\alpha, \beta \in \mathbf{Z}_L$ we have $\mathrm{Tr}_{L/\mathbf{Q}}(\alpha, \beta) \in \mathbf{Z}$. If $\mathbf{Z}_L^\perp$ is the submodule of $\beta \in L$ such that $\mathrm{Tr}_{L/\mathbf{Q}}(\alpha, \beta) \in \mathbf{Z}$ for all $\alpha \in \mathbf{Z}_L$ then $\mathbf{Z}_L \subset \mathbf{Z}_L^\perp$. Let us assume there is a finitely generated $\mathbf{Z}$-module M of rank n contained in $\mathbf{Z}_L$, then we have inclusions

$$M \subset \mathbf{Z}_L \subset \mathbf{Z}_L^\perp \subset M^\perp.$$

This implies that $\mathbf{Z}_L$ is a finitely generated $\mathbf{Z}$-module as $M^\perp$ is.

Now to construct such M we start with a generator α of L as $\mathbf{Q}$-algebra. After multiplying α by an integer, we can assume that $\alpha \in \mathbf{Z}_L$ and set M as the $\mathbf{Z}$-module generated by $1, \alpha, \ldots, \alpha^{n-1}$. □

As both $\mathbf{Z}_L$ and $\mathbf{Z}_L^\perp$ are finitely generated $\mathbf{Z}$-module of rank n, one contained in the other, the quotient $\mathbf{Z}_L^\perp / \mathbf{Z}_L$ is a finite group. We define the absolute **discriminant** of L to be the order of this finite group.

PROPOSITION 3.4. *Let L be a number field and $\mathbf{Z}_L$ its ring of integers. Then we have $\mathbf{Z}_L \otimes_{\mathbf{Z}} \mathbf{Q} = L$.*

PROOF. Pick a $\mathbf{Z}$-basis of $\mathbf{Z}_L$. Since this basis is $\mathbf{Q}$-linearly independent, the map $\mathbf{Z}_L \otimes_{\mathbf{Z}} \mathbf{Q} \to L$ is injective. It remains to prove that it is also surjective. For every element $\alpha \in L$, there exists $N \in \mathbf{Z}$ so that the characteristic polynomial $\mathrm{ch}_{L/\mathbf{Q}}(\alpha)$ has integral coefficient thus $N\alpha \in \mathbf{Z}_L$ thus α belongs to the image of $\mathbf{Z}_L \otimes_{\mathbf{Z}} \mathbf{Q}$. □

4. Valuations of number fields

An **valuation** of a number field L is a homomorphism $|.| : L^\times \to \mathbf{R}_+$ such that the inequality

$$|\alpha + \beta| \leq |\alpha| + |\beta|$$

is satisfied for all $\alpha, \beta \in L^\times$. A valuation of L is said to be **nonarchimedean** if it remains bounded on the ring of integers $\mathbf{Z}_L$ and **archimedean** otherwise.

By restricting a valuation $|.|$ of L to the field of rational numbers, we obtain a valuation of $\mathbf{Q}$. By virtue of Theorem 1.2, a valuation of $\mathbf{Q}$ is either equivalent to the real valuation or a p-adic valuation for some prime number p.

LEMMA 4.1. *A valuation of L is archimedean if and only if its restriction to $\mathbf{Q}$ is equivalent to the real valuation, and conversely, it is nonarchimedean if and only if its restriction to $\mathbf{Q}$ is equivalent to a p-adic valuation. In the latter case, the valuation satisfies the ultrametric inequality* (1.6) *and the valuation of all integers $\alpha \in \mathbf{Z}_L$ is less than one.*

PROOF. In the case where the restriction of $|.|$ to $\mathbf{Q}$ is equivalent to the real valuation, $|.|$ is unbounded on $\mathbf{Z}_L$ in other words it is archimedean. However unlike the case of rational numbers, it is generally not true that $|\alpha| \geq 1$ for all $\alpha \in \mathbf{Z}_L - \{0\}$.

In the case where the restriction of $|.|$ to $\mathbf{Q}$ is equivalent to the p-adic valuation for some prime number p, $|.|$ is bounded on $\mathbf{Z}$. We claim that it is also bounded on $\mathbf{Z}_L$, in other words this valuation is nonarchimedean. Indeed, all elements $\alpha \in \mathbf{Z}_L$ satisfies an equation of the form

$$\alpha^r + a_1\alpha^{r-1} + \cdots + a_r = 0$$

where r is the degree of the extension $L/\mathbf{Q}$ and where $a_1, \ldots, a_r \in \mathbf{Z}$. Since $|a_i| \leq 1$, the triangle inequality implies that the positive real number $|\alpha|$ satisfies

$$|\alpha|^r \leq |\alpha|^{r-1} + \cdots + |\alpha| + 1$$

which proves that $|\alpha|$ is bounded for $\alpha \in \mathbf{Z}_L$. The same argument as in the proof of Theorem 1.2 then shows that $|\alpha| \leq 1$ for all $\alpha \in \mathbf{Z}_L$ and the ultrametric inequality (1.6) is satisfied. □

Before classifying all valuations of L, we will classify them up to an equivalence relation. We will say that two valuations of a number field L are topology equivalent if the completions L_u and $L_{u'}$ of L with respect to u and u' are isomorphic as topological fields containing L. A topology equivalence class of valuation of L will be called a **place** of L. If u is a place of L, we will denote by L_u the topological field obtained as the completion of L with respect to a valuation in topology equivalence class u; L_u can

be equipped with different valuations giving rise to the same topology. We will denote by $\bar{\mathscr{P}}_L$ the set of places of L and for each $u \in \mathscr{P}_L$, L_u the completion of L with respect to a valuation in topology equivalence class u.

In virtue of Theorem 1.2, we know that valuations of $\mathbf{Q}$ are of the form $|.|_v^t$ where $|.|_v$ is either the real valuation or the p-adic valuation. The valuation $|.|_v^t$ is equivalent to $|.|_v$ in the the above sense. We have also proved that for every prime number $\mathbf{Q}_p$ is isomorphic as topological fields neither to $\mathbf{R}$ nor to $\mathbf{Q}_\ell$ where ℓ is a different prime number. It follows that the set of places of $\mathbf{Q}$ is $\bar{\mathscr{P}} = \mathscr{P} \cup \{\infty\}$ where $\mathscr{P}$ is the set of primes numbers.

Let $|.|_u$ be a valuation of L at the place u and $|.|_v$ its restriction to $\mathbf{Q}$. We observe that $\mathbf{Q}_v$ can be realized as the closure of $\mathbf{Q}$ in L_u so that as topological field, $\mathbf{Q}_v$ depends only on the place u and not in a particular choice of valuation $|.|_u$ at u. We derive a map $\pi : \bar{\mathscr{P}}_L \to \bar{\mathscr{P}}$ and denote by $\mathscr{P}_L = \pi^{-1}(\mathscr{P})$ and $\mathscr{P}_\infty = \pi^{-1}(\infty)$. According to 4.1, $\mathscr{P}_L$ consists in topology equivalent classes of nonarchimedean valuations and $\mathscr{P}_\infty$ in topology equivalent classes of archimedean valuations of L.

We will give an algebraic description of the set $\pi^{-1}(v)$ of places u above a given place v of $\mathbf{Q}$. If $u \in \pi^{-1}(v)$, we will write $u|v$. In such a circumstance, the field L_u as normed $\mathbf{Q}_v$-vector space is complete, in other words, it is a Banach $\mathbf{Q}_v$-vector space. We will later prove that it is finite dimensional. Let us recall some basic facts about finite dimensional Banach spaces.

LEMMA 4.2. *All linear maps between finite dimensional Banach $\mathbf{Q}_v$-vector spaces are continuous. All finite dimensional subspaces of V in Banach $\mathbf{Q}_v$-vector space are closed.*

PROOF. Since linear maps between finite dimensional Banach vector spaces can be expressed in terms of matrices, they are continuous. It follows that the topology on a n-dimensional Banach $\mathbf{Q}_v$-vector space is the same as product topology on $\mathbf{Q}_v^n$.

Let U be a n-dimensional subspace in a Banach $\mathbf{Q}_v$-vector space V. Let $v \in V - U$. Let U_+ be the $(n+1)$-dimensional subspace generated by U and v. Since U_+ has the same topology as $\mathbf{Q}_v^{n+1}$, U is closed in U_+. It follows that there exists a neighborhood of v in V with no intersection with U. It follows that U is closed in V. □

PROPOSITION 4.3. *Let L be a number field . Let v be a place of $\mathbf{Q}$. The $\mathbf{Q}_v$-algebra $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$ is a direct product of finite extensions of $\mathbf{Q}_v$. The set of factors in this product is in natural bijection with the set of places $u|v$ and the factor corresponding to u is the completion L_u of L at the place u*

$$L \otimes_{\mathbf{Q}} \mathbf{Q}_v = \prod_{u|v} L_u.$$

In particular, for all place $u|v$, L_u is a finite extension of $\mathbf{Q}_v$ and

$$\dim_{\mathbf{Q}}(L) = \sum_{u|v} \dim_{\mathbf{Q}_v}(L_u)$$

PROOF. Let us write L in the form $L = \mathbf{Q}[x]/P$ where P is an irreducible polynomial in $\mathbf{Q}[x]$. Note that in characteristic zero, irreducible polynomial has no multiple zeroes. Let us decompose P as a product $P = P_1 \dots P_m$ of irreducible polynomials in $\mathbf{Q}_v[x]$. Since P has multiple zeros, the P_i are mutually prime. Then we can decompose $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$

$$L \otimes_{\mathbf{Q}} \mathbf{Q}_v = \prod_{i=1}^{m} \mathbf{Q}_v[x]/P_i$$

as product of finite extensions of $\mathbf{Q}_v$.

Let u be a valuation of L that restrict to the valuation v of $\mathbf{Q}$. By construction, L_u is a complete $\mathbf{Q}_v$-algebra containing L as a dense subset. We derive a homomorphism of $\mathbf{Q}_v$-algebras

$$\phi_u : L \otimes_{\mathbf{Q}} \mathbf{Q}_v \to L_u.$$

Since L is a finite-dimensional $\mathbf{Q}$-vector space, its image is a finite dimensional $\mathbf{Q}_v$-vector subspace of the normed vector space L_u. Because $\mathrm{im}(\phi_u)$ is finite dimensional, it is necessarily a closed subspace of the normed vector space L_u. Moreover, as it contains the dense subset L, it is equal to L_u. It follows that ϕ_u is surjective and L_u is a finite extension of $\mathbf{Q}_v$, factor of $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$.

Two valuations of L are equivalent if and only if L_u and $L_{u'}$ are isomorphic as topological fields containing L. In that case they are the same factor of $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$. It follows that the set of equivalence class of valuations $u|v$ is a subset of the set of factors of $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$.

It remains to prove that every factor of $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$ can be obtained as the completion of L with respect to a valuation. Let F be a factor of $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$. F is a finite dimensional $\mathbf{Q}_v$-vector space equipped with a $\mathbf{Q}_v$-norm

$$|\alpha|_F = |\mathrm{Nm}_{F/\mathbf{Q}_v}(\alpha)|_v^{1/r_u}. \tag{4.1}$$

We claim that L is dense in the Banach $\mathbf{Q}_v$-vector space F. Indeed, this derives from the fact that L is dense in $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$ and the surjective map $L \otimes_{\mathbf{Q}} \mathbf{Q}_v \to F$ is continuous. In only remains that (4.1) satisfies the triangle inequality. We will check this statement in the real and p-adic cases separately. □

Up to the fact that (4.1) satisfies the triangle inequality, we have proved that equivalence classes of valuations of a number field L over a given valuation u of $\mathbf{Q}$ are classified by factors of $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$. In order to complete the classification of valuations of K, it remains to determine valuations

of local fields i.e finite extension of $\mathbf{Q}_v$ where $\mathbf{Q}_v$ is either the field of real numbers $\mathbf{R}$ or the field of p-adic numbers $\mathbf{Q}_p$.

Let F be a finite extension of $\mathbf{Q}_v$ the completion of $\mathbf{Q}$ with respect to the real valuation if $v = \infty$ or the p-adic valuation if v is a prime number p. A **positive norm of** F is continuous homomorphism $\|.\| : F^\times \to \mathbf{R}_+$ such that the family of subsets parametrized by $c \in \mathbf{R}_+$

$$B_c = \{x \in F, \|x\| < c\}$$

form a base of neighborhood of 0 in F. A **valuation of** F is a positive norm if it further satisfies the triangle inequality

$$\|x + y\| \leq \|x\| + \|y\|. \tag{4.2}$$

We say that it satisfies the ultrametric inequality if

$$\|x + y\| \leq \max(\|x\|, \|y\|) \tag{4.3}$$

for all $x, y \in F$.

PROPOSITION 4.4. *Let $v \in \bar{\mathscr{P}}$ be a place of $\mathbf{Q}$ and let us $|.|_v$ the real of p-adic valuation of $\mathbf{Q}_v$ depending on either $v = \infty$ or v is a prime number. For every finite extension F of $\mathbf{Q}_v$, (4.1) is the unique valuation $|.|_F : F^\times \to \mathbf{R}_+$, extending the valuation $|.|_v$ on $\mathbf{Q}_v$.*

All positive norms of F are of the forms $\|.\| = |.|_F^t$ for some positive real number t. This positive norm further satisfies the triangle inequality if and only if either v is archimedean and $0 < t \leq 1$, or v is nonarchimedean and t is any positive real number.

The proof of this proposition is a case by case analysis and consists in a series of Lemmas 4.5, 4.6, 4.7 and 4.8. First, if F is an archimedean local field then F is either the field of real numbers $\mathbf{R}$ or the field of complex numbers $\mathbf{C}$ for $\mathbf{C}$ is the only nontrivial extension of $\mathbf{R}$.

LEMMA 4.5. *All positive norms of $\mathbf{R}$ are of the forms $\|.\| = |.|_{\mathbf{R}}^t$ for some positive real number t. This positive norm further satisfies the triangle inequality if and only if $0 < t \leq 1$.*

PROOF. We claim that all continuous homomorphism $\chi : \mathbf{R}^\times \to \mathbf{R}_+$ is of the form $x \mapsto |x|^t$ for some $t \in \mathbf{R}$. Since $\chi(-1)^2 = 1$, we have $\chi(-1) = 1$, and we only have to determine the restriction of χ to $\mathbf{R}_+$. Now since the exponential defines a isomorphism of topological groups $\mathbf{R} \to \mathbf{R}_+$, we only need to prove that all continuous homomorphism $a : \mathbf{R} \to \mathbf{R}$ is of the form $x \mapsto \alpha x$ for some $\alpha \in \mathbf{R}$. Indeed, If $a(1) = \alpha$ then $a(q) = \alpha q$ for all rational number q. It follows by continuity that $a(x) = \alpha x$ for all $x \in \mathbf{R}$.

