Abstract

The current article intends to introduce the reader to the concept of ideles and adeles and to describe some of their applications in modern number theory. These objects take important place in the methods of algebraic number theory and also in the study of zeta functions over number fields. We present a simpler application towards the proofs of several common theorems in number theory, such as the finiteness of the class number and Dirichlet's Unit theorem.

Adeles and Ideles and their applications

Vladislav Vladilenov Petkov

AUGUST 18, 2010

Contents

1 Introduction **2**

2 Definitions and structure of the Adeles and Ideles **3**
2.1 Adeles 4
2.2 Ideles 6
2.3 The main theorems 7

3 The Class number theorem **8**
3.1 The ring of integers 9
3.2 Proof of the Class number theorem 10

4 Dirichlet's Unit theorem and Modell-Weil theorem **11**
4.1 Ideles and the Unit theorem 11
4.2 The Mordell-Weil Theorem 13

5 The Iwasawa-Tate method **16**
5.1 Some basic knowledge on the zeta functions 16
5.2 Local theory 17
5.2.1 Local additive duality 17
5.2.2 Local multiplicative theory 19
5.3 Global theory 21
5.3.1 Global additive duality 21
5.3.2 The global functional equation and some further explanations 22

6 Conclusion **22**

7 Acknowledgements **24**

1 Introduction

The current article studies the basic properties of *adele* rings and the *idele* groups, which play central role in modern research in algebraic number the-

ory. While we postpone the formal definition of these objects for the following section, we include a rather crude intuitive description here. The adele ring represents a *restricted* direct product of the different completions of a given algebraic number field k. The word restricted comes from a requirement of convergence since we want to give the adeles a specific topology. The idele group of k is simply the group of invertible elements inside the adele ring. As we will explain later an important feature is that the topology given on this group is different from the subspace topology induced from the adele ring.

The reason why we study these two objects is their usefulness for understanding algebraic number fields. In cases when elementary methods cannot reveal more information about some field k, for example when its Galois closure is a non-abelian extension, looking at the localizations of its adele ring or idele group could be the key to success. Of course, one can object that it might be easier to consider the localizations of the field itself and therefore the construction of the two very abstract notions we suggested is redundant. Nevertheless, we hope to show that the proposed method has some important benefits in formalizing the transition from global to local problems.

Throughout this article we concentrate on several particular applications of the method of adeles and ideles that reveal some of their utility. Since these applications are somewhat independent beyond the basic properties presented in section 2, we separate them in distinct sections. First we present a neat proof of the classical fact that the Ideal class group of an algebraic number field[1] is finite. Next we present how the general properties of idele groups are used to prove the famous Dirichlet's unit theorem, which states that the group of units in any algebraic number field is finitely generated. As a slight digression we show how this fact proves Mordell-Weil theorem for elliptic curves. Finally, we briefly consider the Iwasawa-Tate method to prove complex continuation of certain zeta functions.

Now we proceed with the formal definitions and immediate results.

2 Definitions and structure of the Adeles and Ideles

In this section we define the concepts of adeles and ideles and prove some basic properties that we would need for the following sections. We ask the readers to excuse us for omitting the definitions of some of the concepts used throughout this article, since they are commonly seen in number theory books. We urge the reader to find the proper introduction to those subjects in the first few chapters of [Weil], [Lang] or [Bump]. In the case of local fields we refer the reader to [Iwasawa], since both [Weil] and [Lang] use the term improperly also for the archimedian completions $\mathbb{R}$ and $\mathbb{C}$.

Although Weil defines the concept of Adeles and Ideles on a broader set of

[1] Since the ring of integers in such field is a Dedekind domain this group is the same as the Picard group.

fields called $A-$fields, which combine finite extensions of $\mathbb{Q}$ and finite extensions of $\mathbb{F}_p(T)$, where T is transcendental over $\mathbb{F}_p$, we would restrict to the first type, as we will not consider the later. Henceforth we fix k to be an algebraic number field.

2.1 Adeles

We start with the following definition.

Definition 2.1. *As an infinite* place ν *of the field* k *we refer to an archimedean completion of an embedding of* k *into* $\mathbb{R}$ *or a pair of equivalent embeddings in* $\mathbb{C}$*. A finite* place *of* k *is a completion according to a non-archimedean valuation* ν*. In either case we denote the completion as* k_ν*. The term* place *is also often used for the norm according to which the completion is taken.*

Note that if ν is an infinite place k_ν is either $\mathbb{R}$ or $\mathbb{C}$. An example of a finite place is the field of $p-$adic numbers $\mathbb{Q}_p$ when $k = \mathbb{Q}$. If ν is a finite place we write r_ν for the maximal compact subring of k_ν and p_ν for the unique maximal ideal of r_ν. These can be identified with the sets $|x|_\nu \leq 1$ and $|x|_\nu < 1$.[2] We write P_∞ for the set of infinite places of k, and P for any finite set of places of k, containing P_∞. We can find such P, as a common result in Galois theory states that any number field k has finitely many infinite places, since the number of its embeddings in $\mathbb{C}$ is $[k : \mathbb{Q}]$. For every such set P define

$$k_A(P) = \prod_{\nu \in P} k_\nu \times \prod_{\nu \notin P} r_\nu. \tag{1}$$

We put a ring structure on $k_A(P)$ defining addition and multiplication componentwise. Thus $k_A(P)$ is a *restricted* product in the sense that it is a subset of $\prod k_\nu$, such that for any element $x = (x_\nu)$ $x_\nu \in r_\nu$ for all but finitely many places. Note that since every k_ν is locally compact and r_ν is compact the set $k_A(P)$ is locally compact under the product topology. This allows us to give the following

Definition 2.2. *The adele ring* k_A *of the algebraic number field* k *is defined as the union of the sets* $k_A(P)$*, where* P *ranges over all finite sets of places such that* $P \supset P_\infty$*. The topological ring structure on* k_A *is that for which each* $k_A(P)$ *is an open subring.*

We will also need the following

Definition 2.3. *For any place* ν *the set* $\{x \in k_A | x_w = 0, \forall w \neq \nu\}$ *is called a quasifactor of* k_A *corresponding to the place* ν*. There is a natural projection from* k_A *onto its quasifactor, which is equivalent to a projection onto the completion* k_ν*.*

[2] Throughout this paper we assume that all valuations are normalized.

Therefore, we would often use k_ν to denote both the quasifactor and the completion.

As for every place $k \subset k_\nu$ there exists a natural diagonal embedding of k into k_A given by $\xi \mapsto (\xi)$. We would name this injection φ. For our results we need to extend the construction of the adele ring to a finitely generated $k-$algebra $\mathscr{A}$. The quasifactors in such case are defined as $\mathscr{A}_\nu = \mathscr{A} \otimes_k k_\nu$ and $\mathscr{A}_A = \mathscr{A} \otimes_k k_A$.

Proposition 2.4. *Let $\mathscr{A}$ be a finitely generated $k-$algebra and let α be a finite subset of $\mathscr{A}$, containing a basis of $\mathscr{A}$ over k. For every finite place ν of k let α_ν be the $r_\nu-$module generated by α in $\mathscr{A}$. Define*

$$\mathscr{A}_A(P, \alpha) = \prod_{\nu \in P} \mathscr{A}_\nu \times \prod_{\nu \notin P} \alpha_\nu.$$

Then there exists a set P_0, such that $\mathscr{A}_A(P, \alpha)$ is open for every $P \supset P_0$. $\mathscr{A}$ is the union of these sets.