Now the family of subsets $B_c = \{x, |x|^t < c\}$ for $c \in \mathbf{R}_+$ form a base of neighborhood of 0 if and only if $t > 0$, and $\|x\| = |x|^t$ satisfies the triangle inequality if and only if $0 < t \leq 1$. □

LEMMA 4.6. *As for* $\mathbf{C}$*, the formula* (4.1) *gives rise to the usual absolute value* $|z|_{\mathbf{C}} = \sqrt{\Re(z)^2 + \Im(z)^2}$*. All positive norms of* $\mathbf{C}$ *are of the forms* $\|.\| = |.|_{\mathbf{C}}^t$ *for some positive real number* t*. All valuations of* $\mathbf{C}$ *are of the form* $z \mapsto |z|^t$ *for some real number* $0 < t \leq 1$*.*

PROOF. Let $\chi : \mathbf{C}^\times \to \mathbf{R}_+$ be a continuous homomorphism. It maps the unit circle on a compact subgroup of $\mathbf{R}_+$. However, $\mathbf{R}_+$ has no compact subgroup but the trivial one. It follows that χ factorizes through the absolute value. It follows from 4.5 that $\chi(z) = |z|^t$ for some $t \in \mathbf{R}_+$. If χ extends the usual absolute value on $\mathbf{R}^\times$ then $t = 1$. It satisfies triangle inequality if and only if $t \leq 1$. □

LEMMA 4.7. *All positive norms of* $\mathbf{Q}_p$ *are of the form* $\|x\| = |\mathrm{Nm}_{F/\mathbf{Q}_p}(x)|_v^t$ *for some positive real number* t*, and satisfy the ultrametric inequality* (4.3)*.*

PROOF. We use similar arguments as for $\mathbf{C}$. Since $\mathbf{Z}_p^\times$ is a compact subgroup of $\mathbf{Q}_p^\times$, the restriction of $\|.\|$ to $\mathbf{Z}_p^\times$ is trivial. If t is the real number such that such that $\|p\| = p^{-t}$ then $\|x\| = |x|_p^t$ for all $x \in \mathbf{Q}_p$. The homomorphism $x \mapsto |x|_p^t$ defines a positive norm of F if and only if $t > 0$, and in this case it satisfies the ultrametric inequality (4.3). □

LEMMA 4.8. *Let* $F/\mathbf{Q}_p$ *be a finite extension of the field of* p*-adic numbers* $\mathbf{Q}_p$ *of degree* r*. Then* $|.|_F$ *defined in* (4.1) *is a valuation of* F*, and it is the unique valuation on* F *whose restriction to* $\mathbf{Q}_p$ *is the* p*-adic valuation. All positive norms of* F *is of the form* $\|x\| = |x|_F^t$ *for some positive real number* t*, and satisfy the ultrametric inequality* (4.3)*.*

PROOF. Let r denote the dimension of F as $\mathbf{Q}_p$-vector space. For every $\alpha \in F$, the multiplication by α defines a $\mathbf{Q}_p$-linear transformation of F and thus has a characteristic polynomial

$$\mathrm{ch}(\alpha) = x^r - c_1 x^{r-1} + \cdots + (-1)^r c_r \in \mathbf{Q}_p[x].$$

An element $\alpha \in F$ is called integral if all coefficients of its characteristic polynomial are in p-adic integers. As in 3.3, we prove that the set $\mathcal{O}_F$ of all integral elements in F is a $\mathbf{Z}_p$-algebra and as a $\mathbf{Z}_p$-module, it is finitely generated. We claim that $\mathcal{O}_F$ is the set of elements $\alpha \in F$ such that $\|\alpha\| \leq 1$.

First we prove that for all $\alpha \in \mathcal{O}_F$, we have $\|\alpha\| \leq 1$. Indeed, $\mathcal{O}_F$ being a finitely generated $\mathbf{Z}_p$-module, is a compact subset of F. The restriction of $\|.\|$ to $\mathcal{O}_F$ is therefore bounded. Since $\mathcal{O}_F$ is stable under multiplication, if the restriction of $\|.\|$ to $\mathcal{O}_F$ is bounded, it is bounded by 1.

Second we prove that of $\|\alpha\| \leq 1$ then α is an integral element of F. Let us choose an arbitrary basis $v_1, \ldots, v_r$ of F as $\mathbf{Q}_p$ vector space. The linear mapping $\mathbf{Q}_p^r \to F$ given by this basis is then a homeomorphism. In particular, the $\mathbf{Z}_p$-module generated by $v_1, \ldots, v_n$ is a neighborhood of

0. By definition of the topology on F, the subsets $B_c = \{x \in F, \|x\| < c\}$ form a system of neighborhood of 0 as $c \to 0$. For c small enough, B_c is contained in $\bigoplus_{i=1}^{r} \mathbf{Z}_p v_i$. Now, B_c being a $\mathbf{Z}_p$-submodule of $\mathbf{Z}_p^n$, it has to be finitely generated. Because it is open, it has to be of rank r. For all $\alpha \in F$ with $\|\alpha\| \leq 1$, the multiplication by α preserves B_c for all t. Thus the multiplication by α preserves a $\mathbf{Z}_p$-submodule of rank r. It follows that its characteristic polynomial of α has coefficients in $\mathbf{Z}_p$.

The set of integral elements $\mathcal{O}_F$ in F is a local ring with maximal ideal

$$\mathfrak{m}_F = \{x \in F, \|x\| < 1\}$$

since elements $x \in \mathcal{O}_F - \mathfrak{m}_F$ have norm one and are obviously invertible elements of $\mathcal{O}_F$. For $\mathcal{O}_F$ is finitely generated as $\mathbf{Z}_p$-module, so is its maximal ideal $\mathfrak{m}_F$. In particular, it is a compact subset of F. We claim $\mathfrak{m}_F$ is generated as $\mathcal{O}_F$-module by a single element.

Indeed, for $\mathfrak{m}_F$ is a compact subset of F, the range of the the positive norm restricted to $\mathfrak{m}_F$ is a compact subset of $\mathbf{R}$. The norm $\|.\|$ reaches its maximum on some element $\varpi \in \mathfrak{m}$. For all $x \in \mathfrak{m}$, we have $\|\varpi\| \geq \|x\|$ and therefore $x = \varpi y$ for some $y \in \mathcal{O}_F$, in other words, ϖ is a generator of $\mathfrak{m}_F$.

Finally, we claim that for all $x \in F^\times$, $\|x\| = \|\varpi\|^n$ for some integer $n \in \mathbf{Z}$. Indeed, if this is not the case, one can form a product of the form $x^m \varpi^n$ with $m, n \in \mathbf{Z}$ such that

$$\|\varpi\| < \|x^m \varpi^n\| < 1$$

contradicting the very definition of ϖ.

It follows that every element $x \in F^\times$ is of the form $x = \varpi^n y$ for some integer n and $y \in \mathcal{O}_F^\times$. If $\|p\| = p^{-t}$ then we will have $\|x\| = |x|_F^t$ for all $x \in F^\times$. For $|x|_F^t$ to be a positive norm of F, the necessary and sufficient condition is $t > 0$. Moreover it satisfies the ultrametric inequality for all $t > 0$. □

A generator ϖ of the maximal ideal $\mathfrak{m}_F$ is called **uniformizing parameter**. There exists a unique integer $e \in \mathbf{N}$, to be called **ramification index** such that $p = \varpi^e y$ with $y \in \mathcal{O}_F^\times$. Since $|p| = p^{-1}$, we must have

$$|\varpi|_F = p^{-1/e}. \tag{4.4}$$

Let us denote by $\mathfrak{f}_F = \mathcal{O}_F/\mathfrak{m}_F$ the residue field. The residue field $\mathfrak{f}_F = \mathcal{O}_F/\mathfrak{m}_F$ is a finite extension of $\mathbf{F}_p$ of degree d dividing $r = \deg(F/\mathbf{Q}_p)$; d is called the **residual degree**.

We claim that the ramification index and the residual degree satisfy the fomrula

$$r = de \tag{4.5}$$

where r is the degree of the extension $F/\mathbf{Q}_p$. Indeed since all element $x \in \mathcal{O}_F$ can be written in the form $x = \varpi^n y$ with $n \in \mathbf{N}$ and $y \in \mathcal{O}_F^\times$, for

every n, the quotient $\mathfrak{m}_F^n/\mathfrak{m}_F^{n+1}$ is one dimensional $\mathfrak{f}_F$-vector space. As $\mathbf{F}_p$-vector space, $\mathfrak{m}_F^n/\mathfrak{m}_F^{n+1}$ has dimension d. It follows that $\mathscr{O}_F/p\mathscr{O}_F$ is a $\mathbf{F}_p$-vector space of dimension de. On the other hand, $\mathscr{O}_F$ is a free $\mathbf{Z}_p$-module of rank r, thus $\mathscr{O}_F/p\mathscr{O}_F$ is a $\mathbf{F}_p$-vector space of rank r and therefore $r = de$.

We will record the following statement that derives from the description of positive norms on local fields archimedean or nonarchimedean.

COROLLARY 4.9. *Let F be a local field F equipped with a positive norm $x \mapsto \|x\|$. For all $c > 0$, the set $\{x \in F; \|x\| \leq c\}$ is a compact subset of F. Moreover the map $\|.\| : F^\times \to \mathbf{R}_+$ is proper.*

Let L be a number field and u an archimedean place of L. We have $u|\infty$ where ∞ is the infinite place of $\mathbf{Q}$. Then L_u can be either $\mathbf{R}$ or $\mathbf{C}$ and we will say that u is a real or complex place correspondingly. By Proposition 4.3, we have $L \otimes_{\mathbf{Q}} \mathbf{R} = \prod_{u|\infty} L_u$. In particular if r is the degree of extension $L/\mathbf{Q}$, r_1 the number of real places and r_2 the number of complex places of L, then we have

$$r = r_1 + 2r_2. \tag{4.6}$$

Let L be an extension of degree r of the field of rational numbers $\mathbf{Q}$. For each valuation u of L dividing a prime number p, we will denote by d_u the residual degree of the extension $L_v/\mathbf{Q}_p$ and e_u the ramification index. Then we have the formula

$$r = \sum_{u|p} d_u e_u. \tag{4.7}$$

We are now going to generalize the product formula (7.3) to number field L. Instead of the valuation $|.|_u$ defined in (4.1) which turns out to be unfit for this purpose, we set

$$\|x\|_F = |\mathrm{Nm}_{F/\mathbf{Q}_v}(x)|_v, \tag{4.8}$$

in other words, if F is a finite extension of $\mathbf{Q}_v$ of degree r, we have $\|x\|_F = |x|_F^r$. In particular as for $\mathbf{C}$, we have

$$\|z\|_{\mathbf{C}} = |z|_{\mathbf{C}}^2 = \Re(z)^2 + \Im(z)^2. \tag{4.9}$$

If F is a finite extension of $\mathbf{Q}_p$ of degree r, of ramification index e and of residual degree d, we have

$$\|\varpi\|_F = |\varpi|_F^r = p^{-d} = |\mathfrak{f}_F|^{-1} \tag{4.10}$$

where ϖ is an uniformizing parameter and $|\mathfrak{f}_F|$ is the cardinal of the residue field $\mathfrak{f}_F$.

PROPOSITION 4.10. *For all $\alpha \in L^\times$, we have $\|\alpha\|_u = 1$ for almost all places u of L, and the product formula*

$$\prod_{u \in \bar{\mathscr{P}}_L} \|\alpha\|_u = 1 \tag{4.11}$$

holds.

PROOF. We claim that for all places v of $\mathbf{Q}$, we have

$$|\mathrm{Nm}_{L/\mathbf{Q}}(\alpha)|_v = \prod_{u|v} \|\alpha\|_u. \tag{4.12}$$

Recall that $L \otimes_{\mathbf{Q}} \mathbf{Q}_v = \prod_{u|v} L_u$. The multiplication by α defines a $\mathbf{Q}_v$-linear endomorphism of $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$ preserving each factor L_u. Its determinant $\mathrm{Nm}_{L/\mathbf{Q}}(\alpha)$ is therefore equal to a product

$$\mathrm{Nm}_{L/\mathbf{Q}}(\alpha) = \prod_{u|v} \mathrm{Nm}_{L_u/\mathbf{Q}_v}(\alpha)$$

from which we derive (4.12).

In virtue of (4.12), the product formula for L can be reduced to the product formula for $\mathbf{Q}$. □

5. Dedekind domains

Let us recall that a **Dedekind domain** is a noetherian integrally closed domain of which every nonzero prime ideals is maximal.

PROPOSITION 5.1. *The ring of integers $\mathbf{Z}_L$ in a finite extension L of $\mathbf{Q}$ is a Dedekind domain.*

PROOF. Every ideal of $\mathbf{Z}_L$ is finitely generated as $\mathbf{Z}$-module thus a fortiori as $\mathbf{Z}_L$-module. It follows that $\mathbf{Z}_L$ is a noetherian ring. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathbf{Z}_L$, $\mathfrak{f} = \mathbf{Z}_L/\mathfrak{p}$ is a domain. The intersection $\mathfrak{p} \cap \mathbf{Z}$ is a nonzero prime ideal thus it is generated by a prime number p. Now $\mathfrak{f}$ is a domain over $\mathbf{F}_p$ and finite dimensional as $\mathbf{F}_p$-vector space. For every $\alpha \in \mathfrak{f}^\times$, the multiplication by α is an injective $\mathbf{F}_p$-linear transformation and therefore surjective. It follows that $\mathfrak{f}$ is a field, in other words $\mathfrak{p}$ is a maximal ideal. □

It is obvious from definition that localization of Dedekind domain is still a Dedekind domain. Local Dedekind domains have very simple structure: they are **discrete valuation ring**. A local ring R is said to be a discrete valuation ring if there exists an element $\varpi \in R$ such that every ideal of R is generated by a power of ϖ.

PROPOSITION 5.2. *Local Dedekind domains are discrete valuation rings.*

PROOF. Let R be a local Dedekind domain, L its field of fraction and $\mathfrak{m}$ its maximal ideal. Assume that $\mathfrak{m} \neq 0$ i.e. $R \neq L$ because otherwise the statement would be vacuous. Because R is a Dedekind domain, it has exactly two prime ideals, namely 0 and $\mathfrak{m}$.

First we claim that for all $x \in \mathfrak{m}$, $R[x^{-1}] = L$ where $R[x^{-1}]$ is the subring of L generated by R and x^{-1}. Let $\mathfrak{p}$ be a prime ideal of $R[x^{-1}]$. The intersection $\mathfrak{p} \cap R$ is a prime ideal of A which does not contain x, thus $\mathfrak{p} \cap R \neq \mathfrak{m}$ in other words $\mathfrak{p} \cap R = 0$. It follows that $\mathfrak{p} = 0$ since if there is a nonzero element $y \in \mathfrak{p}$, yx^n will be a nonzero element of $R \cap \mathfrak{p}$ for some integer n. Since all prime ideals of $R[x^{-1}]$ are zero, $R[x^{-1}]$ is a field. As a field containing R and contained in the field of fractions L of R, the only possibility is $R[x^{-1}] = L$.

Second we claim that for all nonzero element $a \in \mathfrak{m}$, there is $n \in \mathbf{N}$ such that $\mathfrak{m}^n \subset (a)$ where (a) is the ideal generated by a. Since R is noetherean, $\mathfrak{m}$ is finitely generated. Let $x_1, \ldots, x_n$ be aset of generators of $\mathfrak{m}$. Since $a \in R[x_i^{-1}]$, there exists $n_i \in \mathbf{N}$ such that $a = y/x_i^n$ for some $y \in R$. It follows that $x_i^{n_i} \in (a)$. Now for $n \geq \sum_i n_i$, we have $\mathfrak{m}^n \subset (a)$.

Let $n \in \mathbf{N}$ be the smallest integer such that $\mathfrak{m}^n \subset (a)$, and let $b \in \mathfrak{m}^{n-1} - (a)$. We claim that a/b is a generator of $\mathfrak{m}$. Let us consider the R-submodule $M = (b/a)\mathfrak{m}$ of L. Since $b\mathfrak{m} \subset (a)$, we have $M \subset R$. If $(b/a)\mathfrak{m} = \mathfrak{m}$, then b/a is an integral element over R as $\mathfrak{m}$ is a finitely generated R-module. As consequence, $b/a \in R$ since R is integrally closed. We derive the inclusion $b \in (a)$ that contradicts the initial assumption on b. Hence M is a R-submodule of R which is not contained in the maximal ideal $\mathfrak{m}$. The only possibility left is $(b/a)\mathfrak{m} = M = R$ i.e. $\mathfrak{m} = (a/b)R$.

Let ϖ be a generator of the maximal ideal $\mathfrak{m}$. We claim that for all $x \in R$, there exist $n \in \mathbf{N}$ and $y \in R^\times$ such that $x = \varpi^n y$. If $x \notin \mathfrak{m}$ then $x \in \mathbf{R}^\times$ and we are done. If $x \in \mathfrak{m}$ then we can write $x = \varpi x_1$ for some $x_1 \in R$, and we reiterate with x_1 instead of x. If this iteration does not stop, then for all $n \in \mathbf{N}$ there exists $x_n \in R$ such that $y = \varpi^n x_n$. In that case, we have an increasing chain of ideals $(x) \subset (x_1) \subset (x_2) \subset \cdots$ which must eventually stop because R is noetherean. If $(x_n) = (x_{n+1})$ with $x_n = \varpi x_{n+1}$ then $\varpi \in R^\times$ and cannot be a generator of $\mathfrak{m}$ as we have assumed. Thus the iteration process has to stop i.e. there exists $n \in \mathbf{N}$ with $x_n \in R^\times$ and we have $x = \varpi^n x_n$.

Now we prove that every ideal I of R is principal. Since R is noetherean, I is finitely generated. Let $x_1, \ldots, x_r$ be a system of generators of I and let us write $x_i = \varpi^{n_i} y_i$ with $y_i \in R^\times$. We can assume that $n_1 \leq n_2 \leq \cdots \leq n_r$. Then I is generated by x_1. □

COROLLARY 5.3. *Let L be a number field, $\mathbf{Z}_L$ its ring of integers. There is a canonical bijection between the set of nonarchimedean places of L and the set of maximal ideals of $\mathbf{Z}_L$.*

PROOF. If $\mathfrak{p}$ is a maximal ideal of $R = \mathbf{Z}_L$, then the local ring $R_\mathfrak{p}$ is of discrete valuation i.e. there exists an uniformizing parameter ϖ in the maximal ideal $\mathfrak{m}_\mathfrak{p}$ of $R_\mathfrak{p}$ such that every nonzero element $x \in R_\mathfrak{p}$ can be written uniquely in the form $x = \varpi^n y$ for some $n \in \mathbf{N}$ and $y \in R_\mathfrak{p}^\times$. Thus every element $x \in L^\times$ can be uniquely written in the form $x = \varpi^n y$ with $n \in \mathbf{Z}$ and $y \in R_\mathfrak{p}^\times$. The map $x \mapsto q^{-n}$ where q is any real number greater than 1 defines a ultrametric valuation of R. These valuations are topology equivalent and give rise to a place of L to be denoted $u_\mathfrak{p}$.

Conversely if u is a nonarchimedean place of L lying over a a prime number p, then the completion L_u is a finite extension of $\mathbf{Q}_p$, its ring of integers $\mathcal{O}_u$ contains the ring of integers R of L. Now, $\mathcal{O}_u$ is also a complete discrete valuation ring with maximal ideal $\mathfrak{m}_u$. If we set $\mathfrak{p}_u = \mathfrak{m}_u \cap R$ then $\mathfrak{p}_u$ is a prime ideal of R. Since $R/\mathfrak{p}_u$ is a subring of the residual field $\mathfrak{f}_u$ of $\mathcal{O}_u$ which is finite, $R/\mathfrak{p}_u$ is also finite and therefore $\mathfrak{p}_u$ is a maximal ideal.

The two maps $\mathfrak{p} \mapsto u_\mathfrak{p}$ and $u \mapsto \mathfrak{p}_u$ that just have been defined between the set of maximal ideals of $\mathbf{Z}_L$ and the set of nonarchimedean valuations of L, are inverse one of each other. □

We recall that a module M over a commutative ring R is said to be locally free of rank r if for every prime ideal $\mathfrak{p}$ of R, the localization $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module of rank r where $R_\mathfrak{p}$ is the localization of R at $\mathfrak{p}$. An **invertible R-module** is a shorthand for locally free R-module of rank one.

COROLLARY 5.4. *A finitely generated module M over a Dedekind domain R is locally free if and only if it is torsion-free.*

PROOF. One can be reduced to prove the local statement that a finitely generated module over a local Dedekind domain is free if and only if it is torsion free. As we know from Propostion 5.2 that local Dedekind domains are principal, this statement derive from the classification of modules over principal ideal domain, see [**?**] for more details. □

PROPOSITION 5.5. *Let R be a noetherean ring. Then set* $\mathrm{Cl}(R)$ *of isomorphism classes of invertible R-modules is a commutative group under tensor product.*

PROOF. We only need to prove the existence of an inverse. The inverse of an invertible R-module M is given by $M' = \mathrm{Hom}_R(M, R)$. Since the operation $M \mapsto M'$ commutes with localization, M' is an invertible module as long as M is. For the natural map $M \otimes_R M' \to R$ is an isomorphism after localization, it is an isomorphism. □

In what follows, we will consider a Dedekind domain R of field of fractions L. This discussion applies to the ring of integers $\mathbf{Z}_L$ in any number field L or its localizations.

If M is an invertible R-module, then $M \otimes_R L$ is one-dimensional L-vector space. We will denote by $\mathrm{Cl}^+(R)$ the group of isomorphism classes of invertible R-modules M equipped with an isomorphism $\iota : M \otimes L \to L$.

The group $\mathrm{Cl}^+(R)$ can be conveniently described as the group of fractional ideals where a **fractional ideal** of R is a nonzero finitely generated R-submodule of L.

PROPOSITION 5.6. *By mapping the isomorphism class of a pair (M,ι) where M is an invertible R-module and $\iota : M \otimes_R L \to L$ is an isomorphism of L-vector spaces, on the fractional ideal $m = \iota(M)$, we obtain a map from $\mathrm{Cl}^+(R)$ on the set of fractional ideals.*

The induced group law on the set of fractional ideals is given as follows: if $m, m' \subset L$ are fractional ideals then mm' is the module generated by elements of the form $\alpha\alpha'$ where $\alpha \in m$ and $\alpha' \in m'$. The inverse m^{-1} is the submodule generated be elements $\beta \in L$ such that $\alpha\beta \in A$ for all $\alpha \in m$.

PROOF. For locally free R-modules are torsion-free, the map ι induces an isomorphism from M on its image m. It follows that the map from $\mathrm{Cl}^+(R)$ to the set of nonzero finitely generated R-submodules of L is injective. All R-submodules of L are torsion free, nonzero finitely generated R-submodules m of L are automatically locally free of rank one. It follows that the above mentioned map is also surjective.

If (M,ι) and (M',ι') are elements of $\mathrm{Cl}^+(R)$ with $m = \iota(M)$, $m' = \iota(M')$ corresponding submodules in L, $(M \otimes_R M', \iota \otimes_R \iota')$ will correspond to the submodule $(\iota \otimes \iota')(M \otimes_R M')$ generated by elements of the form $\alpha\alpha'$ where $\alpha \in m$ and $\alpha' \in m'$.

If $m \subset L$ is a finitely generated R-submodule of L then a R-linear map $M \to A$ is just a map $m \to L$ with range in R. Now a R-linear map $m \to L$ extends uniquely to a L-linear map $m \otimes_R L \to L$ which must be necessarily given by an element $\beta \in L$. This is equivalent to an element $\beta \in L$ such that $\beta m \subset A$. □

Let $\mathscr{P}(R)$ denote the set of maximal ideals in R and $\mathbf{Z}\mathscr{P}(R)$ the free abelian group generated by this set. As $\mathscr{P}(R)$ can naturally be embedded into the set of all nonzero finitely generated R-submodules of L, there is a canonical homomorphism of abelian groups $\mathbf{Z}\mathscr{P}(R) \to \mathrm{Cl}^+(R)$.

THEOREM 5.7. *The inclusion $\mathscr{P}(R) \subset \mathrm{Cl}^+(R)$ induces an isomorphism between the free abelian group $\mathbf{Z}\mathscr{P}(R)$ generated by $\mathscr{P}(R)$ and the group $\mathrm{Cl}^+(R)$ of fractional ideals of R.*

PROOF. First we prove that the map $\mathbf{Z}\mathscr{P}(R) \to \mathrm{Cl}^+(R)$ is injective. If it is not, there exists an element $\sum_{i\in I} r_i \mathfrak{p}_i \in \mathbf{Z}\mathscr{P}(R)$ such that $\prod_{i\in I} \mathfrak{p}_i^{r_i} = A$. Here I is a finite set of indices, $\mathfrak{p}_i$ are distinct maximal ideals indexed by I and $r_i \in \mathbf{Z}$. Let separate $I = I_+ \cup J$ such that $r_i > 0$ for all $i \in I_+$ and $r_j \leq 0$ for all $j \in J$. We can assume that I_+ is non empty. Under this notation, we have

$$\prod_{i\in I_+} \mathfrak{p}_i^{r_i} = \prod_{j\in J} \mathfrak{p}_j^{-r_j}.$$

Fix an element $i \in I_+$. One can choose for each $j \in J$ an element $\alpha_j \in \mathfrak{p}_j$ which does not belong to $\mathfrak{p}_i$ and form the product $\prod_{j\in J} \alpha_j^{r_j}$ that belongs to the right hand side but does not belong to $\mathfrak{p}_i$ a fortiori to the left hand side.

Now we prove that $\mathbf{Z}\mathscr{P}(R) \to \mathrm{Cl}^+(R)$ is surjective. For every finitely generated R-submodule m of L, we claim that m can be written as $m = m_1 m_2^{-1}$ where m_1, m_2 are R-submodules of R. Indeed, one can tale $m_2 = m^{-1} \cap A$ which is a nonzero R-submodule of R and $m_1 = m m_2$.

Now we prove that every nonzero ideal of R lies in the image of the homomorphism $\mathbf{Z}\mathscr{P}(R) \to \mathrm{Cl}^+(R)$. Assume that there exists a nonzero R-submodule m of R which does not lie in this image. We can assume that m is maximal with this property. Now m is an ideal, there exists a maximal ideal $\mathfrak{p} \in \mathscr{P}(R)$ such that $m \subset \mathfrak{p}$. Since $\mathfrak{p}^{-1} m$ contains strictly m, it does lie in the image of $\mathbf{Z}\mathscr{P}(R) \to \mathrm{Cl}^+(R)$, and then so does m. We reached a contradiction that shows indeed all non zero ideals of R lie in the image of $\mathbf{Z}\mathscr{P}(R) \to \mathrm{Cl}^+(R)$. □

The homomorphism $\mathrm{Cl}^+(R) \to \mathrm{Cl}(R)$ mapping the class of isomorphism of (M, ι) on the class of isomorphism of M is surjective. The group $L^\times$ of invertible elements of L acts on $\mathrm{Cl}^+(R)$ by mapping the class of isomorphism of (M, ι) on the class of isomorphism of $(M, \alpha\iota)$ for all $\alpha \in L^\times$. In terms on R-submodules of L, α maps a fractional $m \subset L$ on $\alpha m \subset L$.

The orbits of $L^\times$ in $\mathrm{Cl}^+(R)$ are exactly the fibers of the map $\mathrm{Cl}^+(R) \to \mathrm{Cl}(R)$ so that $\mathrm{Cl}(R)$ can be identified with the quotient set of $\mathrm{Cl}^+(R)$ by the action of $L^\times$. However, the action of $L^\times$ on $\mathrm{Cl}^+(R)$ contains more information than the mere quotient set.

PROPOSITION 5.8. *The orbits of $L^\times$ in $\mathrm{Cl}^+(R)$ are exactly the fibers of the map $\mathrm{Cl}^+(R) \to \mathrm{Cl}(R)$ so that $\mathrm{Cl}(R)$ can be identified with the quotient set of $\mathrm{Cl}^+(R)$ by the action of $L^\times$. The stabilizer of $L^\times$ at any point $m \in \mathrm{Cl}^+(R)$ is equal to $R^\times$ for all $m \in \mathrm{Cl}^+(R)$.*

PROOF. Let $m \in \mathrm{Cl}^+(R)$ be a nonzero finitely generated R-submodule of L. An automorphism of m induces a L-linear automorphism of $m \otimes L = L$ thus an element $\alpha \in L^\times$ which has to satisfies $\alpha m = m$.

If $\mathfrak{p}$ is a maximal ideal of R, we will denote by $R_\mathfrak{p}$ the localization of R at $\mathfrak{p}$ and $m_\mathfrak{p}$ the localization of m. If $\alpha \in L^\times$ such that $\alpha m = m$ then $\alpha m_\mathfrak{p} = m_\mathfrak{p}$ for all $\mathfrak{p} \in \mathscr{P}(R)$. Since $m_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module of rank one, this implies that $\alpha \in R_\mathfrak{p}^\times$. Since R is normal, an element $\alpha \in L^\times$ such that $\alpha \in R_\mathfrak{p}$ lies necessarily in R. For the same argument applies to α^{-1}, we have $\alpha \in R^\times$. □

Let L be a number field and $\mathbf{Z}_L$ its ring of integers in L. Let $\bar{\mathscr{P}}_L = \mathscr{P}_L \cup \mathscr{P}_\infty$ be the set of places of L, where $\mathscr{P}_L$ the set of nonarchimedean places is the set of maximal ideals of $\mathbf{Z}_L$, and $\mathscr{P}_\infty$ the set of archimedean places. Let $S \subset \mathscr{P}_L$ be a finite set of nonarchimedean places. Let R_S denote the localization of $\mathbf{Z}_L$ away from S i.e. R_S is generated by elements of L of the form $\alpha\beta^{-1}$ where $\alpha, \beta \in \mathbf{Z}_L$ and $\beta \notin \mathfrak{p}$ for all maximal ideals $\mathfrak{p} \notin S$. In particular the set $\mathscr{P}(R_S)$ of maximal ideals in R_S is $\mathscr{P}(\mathbf{Z}_L) - S$.

We now state together two finiteness theorems whose proof can be found in every textbook of algebraic number theory, for instant [**9**]. The first statement is concerned with the finiteness of class number and the second with the Dirichlet unit theorem. We will later reformulate these theorems and their proof in the language of adèles.

THEOREM 5.9. *The group* $\mathrm{Cl}(R_S)$ *of isomorphism classes of invertible* R_S*-modules is finite. The group of invertible elements* $R_S^\times$ *is finitely generated of free rank equal to* $|S| + |S_\infty| - 1$.

6. Quadratic fields

For number fields of degree two over $\mathbf{Q}$, explicit calculations can be done on objects that have been earlier introduced for general number fields. Quadratic number fields are of the form $L = \mathbf{Q}[x]/(x^2 - d)$ for some square free integer d. If $d > 0$, then $\mathbf{R}$ contains square root of of d, thus $L_\mathbf{R} = L \otimes_\mathbf{Q} \mathbf{R} = \mathbf{R} \times \mathbf{R}$; in this case L is said to be a real quadratic field. If $d < 0$, then $L_\mathbf{R} = \mathbf{C}$; and L is said to be a complex quadratic field.

For $d = -1$, we embed $L = \mathbf{Q}[x]/(x^2 + 1)$ in the field of complex numbers by mapping x on i which is our favorite square root of -1. The ring of integers $\mathbf{Z}_L$ of L is then the ring of Gauss integers

$$R = \{a + ib \text{ with } a, b \in \mathbf{Z}\}, \tag{6.1}$$

which is an Euclidean domain in the sense that for all $\alpha \in L$, there exists $\beta \in R$ such that $\|\alpha - \beta\| < 1$ with respect to the usual norm for complex number. It is known that Euclidean domains are principal ideal domain, and therefore the group of ideal classes $\mathrm{Cl}(R)$ is trivial. We observe that in general, an integral element $\alpha \in \mathbf{Z}_L$ is invertible if only if its norm $\mathrm{Nm}_{L/\mathbf{Q}}(\alpha) \in \{\pm 1\}$. In the case of the ring R of Gaussian integers, it follows that $R^\times = \{\pm 1, \pm i\}$.

It follows from the calculation that the module $R^\perp$ of elements $\alpha \in L$ such that $\mathrm{Tr}_{L/\mathbf{Q}}(\alpha\beta) \in \mathbf{Z}$ for all $\beta \in R$, is

$$R^\perp = \{a + ib \text{ with } 2a, 2b \text{ and } a+b \in \mathbf{Z}\},$$

and therefore the discriminant $d_L = |R^\perp/R|$ is equal to 2.