Proof. [Weil]. □

Theorem 2.5. *If k'/k is a finite extension and ν is a place of k there exists a unique isomorphism $\Phi_\nu : (k'/k)_\nu \to \prod k'_w$, where w runs over the set of places of k' that lie over ν, such that Φ_ν is $k_\nu-$linear and $\Phi_\nu(\xi) = (\xi, \ldots, \xi)$ for any element $\xi \in k'$.*

Proof. [Weil]. For the finite cases look also in [Iwasawa]. □

These results lead us to our first important theorem.

Theorem 2.6. *Let k'/k be a finite extension and $(k'/k)_A$ denote the adele $k-$algebra of k'. Let k'_A be the adele ring of the number field k'. Then there exist a unique isomorphism Φ of $(k'/k)_A$ onto k'_A, with the following properties: (i) Φ is trivial on the natural embedding of k' in k'_A and $(k'/k)_A$. (ii) for every quasifactor Φ induces a $k_\nu-$linear isomorphism Φ_ν of $(k'/k)_\nu$ onto the product $\prod k'_w$ of quasifactors of k'_A, where w runs over the places of k' that lie over ν.*

Proof. Let $\mathscr{A} = (k'/k)$, hence $\mathscr{A}_A = (k'/k)_A$. By theorem (2.5) there exist a unique isomorphism Φ_ν of $(k'/k)_\nu$ onto $\prod k'_w$, such that it is $k_\nu-$linear and it sends elements of k' to the corresponding diagonal elements. Let α be a basis of k' over k. Then by the same theorem the module α_ν maps onto the product $\prod r'_w$. By proposition (2.4) this is true for all but finitely many quasifactors. Let P_0 be a finite set such that Φ_ν has the above property for all $\nu \notin P_0$. For every place w of k' set $f(w)$ to be the underlying place of k. Then the product of the mappings Φ_ν determine an isomorphism Φ_P of $\mathscr{A}(P, \alpha)$ onto $k'_A(f^{-1}(P))$, for all $P \supset P_0$. As every set $f^{-1}(P)$ is finite the above expression makes sense. Since $f^{-1}(P')$ is contained in $f^{-1}(P)$ for $P = f^{-1}(P')$, k'_A is the union of the sets $k'_A(P)$ for $P \supset P_0$. As $\Phi_{P'}$ extends Φ_P whenever $P' \supset P$, there is an isomorphism Φ of $\mathscr{A}_A$ onto k'_A which coincides with Φ_P on the domain of definition of the later, if $P \supset P_0$. Therefore, Φ has the desired properties and is uniquely determined. Note also that since $\mathscr{A}(P, \alpha)$ is an open subring of $\mathscr{A}_A$ the isomorphism is also continuous. □

We have the following corollary.

Corollary 2.7. *Let k'/k be a finite extension and E/k' a finite dimensional algebra. Call E/k the underlying $k-$algebra. The the identity mapping of E/k onto E/k' can be extended uniquely to a k_A-linear isomorphism of $(E/k)_A$ into $(E/k')_A$.*

This result shows us that it is equivalent to extend a field and to construct the adele algebra and construct the adele ring of the extension directly. This isomorphism would help us on several occasions in the later results.

2.2 Ideles

Here we present the second central object in our paper.

Definition 2.8. *Let $\mathscr{A}$ an algebra of finite dimension over a field k. we define the* idele group *of $\mathscr{A}$ to be the set $\mathscr{A}_A^\times$ of invertible elements of $\mathscr{A}_A$ with the coarsest topology such that $x \mapsto (x, x^{-1})$ is a homeomorphism of $\mathscr{A}_A^\times$ onto its image in $\mathscr{A}_A^\times \times \mathscr{A}_A^\times$.*

Note that the above statement is equivalent to requiring that multiplication and inversion are continuous in the given topology. As the subspace topology induced on $\mathscr{A}_A^\times$ as a subset of $\mathscr{A}_A$ does not satisfy the second condition, the idele topology is different. Let $f(x, y) = xy$ be a map from $\mathscr{A} \times \mathscr{A}$ onto $\mathscr{A}$. Then $\mathscr{A}_A^\times$ is homeomorphic to $f^{-1}(1)$ and since f is trivially continuous the idele group is locally compact. Further, similarly to the adeles there is a natural embedding of $\mathscr{A}^\times$ in $\mathscr{A}_A^\times$. Alternative definition of the ideles is given through the following proposition.

Proposition 2.9. *Let $\mathscr{A}$, α, α_ν and P_0 be as in proposition (2.4). Let P be any finite set of places containing P_0. Then the group*

$$\mathscr{A}(P, \alpha)^\times = \prod_{\nu \in P} \mathscr{A}_\nu^\times \times \prod_{\nu \notin P} \alpha_\nu^\times$$

is an open subgroup of $\mathscr{A}_A^\times$; the topologies induced by $\mathscr{A}_A^\times$ and $\mathscr{A}_A$ are the same as the product topology of the right-hand side of the above expression; and $\mathscr{A}_A^\times$ is the union of these groups.

Proof. [Weil]. □

For a field k we define the norm of an idele $a = (a_\nu)$ as

$$|a|_{k_A} := \prod_\nu |a_\nu|_\nu. \tag{2}$$

Now we proceed with the basic results about adeles and ideles we would need.

2.3 The main theorems

Theorem 2.10. *Let k be a number field and $\mathscr{A}$ a finite dimensional k-algebra. Then $\mathscr{A}$ is discrete in $\mathscr{A}_A$, and $\mathscr{A}_A/\mathscr{A}$ is compact.*

Proof. From the corollary of theorem (2.6) we see that it is sufficient to prove the statement for $k = \mathbb{Q}$.

For each prime p, let $\mathbb{Q}^{(p)}$ be the set of elements ξ of $\mathbb{Q}$ such that $|\xi|_{p'} \leq 1$ for all other primes p'. These are the rational numbers with powers of p in the denominator.

Lemma 2.11. *For every prime p, $\mathbb{Q}_p = \mathbb{Q}^{(p)} + \mathbb{Z}_p$ and $\mathbb{Q}^{(p)} \cap \mathbb{Z}_p = \mathbb{Z}$.*

Proof. Obvious. □

Lemma 2.12. *Put $A_\infty = \mathbb{R} \times \prod \mathbb{Z}_p$ and let φ be the canonical injection of $\mathbb{Q}$ into $\mathbb{Q}_A$. Then $\mathbb{Q}_A = \varphi(\mathbb{Q}) + A_\infty$ and $\varphi(\mathbb{Q}) \cap A_\infty = \varphi(\mathbb{Z})$.*

Proof. Note that with the notation in section 2.1 $A_\infty = \mathbb{Q}_A(P_\infty)$. Therefore, it is an open subring of $\mathbb{Q}_A$. Take any $x = (x_\nu)$ in $\mathbb{Q}_A$; call P the set of primes such that x_p is not in $\mathbb{Z}_p$; by definition it is a finite set. For each $p \in P$, by the first lemma we can write $x_p = \xi_p + x'_p$, with $\xi_p \in \mathbb{Q}^{(p)}$ and $x'_p \in \mathbb{Z}_p$. For p not in P, define $\xi_p = 0$ and $x'_p = x_p$. Let $\xi = \sum \xi_p$ and $y = x - \varphi(\xi)$. If $y = (y_\nu)$ for every prime we have

$$y_p = x_p - \xi_p - \sum_{p' \neq p} \xi_{p'} = x'_p - \sum_{p' \neq p} \xi_{p'}.$$

By the definition of $\mathbb{Q}^{(p)}$ all terms on the right hand side are in $\mathbb{Z}_p$. Thus, as the p-adic valuation is non-archimedean, y is in A_∞. Therefore, x is in $\mathbb{Q}^{(p)} + A_\infty$. The second part of the lemma is obvious. □

We now have the tools to complete the proof of the theorem. As A_∞ is open in $\mathbb{Q}_A$, the first assertion will be true if we show that $\varphi(\mathbb{Q}) \cap A_\infty$, i.e. $\varphi(\mathbb{Z})$, is discrete in A_∞. The projection of $\varphi(\mathbb{Z})$ on the factor $\mathbb{R}$ of the product A_∞ is $\mathbb{Z}$, which is discrete in $\mathbb{R}$. The result follows. Let $I = [-1/2, 1/2]$ in $\mathbb{R}$ and let $C = I \times \prod \mathbb{Z}_p$. Clearly $A_\infty = \varphi(\mathbb{Z}) + C$, hence $\mathbb{Q}_A = \varphi(\mathbb{Q}) + C$. As C is compact we finish the proof of the theorem. □

We now prove the following important result.