For every prime number $p \neq 2$, either (p) remains a prime ideal in L or (p) splits as product of two distinct prime ideals $(p) = \mathfrak{p}_1\mathfrak{p}_2$. The first case happens when R/pR is a quadratic extension of $\mathbf{F}_p$; and the second case happens when R/pR is a product of two copies of $\mathbf{F}_p$. One can check that the latter happens if and only if -1 is a square modulo p. One can also derive from the fact $\mathbf{F}_p^\times$ is a cyclic group of order $p-1$ that -1 is a square modulo p if and only if $p \equiv 1 \mod 4$. Now if p is a prime number satisfying this congruence, (p) splits in the ring of Gauss integers into product of two distinct prime ideals $(p) = \mathfrak{p}_1\mathfrak{p}_2$. Since R is known to be a principal domain, $\mathfrak{p}_1$ is generated by an element of the form $\alpha = a + ib$, and then it can be shown that $p = a^2 + b^2$. This is the classical argument proving that an odd prime number can be expressed as sum of two squares if and only if it is congruent to 1 modulo 4.

For every imaginary quadratic field L, we claim that $\mathbf{Z}_L^\times$ is finite. Indeed, $\mathbf{Z}_L$ is a discrete subgroup of $L_{\mathbf{R}} = \mathbf{C}$. The group of inevrtible elements $\mathbf{Z}_L^\times$ is the intersection of $\mathbf{Z}_L$ with the unit circle $\mathbf{C}^1$ which is compact. This intersection is necessarily finite since it is both discrete and compact.

Let us consider now a real quadratic field $L = \mathbf{Q}[x]/(x^2 - d)$ where d is a positive square free integer. Then $L_{\mathbf{R}}$ splits into product of two copies of $\mathbf{R}$ corresponding to two different embeddings $L \to \mathbf{R}$ mapping x on $\pm\sqrt{d}$. The ring of integers $\mathbf{Z}_L$ contains $\{a+bx, a, b \in \mathbf{Z}\}$ as subgroup of index one or two. It is embedded in $L_{\mathbf{R}}$ by mapping $a + bx$ on $(a + b\sqrt{d}, a - b\sqrt{d})$. The group of invertible elements $\mathbf{Z}_L$ is the intersection of the image of $\mathbf{Z}_L$ in $L_{\mathbf{R}}$ with the union of hyperbolas $H_\pm = \{(u,v) \in \mathbf{R}^2; uv = \pm 1\}$.

We claim that $\mathbf{Z}_L^\times = \tau \times \mathbf{Z}$ where τ is a torsion group. First, $\mathbf{Z}_L$ is a discrete subgroup of $L_{\mathbf{R}} = \mathbf{R}^2$, its intersection with the hyperbolas $H_\pm$ is a discrete subset of $H_\pm$. It is in fact a discrete subgroup of $H_\pm$ with respect to coordinate wise multiplication. It follows that the free rank of $\mathbf{Z}_L^\times$ is no more than one. In order to prove that the free rank on $\mathbf{Z}_L^\times$ is equal to one, one prove that there exists a positive constant c such that

$$H_\pm \subset \bigcup_{\alpha \in \mathbf{Z}_L^\times} \alpha B_c$$

where $B_c = \{(u,v) \in \mathbf{R}^2; |u| \leq c \text{ and } |v| \leq c\}$. One can recognize the classical argument permitting a description of the set of solutions of the Pell equation $a^2 - db^2 = 1$. As we will see, this argument can be generalized

to prove the Dirichlet's theorem on the group of invertible elements in $\mathbf{Z}_L$ for every number field L.

7. Adèles and idèles for number fields

We will denote by $\bar{\mathscr{P}}_L = \mathscr{P}_L \cup \mathscr{P}_\infty$ the set of all places of L; $\mathscr{P}_L$ is the of nonarchimedean places and $\mathscr{P}_\infty$ the set of archimedean places. If we denote by $\mathbf{Z}_L$ the ring of integers in L, the set of nonarchimedean places of L can be identified with the set $\mathscr{P}_L = \mathscr{P}(\mathbf{Z}_L)$ of maximal ideals in $\mathbf{Z}_L$, see 5.3. For every $v \in \mathscr{P}_L$, we will denote by L_v the completion of L at v and $\mathscr{O}_v$ its ring of integers. The set of archimedean places of a number field L is in bijection with the set of factors in the decomposition of $L_{\mathbf{R}} = L \otimes_{\mathbf{Q}} \mathbf{R}$ as product of fields, see 4.3

$$L_{\mathbf{R}} = \prod_{u \in \mathscr{P}_\infty} L_u,$$

where the completion of L at the place $u \in S_\infty$ is denoted by L_u; it can be either $\mathbf{R}$ or $\mathbf{C}$. The real vector space $L_{\mathbf{R}}$ is called the Minkowski space of L.

An **adèle** of L is a sequence $(x_v; v \in \bar{\mathscr{P}}_L)$ where $x_v \in L_v$ for all places and $x_v \in \mathscr{O}_v$ for almost all nonarchimedean places. The **ring of adèles** $\mathbf{A}_L$ of L can be factorized as a direct product

$$\mathbf{A}_L = L_{\mathbf{R}} \times \mathbf{A}_{L,\mathrm{fin}}$$

where the ring of finite adèles $\mathbf{A}_{L,\mathrm{fin}}$ is the ring of all sequences $(x_v; v \in \mathscr{P}_L)$ where $x_v \in L_v$ for all $v \in \mathscr{P}_L$ and $x_v \in \mathscr{O}_v$ for almost all v. The ring of finite adèles can be seen as a direct limit of smaller subrings

$$\mathbf{A}_{L,\mathrm{fin}} = \varinjlim \mathbf{A}_{L,S} \tag{7.1}$$

over all finite subsets $S \subset \mathscr{P}_L$ where $\mathbf{A}_{L,S}$ is the subring of $\mathbf{A}_L$ of adeles (x_v) such that $x_v \in \mathscr{O}_v$ for all nonarchimedean place $v \notin S$. We have

$$\mathbf{A}_{L,S} = \prod_{v \in \mathscr{P}_L - S} \mathscr{O}_v \times \prod_{v \in S} L_v.$$

If we denote by R_S the localization of $\mathbf{Z}_L$ away forom S, then the set of maximal ideal $\mathscr{P}(R_S)$ is $\mathscr{P}_L - S$, and we have

$$\prod_{v \in \mathscr{P}_L - S} \mathscr{O}_v = \varprojlim_N R_S/N = \hat{R}_S$$

where the projective limit is taken over the set of nonzero ideals N of R_S ordered by inclusion relation. It follows that

$$\mathbf{A}_{L,S} = \hat{R}_S \times \prod_{v \in S} L_v.$$

We note that $\hat{R}_S$ is compact as projective limit of finite sets.

For all finite subsets $S \subset \mathscr{P}_L$, let us equip $\mathbf{A}_{L,S}$ with the product topology which is the coarsest one such that the projection to every factor is continuous. We will equip $\mathbf{A}_L$ with the finest topology on $\mathbf{A}_L$ such that for every finite subset S of $\mathscr{P}_L$, the inclusion $\mathbf{A}_{L,S} \to \mathbf{A}_L$ is continuous. A base of the topology of $\mathbf{A}_L$ consists of open subsets of the form $U_{S,\infty} \times \prod_{v \notin S} \mathscr{O}_v$ where S is a finite subset of $\mathscr{P}_L$ and $U_{S,\infty}$ is an open subsets of $\prod_{v \in S \cup \mathscr{P}_\infty} L_v$.

We claim that $\mathbf{A}_L$ is locally compact. Indeed we can construct a compact neighborhood of 0 with boxes that will prove to be useful for other purposes. The size of a box is given by a sequence of positive real integers $c = (c_v; v \in \bar{\mathscr{P}}_L)$ with $c_v = 1$ for almost all v. The **box** B_c of size c around 0 is the subset of $\mathbb{A}_L$ of all sequences $(x_v; v \in \bar{\mathscr{P}}_L)$ with $x_v \in L_v$ satisfying $|x_v| \leq c_v$ for every place $v \in \bar{\mathscr{P}}_L$. Since the subset of L_v defined by the inequality $|x_v| \leq c_v$ is compact, the product B_c is compact according to Tychonov's theorem.

For S being the empty set, we have $A_\emptyset = \mathbf{Z}_L$, and therefore $\mathbf{A}_{L,\emptyset} = \hat{\mathbf{Z}}_L$. The ring of finite adèles can also be described as

$$\mathbf{A}_{L,\mathrm{fin}} = \hat{\mathbf{Z}}_L \otimes_{\mathbf{Z}} \mathbf{Q} \tag{7.2}$$

by the same argument as in the particular case of the field of rational numbers.

THEOREM 7.1. *The ring $\mathbf{A}_L$ of adèles of L is locally compact for all number fields L. The field L embeds diagonally in $\mathbf{A}_L$ as a discrete cocompact subgroup. More precisely, the quotient $\mathbf{A}_L/L$ can be identified with a profinite covering of $L_{\mathbf{R}}/\mathbf{Z}_L$.*

PROOF. Let us consider the box B_c of size (c_v) with $c_v = 1$ for all nonarchimedean places v. This is a compact neighborhood of 0 in $\mathbf{A}_L$ whose intersection with L is finite. Indeed, if $\alpha \in L \cap B_c$ then $\alpha \in \mathbf{Z}_L$ for $\alpha \in \mathscr{O}_v$ for all $v \in \mathscr{P}_L$. It follows that α satisfies the equation $\alpha^r + a_1\alpha^{r-1} + \cdots + a_r = 0$ where r is the degree of $L/\mathbf{Q}$ and $\alpha_i \in \mathbf{Z}$. Now the integers a_i can be expressed as elementary symmetric functions of variables $\phi(\alpha)$ where $\phi : L \to \mathbf{C}$ runs over the set of embeddings of L into the field of complex numbers. The real absolute value of a_i can be therefore bounded by a quantity depending on $(c_v; v \in \mathscr{P}_\infty)$. There are thus only finitely many possible integers a_i, and this infers the finiteness of $L \cap B_c$. The same argument shows that $L \cap B_c = \{0\}$ for small enough $(c_v; v \in \mathscr{P}_\infty)$. In other words, L is a discrete subgroup of $\mathbf{A}_L$.

There is an exact sequence

$$0 \to \hat{\mathbf{Z}}_L \times L_{\mathbf{R}} \to \mathbf{A}_L \to \bigoplus_{v \in \mathscr{P}_L} L_v/\mathscr{O}_v \to 0$$

where $\bigoplus_{v\in\mathscr{P}_L} L_v/\mathscr{O}_v$ is the subgroup of $\prod_{v\in\mathscr{P}_L} L_v/\mathscr{O}_v$ consisting of sequence (x_v) with members $x_v \in \mathbf{Q}_v/\mathbf{Z}_v$ vanishing for almost all $v \in \mathscr{P}_L$. Consider now the homomorphism between two exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & L & \longrightarrow & L & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \hat{\mathbf{Z}}_L \times L_{\mathbf{R}} & \longrightarrow & \mathbf{A}_L & \longrightarrow & \bigoplus_{v\in\mathscr{P}_L} L_v/\mathscr{O}_v & \longrightarrow & 0 \end{array}$$

Since the middle vertical arrow is injective and the right vertical arrow is surjective with kernel $\mathbf{Z}$, the snake lemma infers an exact sequence

$$0 \to \mathbf{Z}_L \to \hat{\mathbf{Z}}_L \times L_{\mathbf{R}} \to \mathbf{A}_L/L \to 0,$$

$\mathbf{Z}$ being diagonally embedded in $\hat{\mathbf{Z}}\times\mathbf{R}$. In other words, there is a canonical isomorphism

$$\mathbf{Z}_L/L \to \left(\hat{\mathbf{Z}}_L \times L_{\mathbf{R}}\right)/\mathbf{Z}_L \tag{7.3}$$

Dividing both side by $\hat{\mathbf{Z}}_L$, one gets an isomorphism

$$\mathbf{A}_L/(\mathbf{Q}+\hat{\mathbf{Z}}_L) \to L_{\mathbf{R}}/\mathbf{Z}_L. \tag{7.4}$$

As we have seen that $L_{\mathbf{R}} = L\otimes_Q \mathbf{R} = \mathbf{Z}_L \otimes_{\mathbf{Z}} \mathbf{R}$, the quotient $L_R/\mathbf{Z}_L$ is homeomorphic to a product of r circles, and in particular it is compact. Furthermore, for every finite index subgroup K of $\hat{Z}_L$ the quotient $\mathbf{A}_L/(L+K)$ is a finite covering of the torus $L_{\mathbf{R}}/\mathbf{Z}_L$, and therefore $\mathbf{A}_L/L$ is a profinite covering of $L_{\mathbf{R}}/\mathbf{Z}_L$. In particular, it is compact.

As for the compactness of $\mathbf{A}_L/L$, one can also argue as follows. Let $\alpha_1,\ldots,\alpha_r$ be a basis of the $\mathbf{Q}$-vector space L. With this choice being made, L can be identified with $\mathbf{Q}^r$ and $\mathbf{A}_L$ with $\mathbf{A}^r$, and consequently

$$\mathbf{A}_L/L = (\mathbf{A}/\mathbf{Q})^r$$

and therefore $\mathbf{A}_L/L$ is compact. □

Let us now introduce the notion of **idèles in number fields**. An idèle of L is a sequence $(x_v, v\in\bar{\mathscr{P}}_L)$, v being finite or infinite place of L, consisting of $x_v \in L_v^\times$ with $x_v \in \mathscr{O}_v^\times$ for almost all finite places. The group of idèles $\mathbb{A}_L^\times$ is nothing but the group of invertible elements in the ring of adèles $\mathbb{A}_L$. It is equipped with the coarsest topology permitting the inclusion $\mathbb{A}_L^\times \subset \mathbb{A}_L$ as well as the inversion $\mathbb{A}_L^\times \to \mathbb{A}_L, x\mapsto x^{-1}$ to be continuous. A base of the topology of $\mathbf{A}_L^\times$ consists of open subsets of the form $U_{S\cup\mathscr{P}_\infty}\times\prod_{\mathscr{P}_L-S}\mathscr{O}_v^\times$ where S is a finite subset of $\mathscr{P}_L$ and $U_{S\cup\mathscr{P}_\infty}$ is an open subset in $\prod_{v\in S\cup\mathscr{P}_\infty} L_v^\times$.

The group of idèles $\mathbf{A}_L^\times$ is equipped with a norm

$$\|.\|_L : \mathbf{A}_L^\times \to \mathbf{R}_+$$

defined by

$$\|x\|_L = \prod_{v\in\mathscr{P}_L\cup\mathscr{P}_\infty} \|x_v\|_v$$

for all idèles $x = (x_v; v \in \bar{\mathscr{P}}_L) \in \mathbf{A}_L^\times$. For almost all finite places v, $\|x_v\|_v = 1$ so that the infinite product is well defined. The product formula (4.11) implies that the restriction of the norm to the diagonal subgroup $L^\times$ of $\mathbf{A}_L^\times$ is trivial.

Let denote by $\mathbf{A}_L^1$ the kernel of the norm $\|.\| : \mathbf{A}^\times \to \mathbf{R}_+$ in other words the group of norm one idèles. We have an exact sequence

$$1 \to \mathbf{A}_L^1 \to \mathbf{A}_L^\times \to \mathbf{R}_+ \to 1.$$

The group of idèles of norm one $\mathbf{A}_L^1$ is thus a closed subgroup of the group of idèles. We will equip it with the induced topology as closed subset of $\mathbf{A}^\times$. With respect to this topology, $\mathbf{A}_L^1$ is locally compact.

THEOREM 7.2. *The group of norm one idèles $\mathbf{A}_L^1$ contains $L^\times$ as discrete co-compact subgroup.*

Before starting the proof of this theorem, let us discuss its relation with classical finiteness theorems in algebraic number theory.

The group $\hat{\mathbf{Z}}_L^\times = \prod_{v\in\mathscr{P}_L} \mathscr{O}_v^\times$ can be embedded as compact subgroup of $\mathbf{A}_L^\times$ by setting all component at archimedean places to be one. We have an exact sequence

$$0 \to L_{\mathbf{R}}^\times \times \hat{\mathbf{Z}}_L^\times \to \mathbf{A}_L^\times \to \bigoplus_{v\mathscr{P}_L} L_v^\times/\mathscr{O}_v^\times \to 0$$

where $\bigoplus_{v\in\mathscr{P}_L} L_v^\times/\mathscr{O}_v^\times$ is the set of sequences $(n_v, v \in \mathscr{P}_L)$ with $n_v \in L_v^\times/\mathscr{O}_v^\times$, n_v vanish for almost all v. We observe that there is a canonical isomorphism between $L_v^\times/\mathscr{O}_v^\times$ and $\mathbf{Z}$ so that the n_v can be seen as integers.

Restricted to the norm one idèles, we have an exact sequence

$$0 \to L_{\mathbf{R}}^1 \times \hat{\mathbf{Z}}_L^\times \to \mathbf{A}_L^1 \to \bigoplus_{v\in\mathscr{P}_L} L_v^\times/\mathscr{O}_v^\times \to 0$$

where $L_{\mathbf{R}}^1 = L_{\mathbf{R}}^\times \cap \mathbf{A}_L^1$ is the subgroup of $L_{\mathbf{R}}^\times$ consisting of elements $(x_v; v \in \mathscr{P}_\infty)$, such that $\prod_{v\in\mathscr{P}_\infty} \|x_v\|_v = 1$. There is homomorphism of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & L^\times & \longrightarrow & L^\times & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L_{\mathbf{R}}^1 \times \hat{\mathbf{Z}}_L^\times & \longrightarrow & \mathbf{A}_L^1 & \longrightarrow & \bigoplus_{v\in\mathscr{P}_L} L_v^\times/\mathscr{O}_v^\times & \longrightarrow & 0 \end{array} \tag{7.5}$$

of which middle vertical arrow is injective. We observe that $\bigoplus_{v\in\mathscr{P}_L} L_v^\times/\mathscr{O}_v^\times$ is nothing but the group $\mathrm{Cl}^+(\mathbf{Z}_L)$ of fractional ideals of $\mathbf{Z}_L$. According to

5.8, the kernel of the right vertical map has kernel $L^\times \cap \hat{\mathbf{Z}}_L^\times = \mathbf{Z}_L^\times$ is the group $\mathbf{Z}_L^\times$ of invertible elements in $\mathbf{Z}_L$, and its cokernel is

$$\mathrm{Cl}_L = \Big(\bigoplus_{v \in \mathscr{P}_L} L_v^\times / \mathscr{O}_v^\times \Big) / L^\times .$$

the group of ideal classes $\mathrm{Cl}_L = \mathrm{Cl}(\mathbf{Z}_L)$ of L.

We derive from the exact sequence of complexes a long exact sequence

$$0 \to \left(\hat{\mathbf{Z}}_L^\times \times L_{\mathbf{R}}^1\right) / \mathbf{Z}_L^\times \to \mathbf{A}_L^1 / L^\times \to \mathrm{Cl}_L \to 0. \tag{7.6}$$

The group $\mathbf{A}_L^1 / L^\times$ is compact of and only if both $\left(\hat{\mathbf{Z}}_L^\times \times L_{\mathbf{R}}^1\right) / \mathbf{Z}_L^\times$ and Cl_L are compact. As Cl_L is discrete, it is compact if and only if it is finite. Since $\hat{\mathbf{Z}}_L^\times$ is compact, $\left(\hat{\mathbf{Z}}_L^\times \times L_{\mathbf{R}}^1\right) / \mathbf{Z}_L^\times$ if and only if $L_{\mathbf{R}}^1 / \mathbf{Z}_L^\times$ is compact. Now, we have a homomorphism with compact kernel

$$\log_{\mathscr{P}_\infty} : L_{\mathbf{R}}^\times \to \prod_{u \in \mathscr{P}_\infty} \mathbf{R}$$

mapping $(x_u; u \in \mathscr{P}_\infty)$ to $(y_u; u \in \mathbf{R})$ with $y_u = \log \|x_u\|_u$. The subgroup L_R^1 is the preimage of the hyperplane $H_{\mathbf{R}}$ in $\prod_{u \in \mathscr{P}_\infty} \mathbf{R}$ defined by the equation

$$\sum_{u \in \mathscr{P}_\infty} y_u = 0.$$

LEMMA 7.3. *The restriction of* $\log_{\mathscr{P}_\infty}$ *to* $\mathbf{Z}_L^\times$ *has finite kernel. Its image is a discrete subgroup of* $H_{\mathbf{R}}$.

PROOF. Both statement follows from 4.9. First, the kernel of $\log_{\mathscr{P}_\infty} : L_{\mathbf{R}}^1 \to H_{\mathbf{R}}$ is a compact group whose intersection with the discrete subgroup $\mathbf{Z}_L^\times$ is necessarily finite. Second, let U be a compact neighborhood of the neutral element of $L_{\mathbf{R}}^1$ such that $U \cap \mathbf{Z}_L^\times = \{1\}$. Because $\log_{\mathscr{P}_\infty}$ is proper, $\log_{\mathscr{P}_\infty}^{-1}(\log_{\mathscr{P}_\infty}(U))$ is a compact subset of $L_{\mathbf{R}}^1$ whose intersection with $\mathbf{Z}_L^\times$ is necessarily finite. It follows that $\log_{\mathscr{P}_\infty}(\mathbf{Z}_L^\times)$ has finite intersection with $\log_{\mathscr{P}_\infty}(U)$ which is a compact neighborhood of 0 in $H_{\mathbf{R}}$. □

Now, the quotient $L_{\mathbf{R}}^1 / \mathbf{Z}_L^\times$ is compact if and only if $H_{\mathbf{R}} / \log_{\mathscr{P}_\infty}(\mathbf{Z}_L^\times)$ is compact. According to the lemma, $\log_{\mathscr{P}_\infty}(\mathbf{Z}_L^\times)$ is a discrete subgroup of $H_{\mathbf{R}}$, and therefore its ranks is at most the real dimension of $H_{\mathbf{R}}$, namely $|\mathscr{P}_\infty| - 1$. The compactness of this quotient implies that the rank of $\log_{\mathscr{P}_\infty}(\mathbf{Z}_L^\times)$ is equal $|\mathscr{P}_\infty| - 1$. Thus the compactness of $\mathbf{A}_L^1 / L^\times$ implies both the finiteness of class number of L and Dirichlet's theorem on the rank of $\mathbf{Z}_L$. Conversely, if Cl_L is finite and $L_R^1 / \mathbf{Z}_L^\times$ is compact, then $\mathbf{A}_L^1 / L^\times$ is also compact.

We also observe that the same argument applies when we replace $\mathbf{Z}_L$ by its localization R_S away from a finite set of places $S \subset \mathscr{P}_L$. We also have an exact sequence

$$0 \to \left(\hat{R}_S^\times \times \prod_{v \in S \cup \mathscr{P}_\infty}^1 L_v^\times \right) / R_S^\times \to \mathbf{A}_L^1 / L^\times \to \mathrm{Cl}(R_S) \to 0$$

where $\prod^1_{v\in S\cup\mathscr{P}_\infty} L_v^\times$ is the subgroup of $\prod_{v\in S\cup\mathscr{P}_\infty} L_v^\times$ consisting of elements $(x_v; v\in S\cup\mathscr{P}_\infty)$ such that $\prod_{v\in S\cup\mathscr{P}_\infty}\|x_v\|_v = 1$. For all finite subset S of $\mathscr{P}_L$, the compactness of $\mathbf{A}_L^1/L^\times$ is equivalent to the finiteness of $\mathrm{Cl}(R_S)$ and the compactness of the quotient $(\prod_{v\in S\cup\mathscr{P}_\infty} L_v^\times)/R_S^\times$ combined. We note that the compactness of the latter implies that the group $R_S^\times$ is a finitely generated abelian group of rank $|S\cup\mathscr{P}_\infty|-1$.

We observe in particular that the conjunction of the finiteness of class number $\mathrm{Cl}(R_S)$ and the compactness of $(\prod_{v\in S\cup\mathscr{P}_\infty} L_v^\times)/R_S^\times$ is a statement independent of the choice of the finite subset S of $\mathscr{P}_L$.

PROOF. (of Theorem 7.2) The discreteness of $L^\times$ as subgroup of $\mathbf{A}_L^\times$ can be proved in the same manner as the discreteness of L in $\mathbf{A}_L$ in Theorem 7.1.

For proving the discreteness of L as subgroup of $\mathbf{A}_L$, we used the fact that the intersection of L with a box B_c is a finite set which is even reduced to 0 if c is set to be small. There is a converse to this namely if c is set to be large then $B_c\cap L\neq\{0\}$. The proof of the following lemma is postponed to 3.4 after the discussion on Haar measure. This is an adelic variant of Minskowski's theorem on symmetrical convex set in Euclidean space.

LEMMA 7.4 (Minkowski). *There exists a constant $C>0$, depending only on the discriminant of L, such that for all sequences $c=(c_v; v\in\bar{\mathscr{P}}_L)$ of positive real numbers c_v with $c_v=1$ for almost all v satisfying $\prod_v c_v > C$, the intersection $L^\times$ with $B_c=\{x=(x_v)\in\mathbf{A}_L, \|x_v\|\leq c_v\}$ is not empty.*

Admitting this lemma for the moment, we will now complete the proof of Theorem 7.2. Let B_c be the box associated to a sequence $c=(c_v; v\in\bar{\mathscr{P}}_L)$ of positive real numbers satisfying $\prod_v c_v > C$ as above. We claim that

$$\mathbf{A}_L^1 \subset \bigcup_{\alpha\in L^\times} \alpha B_c. \tag{7.7}$$

Indeed if $x\in\mathbf{A}_L^1$, $x^{-1}B_c$ is also a box $B_{c'}$ with $c'_v = \|x_v\|_v^{-1}c_v$ for all $v\in\bar{\mathscr{P}}_L$ satisfying $\prod_v c'_v = \prod_v c_v$. By Minkowski's Lemma 7.4, we know that there exists an element $\alpha\in B_{c'}\cap L^\times$. But if $\alpha\in x^{-1}B_c$ then $x\in\alpha^{-1}B_c$ and therefore the inclusion (7.7) is proved. It remains to prove that $B_c\cap\mathbf{A}_L^1$ is compact subset of $\mathbf{A}_L^1$, as asserted by the following lemma. □

LEMMA 7.5. *The intersection $B_c\cap\mathbf{A}_L^1$ is compact subset of $\mathbf{A}_L^1$.*

PROOF. Since B_c is a compact subset of $\mathbf{A}_L$, it is enough to prove that $\mathbf{A}_L^1$ is a closed subset of $\mathbf{A}_L$ and $\mathbf{A}_L$ and $\mathbf{A}_L^\times$ induce on $\mathbf{A}_L^1$ the same topology.

First we prove that the complement $\mathbf{A}_L^1$ in $\mathbf{A}_L$ is an open subset of $\mathbf{A}_L$. We will construct for each $x\in\mathbf{A}_L-\mathbf{A}_L^1$ an open neighborhood U in $\mathbf{A}_L$ which has no intersection with $\mathbf{A}_L^1$. We will divide the problem in three cases:

(1) If $x = (x_v) \in \mathbf{A}_L - \mathbf{A}_L^\times$, then $x_v \in \mathscr{O}_v$ for almost all places $v \in \mathscr{P}_v$ but $x_v \notin \mathscr{O}_v^\times$ for infinitely many places. In this case, the infinite product $\prod_{v\in\bar{\mathscr{P}}_v} \|x_v\|_v$ converges to zero. Then there exists then a finite set $S \subset \mathscr{P}$ such that $x_v \in \mathscr{O}_v$ for all $v \notin S$, and $\prod_{v\in S\cup\mathscr{P}_\infty} \|x_v\|_v < 1$. We will set U to be $\prod_{v\in S\cup\mathscr{P}_\infty} U_v \times \prod_{v\in\mathscr{P}-S} \mathscr{O}_v$ where U_v is the subset of $u_v \in L_v$ such that $\|u_v\| < \|x_v\| + \epsilon$ for a small positive real number ϵ. If ϵ is small enough, for all $u \in U$, either $u \notin \mathbf{A}_L^\times$ or $u \in \mathbf{A}_L^\times$ and $\|u\| < 1$.
(2) If $x = (x_v) \in \mathbf{A}_L^\times$ and $\|x\| < 1$, the same argument works.
(3) In the case $x = (x_v) \in \mathbf{A}_L^\times$ and $\|x\| > 1$, the argument needs to be refined. Let S be a finite subset of $\mathscr{P}_L$ such that for all non archimedean place $v \notin S$, we have $x_v \in \mathscr{O}_v^\times$. By enlarging S, we can also assume that for all $v \in \mathscr{P}_v - S$, $q_v > \|x\|$ where q_v denote the cardinal of the residue field of v. We will set U to be $\prod_{v\in S\cup\mathscr{P}_\infty} U_v \times \prod_{v\in\mathscr{P}-S} \mathscr{O}_v$ where U_v is the subset of $u_v \in L_v$ such that $\|x_v\| - \epsilon < \|u_v\| < \|x_v\| + \epsilon$ for a small positive real number ϵ. We claim that for ϵ small enough $U \cap \mathbf{A}_L^1 = \emptyset$. In fact, if $u = (u_v) \in U$, if $\|u_v\| = 1$ for all $v \in \mathscr{P}_L - S$, we will have $\|u\| > 1$, and in contrast if there exists al least one place $v \in \mathscr{P}_L - S$ such that $\|u_v\| < 1$ then $\|u_v\| \leq q_v^{-1}$ and we will have $\|u\| < 1$.

Second we prove that $\mathbf{A}_L$ and $\mathbf{A}_L^\times$ induce on $\mathbf{A}_L^1$ the same topology. For all open subset V of $\mathbf{A}_L$, $V \cap \mathbf{A}_L^\times$ is an open subset of $\mathbf{A}_L^\times$. It follows that the topology induced by $\mathbf{A}_L$ on $\mathbf{A}_L^1$ is coarser than the one induced by $\mathbf{A}_L^1$. The converse direction amounts to prove that for all open subset U of $\mathbf{A}_L^\times$, there exists an open subset V of $\mathbf{A}_L$ such that $U \cap \mathbf{A}_L^1 = V \cap \mathbf{A}_L^1$.

We can assume that U is of the form $U = \prod_{v\in S\cup\mathscr{P}_\infty} U_v \times \prod_{v\in\mathscr{P}_L-S} \mathscr{O}_v^\times$ where S is a finite subset of $\mathscr{P}_L$ and U_v is an open subset of $L_v^\times$ for every $v \in S \cup \mathscr{P}_\infty$. We can further assume that for all $v \in S \cup \mathscr{P}_\infty$, the norm $\|.\|_v$ is bounded on U_v, and consequently $\|u\| < C$ for some constant C for all $u \in U$. By enlarging S if necessary, we can assume that for all $v \in \mathscr{P}_L - S$, $q_v > C$ where q_v is the cardinal of the residue field at v. In these circumstances, we set $V = \prod_{v\in S\cup\mathscr{P}_\infty} U_v \times_{v\in\mathscr{P}_L-S} \mathscr{O}_v$, and we can prove that $U \cap \mathbf{A}_L^1 = V \cap \mathbf{A}_L^1$ by the same argument as in the third case above. □

One may observe that the main ingredient in the proof of Lemma 7.5 is the finiteness of the number of prime ideals whose norm is no greater than a given number. This is hardly surprising because the same ingredient plays also a crucial in the proof of Dirichlet's theorem on the group of units, and in particular in the study of the solution of Pell's equation.

A. Compactness

B. Local rings

C. Bibliographical comments

D. Exercices

EXERCICE 1. Construct an isomorphism of topological rings between the ring of p-adic integers $\mathbf{Z}_p$ and $\mathbf{Z}[[x]]/(x-p)$.