Theorem 2.13. (Artin's Product Formula) *let k be a number field; then the morphism $z \mapsto |z|_{k_A}$ of $k_A^\times$ into $\mathbb{R}_+^\times$ (the multiplicative group of the positive real numbers) induces the constant 1 on $k^\times$.*

Proof. Let k'/k_0 be a finite extension. Let ν be a place of k_0 and let $x \in k'$. Then if we let w range over the places of k' that lie over ν we obtain

$$\prod_w |x_w|_w = |N_{k'/k_0}(x)|_\nu, \tag{3}$$

where N_{k'/k_0} is the usual norm map. Then formula (3) allows us to reduce the proof to $\prod |N_{k'/k_0}(x)|_\nu = 1$ for every $x \in k'$ or equivalently to $|y|_{k_{0_A}} = 1$ for every $y \in k_0$. Therefore, it is sufficient to prove the result for $k = \mathbb{Q}$, for which it is trivial. □

Define $k_A^1 \subset k_A^\times$ to be the kernel of the morphism $x \mapsto |x|_{k_A}$. We know that k_A^1 contains $k^\times$ and we have the following important corollary.

Corollary 2.14. *For every $\lambda \in \mathbb{R}_+^\times$ let $z(\lambda)$ be the idele such that $z_\nu = 1$ for every finite place ν and $z_w = \lambda$ for every infinite place w. Then $\lambda \mapsto z(\lambda)$ is an isomorphism of $\mathbb{R}_+^\times$ onto a closed subgroup G of $k_A^\times$. Further, $k_A^\times$ is the direct product of that group and k_A^1.*

Proof. Note that the map $\lambda \mapsto z(\lambda)$ is clearly an injective group homomorphism. From proposition (2.9) we know then that this map is an isomorphism of $\mathbb{R}_+^\times$ onto a subgroup G of $k_A(P_\infty)^\times$. We have that $|z(\lambda)|_{k_A} = \lambda^n$, n being the order of P_∞. If $x \in k_A^\times$, then there exists $y \in G$ such that $|x|_{k_A} = |y|_{k_A}$. Therefore, as the norm is multiplicative, $x/y \in k_A^1$. The result follows. □

This allow us to prove the following theorem.

Theorem 2.15. *Let k_A^1 be the subgroup of $k_A^\times$ defined by $|z|_{k_A} = 1$. Then $k^\times$ is a discrete subgroup of k_A^1; the factor group $k_A^1/k^\times$ is compact; and $k_A^\times/k^\times$ is isomorphic to the direct product of that group and a group isomorphic to $\mathbb{R}_+^\times$.*

Proof. Theorem (2.13) shows that $k^\times$ is a subgroup of k_A^1 and theorem (2.10) shows that $k^\times$ is discrete if we look at the two sets as sets of adeles. As the topology on the ideles is finer this property is preserved. The second claim is somewhat technical and requires the introduction of notation we will not utilize and therefore we refer the reader to [Weil] or [Lang] for its proof. The last fact follows immediately from corollary (2.14). □

As we have established the basic properties of the ideles and adeles we proceed with the particular results in the following sections.

3 The Class number theorem

In this section we try to prove the following well known theorem.

Theorem 3.1. (The Class number theorem) *Let k be a number field. Let $h_k = |I(k)/P(k)|$ denote its class number, i.e. the number of equivalence classes of fractional ideals of k. Then h_k is a finite number.*

There are simple proofs of this result that use little but basic number theory and commutative algebra. However, they are often somewhat technical and slow. The one that we propose is much more elegant and shows that power of abstract ideles.

3.1 The ring of integers

Before we begin our proof we must present an equivalent definition of the ring of integers for a number field, which will show us why ideles are applicable. We begin with the usual description.

Definition 3.2. *The* ring of integers *in a number field is the integral closure of* $\mathbb{Z}$ *in that field.*

Here is the alternative definition.

Definition 3.3. *Let* k *be a number field. Define* $\mathfrak{r} = \bigcap(k \cap r_\nu)$*, where* ν *runs over all finite places of* k*.*

Theorem 3.4. *The module* $\mathfrak{r}$ *is the unique maximal order of* k *and is the integral closure of* $\mathbb{Z}$ *in* k*.*

Proof. We need the following lemma.

Lemma 3.5. *Let* G *be a locally compact group with an open subgroup* G_1 *of the form* $G_1 = G' \times G''$*, such that* G' *is locally compact and* G'' *is compact. Let* Γ *be a discrete subgroup of* G*, such that* G/Γ *is compact. Call* Γ' *the projection of* $\Gamma \cap G_1$ *onto* G'*. Then* Γ' *is discrete in* G'*, and* G'/Γ' *is compact.*

Proof. Let W be some compact neighbourhood of the identity in G'. As $W \times G''$ is compact, its intersection with Γ is finite. The projection of this intersection on G' is $W \cap \Gamma'$, hence $W \cap \Gamma'$ is finite. Therefore, Γ' is discrete. Since G_1 is open in G, so are $G_1\Gamma$ and $G \setminus G_1\Gamma$, as unions of left cosets of G_1. This shows that the image of G_1 in the quotient group G/Γ is both open and closed, hence compact. By the isomorphism theorems this image is isomorphic to G_1/Γ_1, with $\Gamma_1 = \Gamma \cap G_1$. Then there exist a compact subset C of G_1 such that $G_1 = C\Gamma_1$. If C' is the projection of C on the factor G', $G' = C'\Gamma'$ and we have that G'/Γ' is compact. □

Write $k_A(P_\infty) = k_\infty \times (\prod r_\nu)$, where the later product is taken over all finite places. from the definition of $\mathfrak{r}$ an element $\xi \in k$ is in $\mathfrak{r}$ if and only if $\varphi(\xi)$ is in the product above.[3] Denote the restriction of $\varphi(\xi)$ to k_∞ by $\varphi_\infty(\xi)$ and to $\prod r_\nu$ by $\psi(\xi)$. As $\mathfrak{r}$ is a subring of k we can apply lemma (3.5) for $G = k_A$, $G_1 = k_A(P_\infty)$, $G' = k_\infty$, $G'' = \prod r_\nu$ and $\Gamma = \varphi(k)$. Remember that we showed that k is discrete in k_A and the quotient k_A/k is compact. With the notations above, we have $\Gamma' = \varphi_\infty(\mathfrak{r})$. By the lemma we see that $\varphi_\infty(\mathfrak{r})$ is then a $\mathbb{R}$-lattice in k_∞. But φ_∞ is the same as the injection induced on $\mathfrak{r}$ by the natural injection of k into $k_\infty = k \otimes_{\mathbb{Q}} \mathbb{R}$. Therefore, $\mathfrak{r}$ is also a $\mathbb{Q}$-lattice in k and as $\mathfrak{r}$ is also a subring it is an order.