EXERCICE 2. Let $P \in \mathbf{Z}_p[x]$ be a monic polynomial $P = x^n + a_1 x^{n-1} + \cdots + a_n$ such that $\bar{P} = x^n + \bar{a}_1 x^{n-1} + \cdots \bar{a}_n \in \mathbf{F}_p[x]$, $\bar{a}_i$ being the image of a_i in $\mathbf{F}_p$, has a simple zero $\bar{\alpha} \in \mathbf{F}_p$. Prove that there exists P has a zero $\alpha \in \mathbf{F}_p$ of which image in $\mathbf{F}_p$ is $\bar{\alpha}$.

EXERCICE 3. Answer the following questions and justify your answers.

(1) Is $\prod_{p\in\mathscr{P}} p\mathbf{Z}_p$ an open subset of $\mathbf{A}_{\text{fin}}$? Is it an closed subset? Is it compact?
(2) Is $\mathbf{A}_{\text{fin}} \cap \prod_{p\in\mathscr{P}} p^{-1}\mathbf{Z}_p$ an open subset of $\mathbf{A}_{\text{fin}}$? Is is a closed subset? Is is compact?

EXERCICE 4. Let d be a square free integer and $L = \mathbf{Q}[x]/(x^2-d)$. Find a $\mathbf{Z}$-basis of the ring of integers $\mathbf{Z}_L$ and calculate the absolute discriminant of L.

EXERCICE 5. Let p be a prime number. Prove that the polynomial $\Phi_p = 1 + x + \cdots + x^{p-1} \in \mathbf{Q}[x]$ is irreducible. Calculate the absolute discriminant of $L = \mathbf{Q}[x]/\Phi_p$.

EXERCICE 6. Let d be a square free integer, $L = \mathbf{Q}[x]/(x^2-d)$. Let p be a prime number not dividing $2d$. Show that $p\mathbf{Z}_L$ is a prime ideal if and only if the congruence $x^2 \cong d \mod p$ has no solution.

EXERCICE 7. Let $R = \mathbf{C}[x,y]/(x^2-y^3)$. Construct a torsion free R-module which is not locally free.

EXERCICE 8. Let R be a Dedekind domain and let $\mathfrak{a}$ be a nonzero ideal. Prove that $A/\mathfrak{a}$ is a principal ideal ring. Prove that all ideal of a Dedekind domain can be generated by two elements.

EXERCICE 9. Let $\rho \in \mathbf{C}$ be a solution of the equation $\rho^2 + \rho + 1 = 0$. Define the Eisenstein integers as the set

$$\mathbf{Z}[\rho] = \{a + b\rho; a, b \in \mathbf{Z}\}.$$

Show that $\mathbf{Z}[\rho]$ is an euclidean ring, and its group of units is $\{\pm 1, \pm\rho, \pm\rho^2\}$.

Let $\lambda = 1 - \rho$. Show that (λ) is a maximal ideal. Decompose (3) as product of maximal ideals in $\mathbf{Z}[\rho]$.

Show that if $\theta \notin (\lambda)$ then $\theta^3 \equiv \pm 1 \mod \lambda^4$. Deduce that if α, β, γ are coprime to λ then the equation $\alpha^3 + \beta^3 + \gamma^3 = 0$ has no solutions.

EXERCICE 10. Prove that for a every number field, there exists a constant H_L such that for every $\alpha \in L$ there exists a nonzero integer t with $|t| \leq H_L$ and $\beta \in \mathbf{Z}_L$ an integral element of L such that $|t\alpha - \beta| < 1$. For Euclidean domain, one can take $H_L = 1$.

Prove that for every ideal $\mathfrak{a} \subset \mathbf{Z}_L$, there exists an ideal $\mathfrak{b} \subset \mathscr{O}_L$ equivalent to $\mathfrak{a}$ in the sens there exists $\alpha \in L^\times$ such that $\mathfrak{b} = \alpha\mathfrak{a}$, satisfying $|\mathbf{Z}_L/\mathfrak{b}| \leq H_L$.

For $L = \mathbf{Q}[\sqrt{-5}]$, prove that one can take $H_L = (1+\sqrt{5})^2$. Factorize $(2), (3), (5)$ and (7) as product of maximal ideals in $\mathbf{Z}_L$. Calculate the class number of L.

EXERCICE 11. Let d be a negative square free integer congruent to 1 modulo 4, $K = \mathbf{Q}[\sqrt{d}]$ and R its ring of integers. Let $\mathrm{Cl}(R)$ the group of isomorphism classes invertible modules.

An integral quadratic form is a function $q(x,y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbf{Z}$, and its discriminant is $b^2 - 4ac$. The group $\mathrm{SL}_2(\mathbf{Z})$ acts on the free module $\mathbf{Z}x \oplus \mathbf{Z}y$ and thus on the set of quadratic forms; this action preserves ths discriminant. Prove that if d is negative square free integer congruent to 1 modulo 4, the set of integral quadratic forms of discriminant d modulo $\mathrm{SL}_2(\mathbf{Z})$-equivalence is in bijection with $\mathrm{Cl}(R)$.

A integral quadratic form $q(x,y) = ax^2 + bxy + cy^2$ of discriminant $d < 0$ is said to be reduced if $|b| \leq a \leq c$ and if either $|b| = a$ or $a = c$ then $b \geq 0$. Then in each $\mathrm{SL}_2(\mathbf{Z})$-equivalence class of quadratic form of discriminant $d < 0$, there is exactly on reduced form.

Calculate class number $h_d = |\mathrm{Cl}(R)|$ for $d \equiv 1 \mod 4$ and $-20 < d < 0$.

EXERCICE 12. Let L be a number field of absolute discriminant d. A place v of L over p is said to be ramified if p is not a prime element in the ring of integers $\mathscr{O}_v$ of L_v. Prove that there is a place $v|v$ ramified if and only if $p|d$.

EXERCICE 13. There are only finitely many number field of degree less than r and of discriminant less than d for given integers $r, d \in \mathbf{N}$.

The proof of Proposition 5.2 follows [**?**, I.2].

CHAPTER 2

Invariant measures

1. Radon measures

We recall that a topological space is locally compact if every element possesses a compact neighborhood. A topological group is locally compact if its unit possesses a compact neighborhood.

If X is a locally compact topological space and K is a compact subset of X, we will denote $C_K(X)$ the space of complex valued continuous functions on X vanishing on $X-K$. For this definition not to be trivial in other words there is a function $f \in C_K(x)$ not vanishing at certain point $x \in X$, K has to be a compact neighborhood of x. For every $f \in C_K(X)$, the sup norm $|f|_{\sup} = \sup_{x\in K} f(x)$ is well defined positive real number. The sup norm equip $C_K(X)$ with a structure of Banach space.

The space $C_c(X)$ of continuous functions with compact support is the union of all spaces $C_K(X)$ for K running over the set of compact subsets of X. It is equipped with the finest topology still permitting all inclusions $C_K(X) \to C_c(X)$ to be continuous. A continuous linear functional on $C_c(X)$ is a linear form $C_c(X) \to \mathbf{C}$ whose restriction to all subspaces $C_K(X)$ is continuous.

A **Radon functional** is a continuous linear functional μ on the space $C_c(X)$ of compactly supported continuous functions of a locally compact topological space X such that if $f \in C_c^+(X)$ is a non-zero positive function, then $\mu(f) > 0$.

Radon functional can be constructed as integration against a Radon measure. Consider the σ-algebra consisting of Borel sets in a topological spaces X. A Borel measure μ is said to be Radon if it is

(1) inner regular i.e. for all Borel set Y in X, $\mu(Y) = \sup_K\{\mu(K)\}$ when K runs over the set of all compact subsets of V,
(2) locally finite if every point has a neighborhood of finite measure.

Assume that X is locally compact and μ is a Radon measure on X. Then for every $f \in C_c(X)$ is integrable with respect to μ and the integral

$$f \mapsto \int_X f(x)\mathrm{d}\mu(x) \tag{1.1}$$

is a positive linear functional on $C_c(X)$.

THEOREM 1.1 (Riesz-Markov-Kakutani). *Let X be a locally compact topological space. Every positive linear form on $C_c(X)$ arises from a unique Radon measure by integration* (1.1).

We will use the symbol μ to denote both the Radon measure and the associated linear functional on $C_c(X)$, and employ the terminology of Radon functionals or Radon measures indistinctly. In the formula

$$\mu(f) = \int_X f(x)\mathrm{d}\mu(x)$$

the symbol μ in the left hand side is to be understood as a Radon functional on $C_c(X)$, and the symbol μ in the right has side is to be understood as a Radon measure.

2. Haar measure

Let us start by recalling some self-evident definitions. A topological group is a topological space equipped with a group structure of which the composition and the inverse are both continuous. In particular, the underlying topology is preserved by the left and right translations as well as the inverse. We will denote $l_x(y) = xy$ the left translation by $x \in G$ and $r_x(y) = yx^{-1}$ the right translation.

We define left and right translations on functions, and on functions with compact support, by the formula $(l_x f)(y) = f(x^{-1}y)$ and $(r_x f)(y) = f(yx)$. We define left and right translations on measures by the formula $(l_x\mu)(f) = \mu(l_{x^{-1}}f)$ and $(r_x\mu)(f) = \mu(r_{x^{-1}}f)$. A Radon measure μ on G is said to be left invariant if $l_x\mu = \mu$ for all $x \in G$. We have similar notion of right invariant Radon measures.

THEOREM 2.1 (Haar-von Neumann). *There exists a left-invariant Radon measure on every locally compact topological group. This measure is unique up to multiplication by a positive constant.*

PROOF. We first prove the **existence** of left-invariant Radon measure. Let $f, g \in C_c^+(G)$ be non-zero positive functions. The ratio $\mu(f) : \mu(g)$, where μ is the invariant measure that we seek to define, must be bounded from above by the sums $\sum_{i=1}^n c_i$ where c_i are positive real numbers such that there exist elements $x_1, \ldots, x_n$ of G satisfying

$$f < \sum_{i=1}^n c_i l_{x_i}(g).$$

We define

$$(f : g) = \inf\left\{ \sum_{i=1}^n c_i \mid f < \sum_{i=1}^n c_i l_{x_i}(g) \right\}$$

to be the infimum of those numbers.

We have just defined a kind of "ratio" $(f : g)$ for all $f, g \in C_c^+(G)$. The purpose of the quote marks is to remind us that this is not a genuine ratio in the sense that there is a triangular inequality

$$(\varphi_1 : \varphi_3) \leq (\varphi_1 : \varphi_2)(\varphi_2 : \varphi_3) \tag{2.1}$$

for all non-zero $\varphi_i \in C_c^+(G)$ but no equality in general.

Let us choose a non-zero positive continuous function with compact support $f_0 \in C_c^+(G)$. We will prove that there exists a left-invariant Radon measure I such that $\mu(f_0) = 1$. We set

$$\nu_\varphi(f) = \frac{(f : \varphi)}{(f_0 : \varphi)} \tag{2.2}$$

We will define $\mu(f)$ as the limit of $\nu_\varphi(f)$ as the support of φ shrinks to an arbitrarily small neighborhood of identity. By its very construction ν_φ is invariant under left translation i.e. $\nu_\varphi(l_x f) = \nu_\varphi(f)$ for all $x \in G$ and $f \in C_c^+(G)$. It can also be easily checked that ν_φ satisfies the sub-additivity inequality

$$\nu_\varphi(f_1 + f_2) \leq \nu_\varphi(f_1) + \nu_\varphi(f_2) \tag{2.3}$$

but no equality in general. We will prove that by constructing an appropriate limit of ν_φ as the support of φ shrinks to an arbitrarily small neighborhood of identity, the inequality (2.3) will becomes an equality.

As the triangular inequality (2.1) implies lower and upper bound for ν_φ

$$\frac{1}{(f_0 : f)} \leq \nu_\varphi(f) \leq (f : f_0),$$

the sought after number $\mu(f)$ satisfies the same inequality. Let B_f denote the closed interval $[1/(f_0 : f), (f : f_0)]$. According to the Tychonov theorem, the infinite product

$$B = \prod_{f \in C_c^+(G)} B_f$$

is compact. For every $\varphi \in C_c^+(G)$, the function $f \mapsto \nu_\varphi(f)$ determines an element of $\nu_\varphi \in B$. For each neighborhood V of identity in G, let $\mathscr{J}_V$ denote the closure of the set $\{\nu_\varphi \mid \varphi \in C_c^+(V)\}$ in B. For any finite collection of neighborhoods of identity $V_1, \ldots, V_n$, the intersection $\mathscr{J}_{V_1} \cap \cdots \cap \mathscr{J}_{V_n}$ is non-empty because we can find a function φ with support contained in $V_1 \cap \cdots \cap V_n$. Since B is compact, the intersection of $\mathscr{J}_V$ for all neighborhood V of identity is non-empty. Let I be an element of this intersection. We will prove that I can be extended a left-invariant Radon measure of G.

Since ν_φ is invariant under left translation i.e. $\nu_\varphi(l_x f) = \nu_\varphi(f)$ for all $x \in G$ and $f \in C_c^+(G)$, I satisfies the same invariant property. We only need to prove that I is additive for positive functions i.e. $\mu(f_1 + f_2) =$

$\mu(f_1)+\mu(f_2)$ for all $f_1, f_2 \in C_c^+(G)$. The extension of $\mu(f)$ to all function $f \in C_c(G)$ is then guaranteed because every continuous function with compact support can be written as the difference of two positive continuous functions with compact support. The existence of Haar measure would now derive from the following lemma.

LEMMA 2.2. *If $I \in \bigcap_V \mathscr{J}_V$ with V running over all neighborhood of identity in G, then $\mu(f_1+f_2)=\mu(f_1)+\mu(f_2)$ for all $f_1, f_2 \in C_c^+(G)$.*

PROOF. For every non-zero positive function φ, ν_φ satisfies the subadditivity inequality

$$\nu_\varphi(f_1+f_2) \leq \nu_\varphi(f_1)+\nu_\varphi(f_2)$$

according to its very definition. Since μ lies in the closure of the ν_φ, it satisfies the same inequality.

We will prove now the opposite inequality

$$\mu(f_1)+\mu(f_2) \leq \mu(f_1+f_2)$$

for every $f_1, f_2 \in C_c^+(G)$. Let us choose an auxiliary $f' \in C_c^+(G)$ that takes value 1 on the union of supports of f_1 and f_2. We will prove that the inequality

$$\mu(f_1)+\mu(f_2) \leq (1+2\epsilon)(\mu(f_1+f_2)+\delta\mu(f')) \tag{2.4}$$

holds for all $\delta, \epsilon > 0$.

Let $f = f_1+f_2+\delta f'$ for some positive real number δ. Set $h_i(x) = \frac{f_i(x)}{f(x)}$ for x in the support of f_i and 0 otherwise. The non-vanishing of f' on the support of f_i implies that $h_i \in C_c^+(G)$ for $i \in \{1,2\}$. We have $f_i = f h_i$ and $h_1+h_2 < 1$.

The main ingredient that come into the proof of (2.4) is the **uniform continuity** of continuous compactly supported functions. The notion of uniform continuity depends upon group action, the right translation of G on itself in the present case. The functions h_i are right equicontinuous in the sense that for every $\epsilon > 0$ there exists a neighborhood V of identity such that for every $y \in V$ and $x \in G$, $|h_i(xy)-h_i(x)| < \epsilon$ for $i \in \{1,2\}$.