Now let $\mathfrak{r}'$ be any subring of $k\mathfrak{r}$, which additive group is finitely generated. Then the r_ν-module generated by $\mathfrak{r}'$ in k_ν is a compact subring, because it is a finitely generated module and r_ν is compact. Since $\mathfrak{r}'$ contains 1 this subring contains r_ν. However, as r_ν is the maximal compact subring of k_ν it follows

[3] Remember φ is the natural embedding of k in k_A.

that $\mathfrak{r}' \subset r_\nu$. As this is true for any finite place we have $\mathfrak{r}' \subset \mathfrak{r}$. This shows that $\mathfrak{r}$ is the unique maximal order. To prove that it is the ring of integers we need to prove another auxiliary result.

Lemma 3.6. *Let a be an element of an order in a finite dimensional $\mathbb{Q}-$algebra $\mathscr{A}$. Then a is integral over $\mathbb{Z}$.*

Proof. Let R be some order containing a and let $a_1, \ldots, a_n$ be a basis of R over $\mathbb{Q}$. We can then write

$$a \cdot a_i = \sum c_{ij} a_j \tag{4}$$

for any $1 \leq i \leq n$, with $c_{ij} \in \mathbb{Q}$. If m is the least common multiple of the denominators of c_{ij} we can consider a new basis $m^2 a_1, \ldots, m^2 a_n$, for which we have $a_i \cdot a_j = \sum c_{ijh} a_h$ and $c_{ijh} \in \mathbb{Z}$. Therefore, we may safely assume that c_{ij} in (4) are integers.

We can rewrite the expression as $\sum(\delta_{ij} a - c_{ij}) a_j = 0$, where δ_{ij} is the Kronecker delta. Let $D(x)$ denote the determinant of the matrix $(\delta_{ij} x - c_{ij})$, for indeterminate x and $D_{ij}(x)$ denote the corresponding minors. These are by definition polynomials in $\mathbb{Z}[x]$ and we have

$$\delta_{hj} D(x) = \sum_i D_{ih}(x)(\delta_{ij} x - c_{ij}). \tag{5}$$

If we substitute $x = a$, multiply the expression by a_j and sum over $1 \leq j \leq n$ we get that $D(a) a_h = 0$ for all h; hence $D(a)x = 0$ for all x in R. For $x = 1$ we get $D(a) = 0$. As $D(x)$ is obviously a monic polynomial, this shows that a is integral over $\mathbb{Z}$ and concludes the proof of the lemma. □

The above lemma shows that any element of $\mathfrak{r}$ is integral over $\mathbb{Z}$. Conversely, if an element a of k is integral over $\mathbb{Z}$ then for any finite place ν a is still integral hence $a \in r_\nu$. Therefore, a is in $\mathfrak{r}$, hence $\mathfrak{r}$ is the ring of integers in k. □

3.2 Proof of the Class number theorem

We proceed with the central part of the proof of theorem (3.1). To ease our notation write $\Omega(P)$ for $k_A(P)^\times$, i.e.

$$\Omega(P) = \prod_{\nu \in P} k_\nu^\times \times \prod_{\nu \notin P} r_\nu^\times.$$

As usual P is a finite set of places that contains P_∞, the set of all infinite places. Recall that by proposition (2.9) $\Omega(P)$ is always an open subgroup of $k_A^\times$. Define $\Omega_1(P) = \Omega(P) \cap k_A^1$, where k_A^1 is defined as in section (2.3).

Theorem 3.7. *The group $k_A^\times / k^\times \Omega(P)$ is finite.*

Proof. By the isomorphism theorems the quotient $k_A^1 / k^\times \Omega_1(P)$ is isomorphic to the quotient of $k_A^1 / k^\times$ by the image of $\Omega_1(P)$ in $k_A^1 / k^\times$. As $\Omega_1(P)$ is open in k_A^1, this image is open; since by theorem (2.15) $k_A^1 / k^\times$ is compact, the quotient

in question is finite. Obviously $\Omega(P)$ contains the group G defined in corollary (2.14) and from the same result we see that $\Omega(P) = \Omega_1(P) \times G$. Therefore, $k_A/k^\times\Omega(P)$ may be identified with $k_A^1/k^\times\Omega_1(P)$, which concludes the proof. □

Let $I(k)$ denote the group of fractional ideals of k and $P(k)$ the subgroup of principal ideals. For any fractional ideal $\mathfrak{a}$ we can consider the completion of $\mathfrak{a}$ at a finite place and call it $\mathfrak{a}_\nu$. By proposition (2.9) we have that for all but finitely many finite places $|a_\nu|_\nu = 1$, where $a = (a_\nu)$ is an element of $k_A^\times$. Thus $a_\nu r_\nu = r_\nu$ for almost all finite places. Therefore, there exists a unique fractional ideal $\mathfrak{a} = id(a)$, such that $\mathfrak{a}_\nu = a_\nu r_\nu$ for all finite places. The map $k_A^\times \to I(k)$, defined by $a \mapsto id(a)$, is trivially surjective and has kernel $\Omega(P_\infty)$. Therefore, we have $I(k) \cong k_A^\times/\Omega(P_\infty)$.

If $\mathfrak{r}$ is defined as in the previous subsection, we have that a fractional ideal is principal if and only if it is of the form $\xi\mathfrak{r}$ for some $\xi \in k$. Thus, as $\mathfrak{r} = \prod(k \cap r_\nu)$ we have that $P(k)$ is isomorphic to the image of $k^\times$ in the group $k_A^\times/\Omega(P_\infty)$. Therefore, the class group $I(k)/P(k)$ is isomorphic to $k_A/k^\times\Omega(P_\infty)$ which is finite by theorem (3.7).

4 Dirichlet's Unit theorem and Modell-Weil theorem

4.1 Ideles and the Unit theorem

In this section we present a proof of Dirichlet's famous Unit theorem which states

Theorem 4.1. (The Unit theorem) *Let k be a number field and let r_1 and $2r_2$ be the numbers of real and complex embeddings of k, respectively. If R is the ring of integers in k and $U = R^\times$ is the group of units in R, then U is finitely generated. In fact we have $U \cong C \times \mathbb{Z}^{r_1+r_2-1}$, where C is the finite cyclic group generated by the roots of unity that lie in k.*

In the following theorems we use the notation from section 3.

Theorem 4.2. *Let F be the set of elements $\xi \in k$, such that $|\xi|_\nu \leq 1$ for all places ν of k. Let $E = F \setminus \{0\}$. Then E is a finite cyclic group, consisting of all the roots of unity in k.*

Proof. If M is the subset of k_A consisting of the elements $x = (x_\nu)$, such that $|x_\nu|_\nu \leq 1$, then $F = M \cap \varphi(k)$. The quasifactor of M for every infinite place is either the interval $[-1, 1]$ or the closed unit disc in $\mathbb{C}$. The quasifactor for any finite place ν is the compact ring of integers r_ν. Therefore, M is compact and as k is discrete in k_A (theorem (2.10)) F must be a finite set. Consequently E is a finite subgroup of $k^\times$ and therefore is cyclic. Conversely, if ξ is a root of unity in k then obviously $|\xi|_w = 1$ for all infinite places w and any prime ideal $\mathfrak{P} \subset R$ does not contain ξ, hence $\xi \in r_\nu$ for every finite valuation ν. Therefore, E is precisely the set of all roots of unity in k. □

Define $E(P) = k^\times \cap \Omega(P)$, i.e., the elements of $k^\times$ for which $|\xi|_\nu = 1$, whenever ν is not in P. Obviously $E(P)$ contains the group E defined above. As $k^\times$ is discrete in k_A, $E(P)$ is discrete in $\Omega(P)$ and therefore in $\Omega_1(P)$. One can also think of the group $E(P)$ as the group of invertible elements in $k(P)^\times$.