Let $\varphi \in C_c(V)$ and choose $c_1, \ldots, c_n$ and $x_1, \ldots, x_n$ such that

$$f < \sum_{j=1}^{n} c_j l_{x_j} \varphi.$$

The inequality $|h_1(xy)-h_1(x)| < \epsilon$ satisfied by $y \in V$ and $x \in G$ implies

$$f_i(y) = f(y)h_i(y) < \sum_{j=1}^{n} c_j (h_i(x_j)+\epsilon) l_{x_j}\varphi$$

hence

$$(f_i : \varphi) < \sum_{j=1}^{n} c_j (h_i(x_j) + \epsilon).$$

It follows that

$$(f_i : \varphi) + (f_2 : \varphi) < \sum_{j=1}^{n} c_j (1 + 2\epsilon).$$

Since $(f : \varphi)$ is defined as the infimum of numbers $\sum_{i=1}^{n} c_i$ obtained as above, we derives the inequality

$$(f_1 : \varphi) + (f_2 : \varphi) < (1 + 2\epsilon)(f : \varphi).$$

The inequality

$$\nu_\varphi(f_1) + \nu_\varphi(f_2) < (1 + 2\epsilon)(\nu_\varphi(f_1 + f_2) + \delta\nu_\varphi(f'))$$

is thus satisfied for all non-zero positive function $\varphi \in C_c^+(V)$. Since I belong to the closure of $\mathscr{J}_V$, this implies the inequality (2.4). □

We now turn to the proof of the **uniqueness** of invariant measure. Let μ and ν be two left-invariant Haar measures. For every positive, continuous compactly supported function $f, g \in C_c^+(G)$ we will prove that the difference between the ratios $\nu(f)/\mu(g)$ and $\nu(f)/\mu(f)$ is arbitrarily small using essesntially the equicontiuity of f and g their property of being left-invariant.

Consider a positive function $f \in C_c^+(G)$ supported on a compact set C and an auxiliary function $f' \in C_c^+(G)$ that takes value 1 on an open subset U containing C. For every $\epsilon > 0$, there is a symmetric neighborhood V of the identity such that $|f(x) - f(xy)| < \epsilon$ for all $x \in C$ and $y \in V$. We also require that $CV \subset U$. It follows from these assumptions that

$$|f(x) - f(xy)| \leq \epsilon f'(x) \tag{2.5}$$

for all $y \in V$. If x or xy lies in C, the inequality $|f(x) - f(xy)| < \epsilon$ is satisfied as we can replace y by y^{-1}. In this case $x \in C \cup CV \subset U$ so that $f'(x) = 1$. If neither x nor xy lies in C, the left hand side of (2.5) the above inequality vanishes while the right hand side is greater or equal to zero.

Let $h \in C_c^+(V)$ be any non-zero positive function supported in V. We also assume h symmetric $h(x) = h(x^{-1})$. We will prove that

$$\left| \frac{\nu(f)}{\mu(f)} - \frac{\nu(h)}{\mu(h)} \right| < \epsilon \frac{\nu(f')}{\mu(f)}. \tag{2.6}$$

We will introduce a temporary notation $\mu(h) = \mu_x h(x)$ where x is a silent variable. Thus on one hand, we write

$$\mu(h)\nu(f) = \mu_y \nu_x h(y) f(x)$$

and on the other hand, using Fubini theorem and the left invariance of I and J, we can rewrite $\nu(h)\mu(f)$ as

$$\nu(h)\mu(f) = \mu_y \nu_x h(x) f(y) = \mu_y \nu_x h(y^{-1}x) f(y).$$

Since $h(y^{-1}x) = h(x^{-1}y)$, this can also expressed as

$$\nu(h)\mu(f) = \nu_x \mu_y h(x^{-1}y) f(y) = \mu_y \nu_x h(y) f(xy).$$

The difference of $|\mu(h)\nu(f) - \nu(h)\mu(f)|$ can now be bounded

$$|\mu(h)\nu(f) - \nu(h)\mu(f)| = \mu_y \nu_x h(y) |f(x) - f(xy)| \leq \epsilon \mu_y \nu_x h(y) f'(x)$$

after (2.5). Therefore

$$|\mu(h)\nu(f) - \nu(h)\mu(f)| \leq \epsilon \mu(h)\nu(f')$$

The inequality (2.6) follows by getting multiplied on both sides with $\mu(f)\mu(h)$.

Let $g \in C_c^+(G)$ and if g' is an auxiliary function for g as f' for f. Then we have also an inequality

$$\left| \frac{\nu(g)}{\mu(g)} - \frac{\nu(h)}{\mu(h)} \right| < \epsilon \frac{\nu(g')}{\mu(g)}$$

for every symmetric positive function h supported in a small enough neighborhood V of the identity. Combining with (2.6), we get

$$\left| \frac{\nu(f)}{\mu(f)} - \frac{\nu(g)}{\mu(g)} \right| < \epsilon \left(\frac{\nu(f')}{\mu(f)} + \frac{\nu(g')}{\mu(g)} \right)$$

for every $\epsilon > 0$. We remember that only the support of h depends on the choice of ϵ, in letting $\epsilon \to 0$ in the above inequality we infer

$$\frac{\nu(f)}{\mu(f)} = \frac{\nu(g)}{\mu(g)}$$

for all $f, g \in C_c^+(G)$. It follows that $J = cI$ for some positive constant c. □

Invariant measures on locally compact groups are defined up to multiplication by a positive constant. It can be a tricky problem to find a **normalization of invariant measure**. For discrete or compact groups, there is however an obvious normalization.

If G is a discrete group, $C_c(G)$ consists of functions with finite support and the functional

$$f \mapsto \sum_{x \in G} f(x) \tag{2.7}$$

is an invariant measure, the counting measure. If G is a compact group, $C_c(G)$ is the space of all continuous functions on G. In particular, the constant function 1_G of value one belongs to this space. In this case, we can normalize the invariant measure $\mu : C(G) \to \mathbf{C}$ such that $\mu(1_G) = 1$,

in other words the total volume of G is equal to one with respect to the normalized invariant measure.

Let G be a locally compact group and H a closed subgroup of G, the quotient G/H is then a locally compact group. Let us be given an invariant measure μ_H on H and an invariant measure $\mu_{G/H}$ on the quotient G/H. Then one can define an invariant measure μ_G on G as follows: for every $f \in C_c(G)$, let $\mathrm{Av}_H(f)$ denote the function

$$\mathrm{Av}_H f(x) = \int_H f(xy) \mathrm{d}\mu_H(y)$$

which is a continuous function with copmact support of G/H. The linear functional

$$\mu_G(f) = \mu_{G/H}(\mathrm{Av}_H(f))$$

is then well defined and invariant; we will write in this case $\mu_G = \mu_{G/H}\mu_H$. This construction applies in particular when H is a discrete group and G/H is a compact group or vice versa. In these case, both H and G/H can be given canonical invariant measures that induce a an invariant measure on G. Of course this measure depends not only on G but on its realization as en extension of a compact group by a discrete group or vice versa.

3. Invariant measure on additive groups

We first consider invariant measures on the basic local fields, those that are obtained as completions of $\mathbf{Q}$ with respect to a valuation, and on the group of adèles of $\mathbf{Q}$.

Over the field of real numbers, we have the Lebesgue that assigns to the interval $[0,1]$ the measure one. For every prime number p, we will normalize the invariant measure on the field of p-adic numbers $\mathbf{Q}_p$ by assigning to the compact open subgroup $\mathbf{Z}_p$ the volume one.

The group of adèles $\mathbf{A}$ is an extension of the compact group $\mathbf{A}/\mathbf{Q}$ by the discrete subgroup $\mathbf{Q}$. We can normalize the invariant measure on $\mathbf{A}$ by the formula (**??**) using the invariant measure on $\mathbf{A}/\mathbf{Q}$ assigning to this compact group the total volume one. In other words, for every continuous function with compact support in $\mathbf{R}$, we have

$$\mu_{\mathbf{A}}(f) = \mu_{\mathbf{A}/\mathbf{Q}}(\mathrm{Av}_{\mathbf{Q}} f)$$

where $\mathrm{Av}_{\mathbf{Q}} f$ is the $\mathbf{Q}$-periodic function defined by

$$\mathrm{Av}_{\mathbf{Q}} f(x) = \sum_{n \in \mathbf{Q}} f(x+n),$$

and $\mu_{\mathbf{A}/\mathbf{Q}}$ is the invariant measure on $\mathbf{A}/\mathbf{Q}$ assigning to this compact group the total volume one. If f is the characteristic function of the box

$$B = \{x_v; |x_v|_v \leq 1 \text{ for all } v \in \mathscr{P}\} \times [0,1]$$

the average $\mathrm{Av}_Q f$ is equal to one almost everywhere as function on $\mathbf{A}/\mathbf{Q}$. It follows that the compact $\{x_v; |x_v|_v \leq 1 \text{ for all } v \in \mathscr{P}\} \times [0,1]$ is to be given the measure one, and more generally for all sequence of positive numbers $c = (c_\infty, c_p; p \in \mathscr{P})$ with $c_p = 1$ for almost all p, the volume of the box $B_c = \{x \in \mathbf{A}; \forall v \in \bar{\mathscr{P}}, |x_v|_v \leq c_v\}$ with respect to the measure $\mu_{\mathbf{A}}$, is equal to

$$\mathrm{vol}(B_c, \mu_A) = 2 \prod_{v \in \bar{\mathscr{P}}} c_v$$

in other words, equal to the product over all places of v of volumes of compact set defined by $|x_c| \leq c_v$ with respect to the normalized Haar measure on $\mathbf{Q}_v$.

Let F be a local field, finite extension of a basic local field $\mathbf{Q}_v$. We claim that F, as locally compact group, can be given a canonical invariant measure. More generally, we claim that every finite dimensional $\mathbf{Q}_v$-vector space equipped with a nondegenerate bilinear form can be given a normalized invariant measure. We will call **density** on V a function

$$\mathrm{d}: \bigwedge^r V \to \mathbf{R}_+ \text{ with } r = \dim_{\mathbf{Q}_v}(V)$$

such that for all $\alpha \in \mathbf{Q}_v$ and all $x \in \bigwedge^r V$ we have $\mathrm{d}(\alpha x) = |\alpha|_v \mathrm{d}(x)$. If V is equipped with a non degenerate bilinear form $q : V \otimes V \to \mathbf{Q}_v$ then $\bigwedge^r V$ is equipped with non degenerate bilinear form $\bigwedge^r q$ and we set

$$\mathrm{d}_q(x) = |\bigwedge^r q(x,x)|_v^{1/2}.$$

A density determine an invariant measure on V. Indeed, for each basis $x = (x_1, \ldots, x_r)$ of V, we have an isomorphism $\mathbf{Q}_v^r \to V$ by setting $(\alpha_1, \ldots, \alpha_r) \mapsto \alpha_1 x_1 + \cdots + \alpha_r x_r$, and then transpose the product measure of $\mathbf{Q}_v^r$ on V. We will denote μ_x the measure obtained that way. Given a density d on V, we set

$$\mu = \mathrm{d}_q(x_1 \wedge \cdots \wedge x_r)\mu_x.$$

This measure does not depend on the choice of basis x. If $x' = (x'_1, \ldots, x'_r)$ is another basis, there is a unique linear transformation $g : V \to V$ such that $x'_i = g(x_i)$ for all $i = 1, \ldots, n$. In this case, we have

$$\mathrm{d}_q(x_1 \wedge \cdots \wedge x_r) = |\det g|_v^{-1} \mathrm{d}_q(x'_1 \wedge \cdots \wedge x'_r) \text{ and } \mu_x = |\det g|_v \mu_{x'}.$$

If F is a finite extension of $\mathbf{Q}_v$, the trace form $q(x,y) = \mathrm{Tr}_{F/\mathbf{Q}_v}(xy)$ is a nondegenerate symmetric form on F as $\mathbf{Q}_v$-vector space. We will denote by μ_F the invariant measure defined with help of the trace form:

$$\mu_F = \mathrm{d}_q(x_1 \wedge \cdots \wedge x_r)\mu_x \tag{3.1}$$

where q is the trace form, and $x_1, \dots, x_r$ is any $\mathbf{Q}_v$-basis of F. Let us now calculate the canonical measure μ_F for different local fields.

LEMMA 3.1. *For $F = \mathbf{C}$ and $\mathbf{Q}_v = \mathbf{R}$, the measure of $B_1 = \{z \in \mathbf{C}, \|z\| \leq 1\}$ with respect to the normalized local measure $\mu_{\mathbf{C}}$ is equal to*

$$\mathrm{vol}(B_1) = 2\pi$$

PROOF. Let us pick the $\mathbf{R}$-basis x of $\mathbf{C}$ with $x_1 = 1$ and $x_2 = i$. The volume of B_1 with respect to μ_x is equal to π and $\mathrm{d}_q(x) = 2$. □

LEMMA 3.2. *Let F be a finite extension of $\mathbf{Q}_p$ of degree r. The volume of $\mathscr{O}_F = \{x \in F, \|x\| \leq 1\}$ with respect to the normalized local measure μ_F is*

$$\mathrm{vol}(\mathscr{O}_F) = \mathrm{discr}(F)^{-1/2}$$

where $\mathrm{discr}(F)$ *is the absolute discriminant of F.*

PROOF. By definition we have $\mathrm{discr}(F) = |\mathscr{O}_F^{\perp}/\mathscr{O}_F|$ where $\mathscr{O}_F^{\perp}$ is the $\mathbf{Z}_p$-submodule of F orthogonal to $\mathscr{O}_F$ with respect to the trace form $q(x,y) = \mathrm{Tr}_{F/\mathbf{Q}_p}(xy)$. If $x_1, \dots, x_r$ form a $\mathbf{Z}_p$-basis of $\mathscr{O}_F$ then we have

$$|(\textstyle\bigwedge^r q)(x_1 \wedge \cdots \wedge x_r, x_1 \wedge \cdots \wedge x_r)| = \mathrm{discr}(F)^{-1}$$

thus $\mathrm{vol}(\mathscr{O}_F) = \mathrm{discr}(F)^{-1/2}$. □

Let L be a number field, finite extension of $\mathbf{Q}$. We claim that $\mathbf{A}_L = L \otimes_{\mathbf{Q}} \mathbf{A}$, as locally compact group, can be given a canonical invariant measure. More generally, we claim that for every finite dimensional $\mathbf{Q}$-vector space V, $\mathbf{A}_V = V \otimes_{\mathbf{Q}} \mathbf{A}$ can be given a canonical invariant measure. For each basis $x = (x_1, \dots, x_n)$ of V, we have an isomorphism $\mathbf{Q}^n \simeq V$ that induces at each place $v \in \mathscr{P}$ an isomorphism $\mathbf{Q}_v^n \to V_v$ and over the adèles $\mathbf{A}^n \to \mathbf{A}_V$. Via these isomorphism, we can transport normalized invariant measures on $\mathbf{Q}_v^n$ and $\mathbf{A}^n$ over V_v and $\mathbf{A}_V$ respectively. If $x' = (x'_1, \dots, x'_n)$ is another basis, there is a unique linear transformation $g : V \to V$ such that $x'_i = g(x_i)$ for all $i = 1, \dots, n$. In this case, we have

$$\mu_v = |\det g|_v \mu'_{v'}$$

where μ_v, respectively μ'_v is the invariant measure on V_v defined with help of basis x, respectively x'. It follows from the product formula (7.3) in Chapter 1 that the measures defined on $V_{\mathbf{A}}$ by basis x and x' are the same

$$\mu = \mu' \prod_{v \in \bar{\mathscr{P}}} |\det g|_v = \mu'.$$

We can also justify this relation by observing that μ induces on the compact group $\mathbf{A}_V / V$ an invariant measure with total volume one and so does μ'. We will denote μ_L the **canonical measure on $\mathbf{A}_L$**.

PROPOSITION 3.3. *Let L be a number field. For every place $u \in \bar{\mathscr{P}}_L$, let μ_u denote the normalized local measure of L_u. Then the normalized adelic measure on $\mathbf{A}_L$ is equal to*

$$\mu_L = \bigotimes_{u \in \bar{\mathscr{P}}_L} \mu_u. \tag{3.2}$$

In particular, if for every sequence of positive real numbers $c = (c_u; u \in \bar{\mathscr{P}}_L)$ with $c_u = 1$ for almost all u, the volume of $B_c = \{(x_u) \in \mathbb{A}_L; \|x_u\|_u \leq c_u\}$ with respect to the normalized adelic measure μ_L is

$$\mathrm{vol}(B_c, \mu_L) = \frac{2^{m_{\mathbf{R}}}(2\pi)^{m_{\mathbf{C}}}}{\sqrt{\mathrm{discr}_L}} \prod_{u \in \bar{\mathscr{P}}_L} c_u \tag{3.3}$$

where discr_L is the absolute discriminant of L, $m_{\mathbf{R}}$ is the number of real places and $m_{\mathbf{C}}$ the number of complex places of L.