Lemma 4.3. *Let G be a group and $G \cong \mathbb{R}^r \times \mathbb{Z}^{s+1-r}$, where $s \geqq r \geqq 0$. If $r > 0$, let λ be a morphism of G into $\mathbb{R}$, non-trivial on $\mathbb{R}^r$. Otherwise let λ be a non-trivial morphism of G into $\mathbb{Z}$. Let G_1 be the kernel of λ, and let Γ be a discrete subgroup of G_1, such that G_1/Γ is compact. Then Γ is isomorphic to $\mathbb{Z}^s$.*

Proof. Every element of G can be written as $(x_0, \ldots, x_s)$, with $x_i \in \mathbb{R}$ for $0 \leq i \leq r$ and $x_i \in \mathbb{Z}$ if $i > r$. The homomorphism λ can be written as

$$(x_0, \ldots, x_s) \mapsto \sum_{i=0}^{s} a_i x_i, \tag{6}$$

with a_i real if $r > 0$ and integer if $r = 0$. As λ is non trivial on $\mathbb{R}^r$ if $r > 0$ or on G if $r = 0$, we may assume that $a_0 \neq 0$. Consider the obvious embedding of G in the vector space $V = \mathbb{R}^{s+1}$; then formula (6) defines λ as a linear form on V. Let V_1 be the subspace of V, which is the kernel of λ, $\lambda(x) = 0$. Then by definition $G_1 = G \cap V_1$. For $1 \leq j \leq s$, call e_j the point (x_i) in V given by $x_0 = -a_j$, $x_j = a_0$ and $x_i = 0$ for $i \neq j$ and $i \neq 0$. Obviously $\{e_1, \ldots, e_s\}$ is a basis of V_1 and therefore generates a $\mathbb{R}-$lattice H in V_1, so that V_1/H is compact. Since G_1 is closed in V_1 and contains H it follows that G_1/H is compact. Consequently, if Γ is as in the lemma V_1/Γ is compact and hence Γ is a $\mathbb{R}-$lattice in V_1. This means that $\Gamma \cong \mathbb{Z}^s$, since $dim_{\mathbb{R}} V_1 = s$. □

Theorem 4.4. *Let P_∞, P, E and $E(P)$ be defined as above. Then $E(P)$ is the direct product of E and a group isomorphic to $\mathbb{Z}^s$, where $s = |P| - 1$.*

Proof. Note that, since $P \supset P_\infty$, P is non-empty. Let θ be the morphism of $\Omega(P)$ into $\mathbb{R}_+^\times$ defined by $z \mapsto |z|_{k_A}$. Then $\ker\theta = \Omega_1(P)$, which is open in k_A^1. Note that $k^\times \cap \Omega_1(P)$ is the same as $k^\times \cap \Omega(P)$. Thus the natural projection of k_A^1 onto $k_A^1/k^\times$ induces a homomorphism of $\Omega_1(P)$ onto its image with a kernel $E(P)$. Therefore, $\Omega_1(P)/E(P)$ is isomorphic to an open subgroup of $k_A^1/k^\times$ and hence is compact. Let U_ν be the standard group of units for a place ν. In other words, $U_\nu = r_\nu^\times = \{x \in k_\nu \,|\, |x|_\nu = 1\}$ for a finite place, $U_\nu = \{1, -1\}$ if ν is real and finally $U_\nu = S^1$ if ν is complex. Put $U = \prod U_\nu$, where ν ranges over all places of k, both finite and infinite. As each U_ν is compact, this is a compact subgroup of $\Omega(P)$ and $\Omega_1(P)$. Let $G = \Omega(P)/U$; clearly it is isomorphic to the direct product of $k_\nu^\times/U_\nu$ for $\nu \in P$. For infinite place w $k_w^\times/U_w$ is isomorphic to $\mathbb{R}_+^\times$, or equivalently to $\mathbb{R}$;[4] in the finite case $k_\nu^\times/U_\nu$ is isomorphic to $\mathbb{Z}$. As a result $G \cong \mathbb{R}^r \times \mathbb{Z}^{s+1-r}$, where r is the number of infinite places (i.e., $r = r_1 + r_2$ in the statement of the Unit theorem) and s is defined as $|P| - 1$. As U is contained in the kernel $\Omega_1(P)$ of θ in $\Omega(P)$, θ produces a

[4] Take the logarithm function as an isomorphism between $\mathbb{R}_+^\times$ and $\mathbb{R}$.

morphism of G into $\mathbb{R}_+^\times$, or in result a morphism λ of G into $\mathbb{R}$. Since $r > 0$ we may apply lemma (4.3) for G and λ. The kernel of λ is the image of $\Omega_1(P)$ in G, i.e., $\Omega_1(P)/U$. Let Γ be the image of $E(P)$ in G. If W is any compact neighbourhood of the identity in $\Omega(P)$, WU is compact and has therefore a finite intersection with $E(P)$ (remember that $E(P) \subset k^\times$). The image of this finite intersection is the intersection of Γ with the image of WU in G, which is a neighbourhood of 1 in G, and thus Γ is discrete. The quotient group G_1/Γ is isomorphic to $\Omega_1(P)/E(P)U$, which is a quotient group of the compact group $\Omega_1(P)/E(P)$. Therefore, G_1/Γ is also compact. Now applying lemma (4.3) we see that $\Gamma \cong \mathbb{Z}^s$. As $E(P) \cap U = E$, the morphism of $E(P)$ onto Γ, induced by the canonical homomorphism of $\Omega(P)$ onto G, has kernel E. Therefore, $E(P)$ is the direct product of E and the group $\mathbb{Z}^s$. □

This theorem immediately give us the proof for the Unit theorem, by taking $P = P_\infty$ and noting that $E(P_\infty)$ is the same as the group of invertible elements in the ring $\mathfrak{r}$, defined in section (3.1), which we proved also to be the ring of integers in k. Thus we have used a very abstract and powerful method to prove this basic number theory result almost avoiding he consideration of algebraic integers.

In a slight digression we present how the Dirichlet's Unit theorem and the Class number theorem may be used in the proof of another important result.

4.2 The Mordell-Weil Theorem

In this section we briefly describe the proof of the Mordell-Weil Theorem that concerns the group of rational points on an elliptic curve E. A basic introduction to the subject of elliptic curves can be found in [Silverman-Tate] and [Ireland]. Since some parts of the proof are very technical though requiring little but high-school level algebra, we refer them to the proper sources. The proof that we present generally follows the one given in [Ireland]. We begin by stating the theorem.

Theorem 4.5. (Mordell-Weil) *Let $E : y^2 = x^3 + ax + b$ be a non-singular elliptic curve over $\mathbb{Q}$ and let $E(\mathbb{Q})$ denote the group of rational points on E. Then $E(\mathbb{Q})$ is a finitely generated abelian group.*

The fact that $E(\mathbb{Q})$ is abelian is trivial from the definition of the addition of points on E. Throughout this section we denote by $\mathcal{O}$ the *point at infinity* which serves as identity for $E(\mathbb{Q})$.

The first part of the proof of this theorem involves tiresome calculations involving the exact formulas for the coordinates of a sum of two points (whether different or not). In this step the notion of a *height* of a rational point is introduced. This quantity represents an estimate of the size of the denominator of the rational x coordinate of a point P. Applying this notion through the *descent argument*, as referred by [Ireland], we can reduce the question to showing that the index of the subgroup $2E(\mathbb{Q})$ is finite in $E(\mathbb{Q})$. This part of the proof is of no interest for us and we recommend the reader to find the details in

[Silverman-Tate] or [Ireland], where it is presented in a very comprehensible way.

Our goal is to prove the following particular.

Proposition 4.6. *The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. Let $f(x) = x^3+ax+b$ be the cubic polynomial from the Weierstrass form of E. Let $\mathbb{Q}[\xi] = \mathbb{Q}[x]/(f(x))$, where ξ corresponds to the equivalence class of x. Note that this is not necessarily a field as $f(x)$ might be reducible. However, it is a ring and we denote by U its group of units. We define a homomorphism from $E(\mathbb{Q})$ to the group U/U^2 as follows.

Definition 4.7. *Let ϕ be a map from $E(\mathbb{Q})$ defined as follows*

i) $\phi(\mathcal{O}) = 1$*;*

ii) If $P = (\alpha, \beta)$, has order other than 1 or 2, i.e. $\beta \neq 0$, define $\phi(P)$ as the image of $\alpha - \xi$ in U/U^2;

iii) If $2P = \mathcal{O}$, then $f(x) = (\alpha - \xi)g(x)$ and $\phi(P) = \alpha - \xi + g(\xi)$.

Note that as $f(x)$ is separable $g(x)$ and $\alpha - x$ are coprime and thus in the last case the expression on the right hand side is indeed a unit. We need the following lemma.

Lemma 4.8. *The map ϕ is a homomorphism.*

Proof. [Ireland] □

Now we have a homomorphism from $E(\mathbb{Q})$ into U/U^2. We claim that the kernel of ϕ is precisely $2E(\mathbb{Q})$. Since $\phi(2P) = \phi(P)^2 = 1$ we have $2E(\mathbb{Q}) \subset \ker\phi$. Let $P = (\alpha, \beta)$ be a point, different from $\mathcal{O}$, such that $\phi(P) = 1$. Therefore, $\alpha - \xi$ must be a square in U. Then we may write

$$\alpha - \xi = (\alpha_1\xi^2 + \alpha_2\xi + \alpha_3)^2, \tag{7}$$

where α_i are rational numbers. As $\xi^3 = -a\xi - b$ we can write

$$l\xi + m = (\alpha_1\xi^2 + \alpha_2\xi + \alpha_3)(-\alpha_1\xi + \alpha_2), \tag{8}$$

where $l, m \in \mathbb{Q}$. If $\alpha_1 = 0$, we would get a linear dependence between 1,ξ and ξ^2, which is a contradiction. Thus squaring the second expression and dividing by α_1^2 we get

$$(e\xi + e')^2 = (\alpha - \xi)(h - \xi)^2 \tag{9}$$

for e, e' and h rational. Therefore, $(ex + e')^2 - (\alpha - x)(h - x)^2$ is a multiple of $f(x)$. However, since $f(x)$ is a monic cubic we get that

$$f(x) = (ex + e')^2 - (\alpha - x)(h - x)^2. \tag{10}$$

Geometrically this means that the line $y = ex + e'$ intersects E at (α, β) or (α, β) and (h, t), for some suitable t. Note also that this means that the multiplicity of the intersection at (h, t) is two. Therefore, $(\alpha, \pm\beta) = -2(h, t)$, which quickly shows that there is a point Q, such that $P = 2Q$. As a result $\ker \phi \subset 2E(\mathbb{Q})$ and thus $\ker \phi = 2E(\mathbb{Q})$.

Consequently, the homomorphism ϕ gives us an injection from $E(\mathbb{Q})/2E(\mathbb{Q})$ into U/U^2. Now fix a root θ of the polynomial $f(x)$ and let $k = \mathbb{Q}(\theta)$. Then $f(x) = (x - \theta)g(x)$ for some quadratic polynomial $g(x)$. For any point $P \neq \mathcal{O}$ if $P = (\alpha, \beta)$ define an ideal $I(P)$, associated with P, as follows

$$I(P) = (\alpha - \beta\theta, h(\alpha, \beta)), \tag{11}$$

where $h(\alpha, \beta) = \beta^2 g(\alpha/\beta)$. As $f(x)$ is monic both $\alpha - \beta\theta$ and $h(\alpha, \beta)$ are algebraic integers in k.

Lemma 4.9. *The set of ideals corresponding to points P is finite.*

Proof. We use that $g(x) - g(\theta) = (x - \theta)t(x)$ for some $t(x) \in \mathbb{Z}[\theta][x]$. Substituting $x = \alpha/\beta$ we see that $g(\theta)\beta^2$ is in the ideal $I(P)$. Similarly $g(\theta)x^2 - g(x)\theta^2 = (x - \theta)l(x)$, for some polynomial $l(x)$ and substituting the same $x = \alpha/\beta$ we see that $g(\theta)\alpha^2$ is also in $I(P)$. As α and β are coprime we see that $g(\theta) \in I(P)$ and hence the latter divides the fixed ideal $(g(\theta))$. Since the ring of integers of k is a Dedekind domain any ideal may have only finitely many divisors. □

Lemma 4.10. $(\alpha - \beta\theta) = I(P)C^2$ *for some ideal C.*

Proof. We write $(\alpha - \beta\theta) = I(P)A_1$ and $(h(\alpha, \beta)) = I(P)A_2$ for some ideals A_1 and A_2. Since $P = (\alpha, \beta) \in E(\mathbb{Q})$ there exists some rational number r/q such that $(r/q)^2 = f(\alpha/\beta)$; thus $\beta^3 r^2 = q^2(\alpha - \beta\theta)h(\alpha, \beta)$. Consequently, the ideal $(q)^2 I(P)A_1A_2$ is a square (remember that β is a square itself). As $I(P)$ is the greatest common divisor of the ideals $(\alpha - \beta\theta)$ and $h(\alpha, \beta)$ the two ideals A_1 and A_2 are coprime and hence each must itself be a square. □

From section 3 we know that the set of ideal classes is finite. Choose a set of representatives $C1, \ldots, C_{h_k}$. Then for any ideal B there are two algebraic integers μ and ν such that $\mu B = \nu C_i$ for some i.

Lemma 4.11. *There is a finite set of algebraic integers S such that for any point $P = (\alpha, \beta)$ one can write $\alpha - \beta\theta = u\gamma\tau^2$, where u is a unit, τ is an algebraic number and $\gamma \in S$.*

Proof. If C is as in the previous lemma then C is equivalent to some C_s and the principal ideal $(\alpha - \beta\theta)$ is equivalent to $I(P)C_s^2$. Therefore, this ideal is principal and hence of the form (γ). By lemma (4.9) and theorem (3.1) the set $S = \{(\gamma)\}$ is finite. Let μ and ν be algebraic integers such that $\mu C = \nu C_s$. Then $(\mu^2(\alpha - \beta\theta)) = I(P)\nu^2 C_s^2 = (\gamma\nu^2)$. Therefore, if $\tau = \nu/\mu$, for some unit u we have $\alpha - \beta\theta = u\gamma\tau^2$. □

Now we have the tools to complete the proof of the Mordell-Weil theorem.

It is sufficient to show that $\phi(E(\mathbb{Q}))$ is a finite set. We may safely assume that P has order other than 1 or 2, as there are totally at most 4 points with such orders. Then $\phi(P)$ is the coset modulo U^2 of $\alpha/\beta - x$, where $P = (\alpha/\beta, x)$, in the group U.

By the Chinese remainder theorem, as $f(x)$ is separable, we can write $\mathbb{Q}[\xi] = \mathbb{Q}[x]/(f(x))$ as the direct product $\prod \mathbb{Q}[\theta]/(f(\theta))$, where θ varies over the roots of $f(x)$. Thus the image of $\phi(E)$ is the product of its images in $k = \mathbb{Q}(\theta)$, for all θ.