PROOF. Let $x = (x_1, \ldots, x_r)$ be a $\mathbf{Q}$-basis of L and let $\bigwedge^r x$ denote the vector $x_1 \wedge \cdots \wedge x_r \in \bigwedge^r V$. By construction $\mu_L = \otimes_{v \in \bar{\mathscr{P}}} \mu_{v,x}$ where $\mu_{v,x}$ is the measure on $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$ obtained by identifying it with $\mathbf{Q}_v^r$ with help of $x_1, \ldots, x_r$. If q denote the trace form on $L \otimes_{\mathbf{Q}} \mathbf{Q}_v$ given by $q(x, y) = \mathrm{Tr}_{L \otimes_{\mathbf{Q}} \mathbf{Q}_v / \mathbf{Q}_v}(xy)$ then we have equality between invariant measures on $L \otimes_{\mathbf{Q}} \mathbf{Q}_v = \prod_{u|v} L_u$

$$|(\textstyle\bigwedge^r q)(\bigwedge^r x, \bigwedge^r x)|_v^{1/2} \mu_{v,x} = \prod_{u|v} \mu_u.$$

Now the formula (3.2) derives from the product formula

$$\prod_{v \in \bar{\mathscr{P}}} |(\textstyle\bigwedge^r q)(\bigwedge^r x, \bigwedge^r x)|_v^{1/2} = 1.$$

The volume of the box B_c with respect to normalized adelic measure μ_L can now be calculated locally. It is of course enough to restrict our self to the case $c_u = 1$ for all $u \in \bar{\mathscr{P}}_L$. The nonarchimedean places will contribute all together the term $\mathrm{discr}_L^{-1/2}$. A complex place will contribute a factor 2π and a real place a factor 2. □

COROLLARY 3.4 (Minkowski). *Let $c = (c_u; u \in \bar{\mathscr{P}}_L)$ be a sequence of positive real numbers with $c_u = 1$ for almost all u such that*

$$\prod_{u \in \bar{\mathscr{P}}} c_u > \pi^{-m_{\mathbf{C}}} \mathrm{discr}_L^{1/2}$$

then $B_c \cap L^\times$ is not empty.

PROOF. Let $c' = (c'_u; u \in \bar{\mathscr{P}}_L)$ defined as follows $c'_u = c_u$ if u is a nonarchimedean place, and $c'_u = c_u/2$ is u is an archimedean place. We have

$$\prod_{u \in \bar{\mathscr{P}}} c'_u > 2^{-m_\infty} \pi^{-m_{\mathbf{C}}} \mathrm{discr}_L^{1/2}$$

and thus according to (3.3)

$$\mathrm{vol}(B_{c'}, \mu_L) > 1.$$

If $1_{B_{c'}}$ denote the characteristic function of $B_{c'}$, then we will have

$$\int_{\mathbf{A}_L} 1_{B_{c'}}(x) \mathrm{d}\mu_L(x) = \int_{\mathbf{A}_L/L} \mathrm{Av}_L(1_{B_{c'}})(\bar{x}) \mathrm{d}\bar{\mu}_L(\bar{x}) > 1.$$

Since $\mathbf{A}_L/L$ has total volume one with respect to $\bar{\mu}_L$, there exists $\bar{x} \in \mathbf{A}_L/L$ such that

$$\mathrm{Av}_L(1_{B_{c'}})(\bar{x}) > 1.$$

It follows that there exists different adèles $x_1, x_2 \in B_{c'}$ such that $x_1 - x_2 \in L^\times$. Now for all non archimedean places u, we have $\|x_1 - x_2\| \leq c'_u = c_u$ and and for all archimedean places, we have $\|x_1 - x_2\| \leq 2c'_u = c_u$. Therefore $x_1 - x_2 \in B_c \cap L^\times$. □

4. Invariant measure on multiplicative groups

We first interprete the positive norms of local fields and of idèles in terms of the scaling effect on invariant measures. Let $\mathrm{Aut}(G)$ denote the group of automorphisms of a locally compact topological group G. This group acts on the space of compactly supported functions $C_c(G)$, the space of Radon measures in preserving the one-dimensional subspace of invariant measure. For all $t \in \mathrm{Aut}(G)$, we denote $f^t(x) = f(t^{-1}x)$ for all function f on $\mathbf{R}$ and $\mu^t(f) = \mu(f^t)$ for all Radon measures. There exists a unique positive constant $|t|_G \in \mathbf{R}_+$ such that $I^t = \|t\|_G I$ for all invariant measures I on G. The positive number $\|t\|_G$ will be called the **positive norm** of t.

Let F be a local field either archimedean or nonarchimedean. Each element $t \in F^\times$ defines an automorphism of F considered as locally compact abelian group. The above discussion on the scaling effect on invariant measure allow us to define a positive real number $\|t\|_F$. We can check this is nothing but positive norm defined **??** in Chapter 1. Let L be a number field. Each idèle $t \in \mathbf{A}_L^\times$ defines an automorphism of $\mathbf{A}_L$ considered as a locally compact abelian group. The positive real number $\|t\|_L$ defined by the scaling effect on invariant measures coincide with the positive norm of idèles $\|t\|_L = \prod_v \|t_v\|_v$ if $t = (t_v, v \in \bar{\mathscr{P}}_L) \in \mathbf{A}_L^\times$.

If G is a discrete group, then automorphism does effect on the counting measure; in other words, for all $t \in \mathrm{Aut}(G)$, $\|t\|_G = 1$. If G is a compact group and $f = 1_G$ the constant function of value one, we have $f^t = f$. It follows that we also have $\|t\|_G = 1$. Thus the positive norm of automorphism in discrete or compact group is always equal to one. Let G be a locally compact commutative group with a discrete cocompact subgroup

H. If $t \in \mathrm{Aut}(G)$ such that $t(H) = H$, then $\|t\|_G = 1$. It follows from this observation that for all principal idèles $t \in L^\times$, $\|t\|_L = 1$.

For every local field F finite extension of basic local field $\mathbf{Q}_v$ either p-adic or real, we have defined a canonical invariant measure μ_F on F defined in (3.1) with aid of the trace form $(x, y) \mapsto \mathrm{Tr}_{F/\mathbf{Q}_v}(xy)$. This allows us to define an invariant measure $\mu_F^\times$ on $F^\times$ by the formula

$$\int_{F^\times} \varphi(x) \mathrm{d}\mu_F^\times(x) = \int_F \frac{\varphi(x)}{\|x\|_F} \mathrm{d}\mu_F(x)$$

that may be abbriated as

$$\mathrm{d}\mu_F^\times(x) = \frac{\mathrm{d}\mu_F(x)}{\|x\|_F}.$$

Let us calculate explicitly the measure $\mu_F^\times$ in archimedean and nonarchimedean cases.

- If $F = \mathbf{R}$ and $K(c_1, c_2)$ is the compact subset of $\mathbf{R}^\times$ consisting of real numbers $x \in \mathbf{R}^\times$ such that $c_1 \leq |x| \leq c_2$ where $c_1 < c_2$ are given positive real numbers, then

  $$\mathrm{vol}(K(c_1, c_2), \mu_{\mathbf{R}}^\times) = 2(\log(c_2) - \log(c_1)).$$

  If we identify $\{\pm 1\} \times \mathbf{R}_+$ with $\mathbf{R}^\times$ by mapping $(\epsilon, y) \mapsto \epsilon \exp(y)$, then there the measure $\mu_{\mathbf{R}}^\times$ can be factorized as $\mu_\pm \times \mu_{\mathbf{R}} = \mu_{\mathbf{R}}^\times$ where $\mu_\pm$ is the counting measure on $\{\pm 1\}$ and $\mu_{\mathbf{R}}$ is the Lebesgue measure on $\mathbf{R}$.
- If $F = \mathbf{C}$ and $K(c_1, c_2)$ is the compact subset of $\mathbf{C}^\times$ consisting of real numbers $x \in \mathbf{R}^\times$ such that $c_1 \leq \|x\| \leq c_2$ where $c_1 < c_2$ are given positive real numbers, then

  $$\mathrm{vol}(K(c_1, c_2), \mu_{\mathbf{C}}^\times) = 2\pi(\log(c_2) - \log(c_1)).$$

  If we identify $\mathbf{C}^1 \times \mathbf{R}$ with $\mathbf{C}^\times$ by mapping $(\tau, y) \mapsto \tau \exp(y)$ for all normed one complex number $\tau \in \mathbf{C}^1$ and $y \in \mathbf{R}$ then there the measure $\mu_{\mathbf{C}}^\times$ can be factorized as $\mu_{\mathbf{C}^1} \times \mu_{\mathbf{R}} = \mu_{\mathbf{C}}^\times$ where $\mu_{\mathbf{C}^1}$ is the invariant measure on $\mathbf{C}^1$ assigning to this compact group the measure 2π and $\mu_{\mathbf{R}}$ is the Lebesgue measure on $\mathbf{R}$.
- If F is a nonarchimedean local field and $K_F = \mathscr{O}_F^\times$ is the maximal compact subgroup of $F^\times$, then

  $$\mathrm{vol}(K_F, \mu_F^\times) = (1 - q^{-1})\mathrm{vol}(\mathscr{O}_F, \mu_F)$$

  where q is the cardinal of the residue field of F.

One observe that the infinite product $\prod_{p \in \mathscr{P}}(1 - p^{-1})$ is convergent to 0, in to order to define an invariant measure on the group of idèles $\mathbf{A}_L^\times$, one needs to renormalize local measures. We set

- If $F = \mathbf{R}$ or $\mathbf{C}$, $\mu_F^* = \mu_F^\times$;

- If F is nonarchimedean, $\mu_F^* = (1-q^{-1})^{-1}\mu_F^\times$ where q is the the cardinal of the residue field of F. In particular

$$\mathrm{vol}(K_F, \mu_F^*) = \mathrm{vol}(\mathscr{O}_F, \mu_F) \tag{4.1}$$

Let L be a number field. For every nonarchimedean place v, let K_v denote the compact open subgroup $\mathscr{O}_v^\times$ in $L_v^\times$ and let choose positive real numbers $c_{1,v} < c_{2,v}$ for each archimedean places v of L and set $K_v = K(c_{1,v}, c_{2,v})$. We normalize the invariant measure μ_L^* on $\mathbf{A}_L^\times$ by assigning to $K = \prod_{v\in\bar{\mathscr{P}}_L} K_v$ the measure

$$\mathrm{vol}(K, \mu_L^*) = \prod_{v\in\mathscr{P}_L} \mathrm{vol}(K_v, \mu_{L_v}^*).$$

This infinite product is well defined since almost all of its terms are equal to one. We can in fact calculate this product explicitly

$$\mathrm{vol}(K, \mu_L^*) = \frac{2^{m_{\mathbf{R}}}(2\pi)^{m_{\mathbf{C}}}}{\sqrt{\mathrm{discr}_L}} \prod_{v\in\mathscr{P}} (\log(c_{2,v}) - \log(c_{1,v}))$$

with aid of 3.2.

PROPOSITION 4.1. *Recall that the quotient $\mathbf{A}_L^\times/\mathbf{A}_L^1$ can be identified with $\mathbf{R}$ by the map $x \mapsto \log(\|x\|)$. Let μ_L^1 be the invariant measure on $\mathbf{A}_L^1$ normalized so that μ_L^*/μ_L^1 is the Lebesgue measure $\mu_{\mathbf{R}}$ on $\mathbf{R}$. This measure induces on the compact quotient $\mathbf{A}_L^1/L^\times$ an invariant measure with respect to which $\mathbf{A}_L^1/L^\times$ has volume*

$$\mathrm{vol}(\mathbf{A}_L^1/L^\times, \mu_L^1) = \frac{2^{m_{\mathbf{R}}}(2\pi)^{m_{\mathbf{C}}} h_L r_L}{\sqrt{\mathrm{discr}_L}\, w_L}$$

where

- *$m_{\mathbf{R}}$, $m_{\mathbf{C}}$ are respectively the number of real places and complex places of L;*
- *discr_L is the absolute discriminant of L;*
- *h_L is the class number of L i.e. the order of its ideal class group $\mathrm{Cl}(R)$ where $R = \mathbf{Z}_L$ is the ring of integers of L*
- *w_L is the order of the group of roots of unit contained in L, in other words the order of the torsion subgroup $R_{\mathrm{tors}}^\times$ of $R^\times$;*
- *r_L is the regulator of L defined as follows: Let $\alpha_1, \ldots, \alpha_{m-1}$ be a $\mathbf{Z}$-basis of $R^\times/R_{\mathrm{tors}}^\times$ with $m = m_{\mathbf{R}} + m_{\mathbf{C}}$ the number of archimedean places of L. Let A denote the $m \times m$ matrix consisting of the $(m-1)$ rows given by $(\log\|\alpha_i\|_v$ with $v \in \mathscr{P}_\infty$, and one row given by $(1, 0, \ldots, 0)$. Then we set*

$$r_L = \|\det(A)\|.$$

PROOF. We recall the exact sequence (7.4) in Chapter 1:

$$0 \to \left(\hat{R}^\times \times L_{\mathbf{R}}^1\right)/R^\times \to \mathbf{A}_L^1/L^\times \to \mathrm{Cl}(R) \to 0 \tag{4.2}$$

where $|\mathrm{Cl}(R)| = h_L$, and therefore it will be sufficient to prove that

$$\mathrm{vol}(\left(\hat{R}^\times \times L_{\mathbf{R}}^1\right)/R^\times) = \frac{2^{m_{\mathbf{R}}}(2\pi)^{m_{\mathbf{C}}} r_L}{\sqrt{\mathrm{discr}_L}\, w_L}.$$

Let us consider the homomorphism $\log : \hat{R}^\times \times L_{\mathbf{R}}^\times \to \prod_{v\in\mathscr{P}_\infty} \mathbf{R}$ mapping $(x_R, x_\infty) \in \hat{R}^\times \times L_{\mathbf{R}}^\times$ to $(y_v; v \in \mathscr{P}_\infty)$ with $y_v = \log(\|x_\infty\|_v)$. Its kernel is the compact group $K = \prod_{v\in\mathscr{P}_L} K_v$ where $K_v = \mathscr{O}_v^\times$ for $v \in \mathscr{P}_L$, $K_v = \{\pm 1\}$ if v is a real place and $K_v = \mathbf{C}^1$ if v is a complex place. The measure μ_L^*, restricted to K is product of the measures μ_v^* assigning to $K_v = \mathscr{O}_v^*$ the measure $\mathrm{vol}(\mathscr{O}_v, \mu_{L_v})$, according to (4.1) if v is nonarchimedean, to $K_v = \{\pm 1\}$ the measure 2 if v is a real place, and to $K_v = \mathbf{C}^1$ the measure 2π if v is a complex place. The measure μ_L^*, restricted to $\hat{R}^\times \times L_{\mathbf{R}}^\times$ can be expressed as the product of the above measure on K with the Lebesgue measure on $\prod_{v\in\mathscr{P}_\infty} \mathbf{R}$.

We have an exact sequence

$$0 \to K/(K \cap R^\times) \to \left(\hat{R}^\times \times L_{\mathbf{R}}^1\right)/R^\times \to H_{\mathbf{R}}/\log(R^\times) \to 0$$

where $H_{\mathbf{R}}$ is the hyperplan in $\prod_{v\in\mathscr{P}_\infty} \mathbf{R}$ defined by the equation $\sum_{v\in\mathscr{P}_\infty} y_v = 0$. We observe that $K \cap R^\times$ is the group of root of units in L so that $|K \cap R^\times| = w_L$, and therefore

$$\mathrm{vol}(K, \mu_L^*) = \frac{2^{m_{\mathbf{R}}}(2\pi)^{m_{\mathbf{C}}}}{\sqrt{\mathrm{discr}_L}\, w_L}.$$

It only remains to prove that

$$\mathrm{vol}(H_{\mathbf{R}}/\log(R^\times)) = r_L.$$

But this is essentially how the regulator r_L has been defined. □