If we consider any root θ the previous lemma shows that in $k^\times/(k^\times)^2$ the image of $\alpha/\beta - x$ is the coset of $(1/\beta)u\gamma$. Since β is the square of a rational integer (i.e. a usual integer in $\mathbb{Z}$) and the group of units of k is finitely generated by Dirichlet's Unit theorem (theorem (4.1)), the coset of $(1/\beta)u\gamma \ mod\,(k^\times)^2$ has a representative of the form $u_1^{\epsilon_1} \dots u_l^{\epsilon_l}\gamma$, where $\{u_i\}$ is a finite set of generators of the group of units and $\epsilon_i \in \{0, 1\}$. Since γ is chosen from a finite set of algebraic integers, the component of $\phi(E)$ corresponding to θ is finite. Therefore, $\phi(E)$ is finite and we conclude the proof of the theorem. □

5 The Iwasawa-Tate method

This chapter considers the connection between the adeles and ideles and zeta functions that play central role in analytic number theory. Essentially the results presented here come from Tate's Thesis, where he considered this relation for the first time. The particular computations are often very confusing and cannot be easily summarized. In such cases we will simply state the facts and refer the reader to [Lang], [Weil]. Certain amount of prior knowledge on Haar measures, Fourier analysis and p-adic numbers is necessary to understand the concepts in this chapter.

We begin by trying to explain why the complicated machinery we are about to develop is relevant for number theorists.

5.1 Some basic knowledge on the zeta functions

Perhaps the most famous zeta function is the Riemann zeta function defined by

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} \tag{12}$$

It is known that this function has analytic continuation to the whole complex plane, besides a simple pole at $s = 1$. Further, it has long been known that this zeta function satisfies the following functional equation

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s), \tag{13}$$

where $\Gamma(s)$ is the usual *Gamma function*. The classical way to derive the equation, which involves using properties of the *Theta function* can be found in [Lang] or [Weil] for example.

The problem of this proof is that it relies on the particular form of the Riemann zeta function. The class of zeta functions is much more broader, however. One of the important class of zeta functions, named Dirichlet's zeta functions is given as an *Euler product* of the form

$$\zeta(s) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}, \tag{14}$$

where p runs over the prime elements of some number field k and χ is a character of its multiplicative group. Note that if $k = \mathbb{Q}$ and $\chi = 1$ the above expression is the Euler product form of the Riemann zeta function, which is equivalent to the definition in (12). Similarly the Dirichlet's zeta functions have analytic continuations to certain domains of the complex plain and satisfy certain functional equations. Applying the tricks of the proof for the particular case of the Riemann zeta function, however, is a hopeless business.

Therefore, mathematicians started to look for general methods to derive the functional equations for different zeta functions and to determine their analytic continuation, poles and residues. One such method comes from the use of ideles and defining zeta functions on their characters. This method is called by some the *Iwasawa-Tate* method and is the central point of this section.

Another benefit from this method is that it immediately describes the *localizations* of the zeta function. These are zeta functions that are defined over a completion of the initial field k. Formula (14) presents such concept, by writing the *global* zeta function as a product of infinitely many *local* factors. To see the local factors one can simply expand into series each term of the product and consider them as a local zeta function corresponding to the completion (or place) at the prime p.

The problem is that equation (14) excludes the local functions at the *infinite* completions. Of course, this is because in the product they cancel. However, some questions require us to consider the local object first and for that we need the form of all localizations of the global zeta function. While this is not trivial when $\zeta(s)$ is written in the classical case, it is much clearer when we transform it as a zeta on the idele group.

We hope that this short description explain our motivation to discuss this topic. Another short introduction to Tate's Thesis may be found in [Thorne], which discusses more thoroughly the further applications of the results, however, still omits the proofs of the main theorems.

5.2 Local theory

5.2.1 Local additive duality

Let k be a number field and let k_ν be its completion according to the place ν. Let Tr denote the trace map on k_ν. We define a character on k_ν, by defining first $\lambda = \lambda_0 \circ Tr$, where λ_0 is defined on $\mathbb{Q}_p$ or $\mathbb{R}$ as follows.

Definition 5.1. *If ν is real we define $\lambda_0(x) = -x \bmod 1$ in $\mathbb{R}/\mathbb{Z}$. If ν is p-adic, we use the canonical embedding of $\mathbb{Q}_p/\mathbb{Z}_p$ into $\mathbb{Q}/\mathbb{Z}$ and of $\mathbb{Q}/\mathbb{Z}$ into $\mathbb{R}/\mathbb{Z}$ to define the character as follows*

$$\lambda_0 : \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}. \tag{15}$$

Now we can prove the following.

Proposition 5.2. *The bilinear map*

$$(x, y) \mapsto e^{2\pi i \lambda(xy)} \tag{16}$$

induces an identification of the additive group of k_ν and its own character group.

Proof. [Lang] □

We now define the additive Haar measures on the localization k_ν.

- dx = the ordinary Lebesgue measure if ν is real;
- dx = *twice* the ordinary Lebesgue measure if ν is complex;
- dx = the measure for which the ring of integers r_ν has a measure $N(\mathfrak{D})^{-1/2}$, if ν is $p-$adic.

In the last case the symbol $N(\mathfrak{D})$ denotes the norm of the *different* $\mathfrak{D}$. This ideal is important in the theory of local fields, however, here it is used merely to provide us with a normalizing constant, we included for completeness. Therefore, the reader must not be frustrated by it and can freely overlook it.[5]

We present our notion of a Fourier transform with the following theorem.

Theorem 5.3. *We define the fourier transform $\hat{f}$ of a function $f \in L_1(k_\nu)$ by*

$$\hat{f} = \int f(x) e^{-2\pi i \lambda(xy)} dx. \tag{17}$$

Then with our choice of measure the inversion formula

$$\hat{\hat{f}} = f(-x), \tag{18}$$

holds for f, such that $\hat{f}$ is also $L_1(k_\nu)$.

Proof. We know that the equality would hold up to some constant factor. Consequently, to prove it we much simply calculate the second Fourier transform of one particular non-zero function. For the real case we pick $f(x) = e^{-\pi x^2}$; for the complex case $f(x) = e^{-2\pi|x|^2}$; and for the p-adic case pick for $f(x)$ the characteristic function of r_ν. The details of the computations are given in [Lang]. □

[5]The precise definition of the different may be found in [Iwasawa] and its relevance to the constants in this section can be further checked in [Lang].

5.2.2 Local multiplicative theory

In this section we define the group of units U for the field k_ν as the set of elements of norm 1. For $\mathbb{R}$ it is the set $\{1, -1\}$ and for $\mathbb{C}$ it is the unit circle. For the p-adic case we have $U = r_\nu \setminus \mathfrak{p}$, where $\mathfrak{p}$ is the unique maximal ideal of the ring of integers r_ν. In this case U is open and in all cases it is compact.

Definition 5.4. *By a* quasi-character *of the field k_ν we mean a continuous homomorphism from $k_\nu^\times$ to the multiplicative group of complex numbers. If a quasi-character is trivial on the group U we say that it is unramified. A quasicharacter of absolute value one is a character in the usual sense.*

Theorem 5.5. *If k_ν is a localization of a number field and c is a quasi-character, there exist unique $s \in \mathbb{C}$ and character χ of $k_\nu^\times$, so that*

$$c(a) = \chi(a) \parallel a \parallel^s, \tag{19}$$

for every element $a \in k_\nu^\times$.

Proof. [Lang]. □

To define our local zeta functions we first choose a *multiplicative* Haar measure on $k_\nu^\times$ as follows:

- $d^*x = \frac{dx}{\|x\|}$ if ν is archimedean.
- $d^*x = \frac{Np}{Np-1}\frac{dx}{\|x\|}$ if ν is non-archimedean.

Here dx is the appropriate additive Haar measure we defined in the previous section. Np is the norm of the prime ideal p in the ring of integers of k. The constant in the second case is again simply for normalization. This choice gives us

$$\int_U d^*x = (N\mathfrak{D})^{-1/2}.$$

Finally, with our choice of a Haar measure we have.

Proposition 5.6. *A function $g(x)$ is in $L_1(k_\nu^\times)$ if and only if $g(x) \parallel x \parallel^{-1}$ is in $L_1(k_\nu \setminus \{0\})$. For such functions we have*

$$\int_{k_\nu^\times} g(x) d^*x = \int_{k_\nu \setminus \{0\}} g(x) \frac{dx}{\parallel x \parallel}. \tag{20}$$

Now we can proceed towards the definition and the properties of local zeta functions.

Definition 5.7. *We define the* Schwartz *space S on the field k_ν as the set of complex valued functions satisfying the following two properties*

$Z1_\nu$ *$f(x)$ and $\hat{f}(x)$ are continuous and $L_1(k_\nu)$.*

$Z2_\nu$ *$f(a) \parallel a \parallel^\sigma$ and $\hat{f}(a) \parallel a \parallel^\sigma$ are in $L_1(k_\nu^\times)$ for any $\sigma > 0$.*

For convenience we will use $f(a)$ as the restriction of $f(x)$ to $k_\nu^\times$.

Definition 5.8. (Local zeta function)
Let $f(x)$ be in S and let $c(a) = \chi(a) \parallel a \parallel^s$ be a quasi-character of k_ν. We define the following zeta function:

$$\zeta(f, c) = \zeta(f, \chi, s) = \int f(a)c(a)d^*a. \tag{21}$$

From our definition of S we know that ζ converges for $Re(s) > 0$.

For a quasi-character c we define its Fourier transform $\hat{c}(a) = \parallel a \parallel c^{-1}(a)$. Now we have the following lemma.

Lemma 5.9. *If $c(a) = \chi(a) \parallel a \parallel^s$ write $Re(c) = Re(s)$. If $0 < Re(c) < 1$ and $f, g \in S$, we have*

$$\zeta(f, c)\zeta(\hat{g}, \hat{c}) = \zeta(\hat{f}, \hat{c})\zeta(g, c). \tag{22}$$

Proof. We use that the multiplicative measure is invariant under the *shearing* automorphism $(a, b) \mapsto (a, ab)$ and the definition of the Fourier transforms $\hat{g}$ and $\hat{c}$. This allows us to transform $\zeta(f, c)\zeta(\hat{g}, \hat{c})$ as

$$\int f(a)\hat{g}(b)c(ab^{-1}) \parallel b \parallel \, d^*a \, d^*b =$$

$$\int f(a)\hat{g}(ab)c(b^{-1}) \parallel ab \parallel \, d^*a \, d^*b =$$

$$\int f(a)g(x)c(b^{-1})e^{-2\pi i\lambda(xab)} \, dx \, da \, db.$$

The last expression is obviously symmetric in g and f which proves the lemma. □

As long as there exists a function $f \in S$, such that $\zeta(\hat{f}, \hat{c})$ is non-zero, we can define the quotient $\zeta(f, c)/\zeta(\hat{f}, \hat{c})$. Then by lemma (5.9) this quotient would be a function of the character c, which does not depend on the choice of Schwarz function g. we shall denote this function $\rho(c)$. Unfortunately the computations that show the existence of the function f for which $\zeta(\hat{f}, \hat{c}) \neq 0$ are too long to be presented here. Therefore, again we refer the reader to [Lang] and simply cite the result.

Theorem 5.10. *A zeta function has an analytic continuation to the domain of all quasi-characters given by a functional equation*

$$\zeta(f, c) = \rho(c)\zeta(\hat{f}, \hat{c}). \tag{23}$$

The factor $\rho(c)$, independent of f, is a meromorphic function defined for $0 < Re(c) < 1$ by the above equation and for all other characters by analytic continuation. Further we immediately get the following properties of ρ:

1. $\rho(c)\rho(\hat{c}) = 1$;

2. $\rho(\bar{c}) = c(-1)\overline{\rho(c)}$;

3. *If* $Re(c) = 1/2$, *then* $|\rho(c)| = 1$.

This result concludes the local theory we need to introduce the Iwasawa-Tate method.

5.3 Global theory

5.3.1 Global additive duality

We begin by defining a global version of the map λ that we introduced in section (5.2.1). Let λ_ν be the local map on k_ν that we defined before. Then for any *idele* $x = (x_\nu)$ we define

$$\lambda(x) = \sum_\nu \lambda_\nu(x_\nu). \tag{24}$$

We immediately get the following result

Theorem 5.11. *The additive group of the Ring of adeles k_A is self-dual under the pairing*

$$< x, y > \mapsto e^{2\pi i \lambda(xy)}. \tag{25}$$

Similarly we define the quasicharacters of the group of ideles as $c(a) = \sum c_\nu(a_\nu)$ for any idele $a \in k_A^\times$. Naturally we put $\hat{c}(a) = |a|_A c^{-1}(a)$. If d^*a_ν is the local multiplicative Haar measure defined in the previous section we construct a global Haar measure on $k_A^\times$ as $d^*a = \prod d^*a_\nu$. Now we can define the *Schwartz* space on $k_A^\times$.

Definition 5.12. *A complex valued function f on the group of ideles is defined as the product of local functions f_ν. The global Fourier transform of $f(a)$ is defined as the product of the local Fourier transforms of its components. The function f is called a* Schwartz *function if it satisfies the following conditions*

*Z*1 *$f(x)$ and $\hat{f}(x)$ are continuous and $L_1(k_A^\times)$.*

*Z*2 *For ideles a and adeles x, ranging over compact subsets of the corresponding groups, the sums $\sum_{\alpha\in k} f(a(x+\alpha))$ and $\sum_{\alpha\in k} \hat{f}(a(x+\alpha))$ converge absolutely and uniformly.*

*Z*3 *$f(a) \parallel a \parallel^\sigma$ and $\hat{f}(a) \parallel a \parallel^\sigma$ are in $L_1(k_A^\times)$ for any $\sigma > 1$.*

We call the space of Schwartz *functions S.*

Now we can define the global zeta functions on the idele group.

Definition 5.13. *Let $f \in S$, c be a quasicharacter of $k_A^\times$. We define the following zeta function*

$$\zeta(f,c) = \zeta(f,\chi,s) = \int f(a)c(a)d^*a, \tag{26}$$

where χ is a character of $k_A^\times$ uniquely determined by $c(a) = \chi(a)|a|_A^s$.

5.3.2 The global functional equation and some further explanations

The following is the main theorem in Tate's Thesis and the main result in this section.

Theorem 5.14. (The Functional equation) *Any zeta function $\zeta(f,c)$ has analytic continuation to the domain of all quasicharacters. It is single valued and holomorphic except possibly at the points $c(a) = 1$ and $c(a) = |a|_A$.*[6] *The function satisfies the following functional equation*

$$\zeta(f,c) = \zeta(\hat{f},\hat{c}). \tag{27}$$

Proof. Since the proof of this result is very hard and long we refer the reader to [Lang]. □

The relation between the zeta functions over the idele group and the classical Dirichlet's zeta functions is not trivial. The particular details involve several notions, such as the different $\mathfrak{D}_p$ of k, for which we do not want to spend too much time. We simply mention that, if χ is a character of $k^\times$ and $L(s,\chi)$ is a Dirichlet's zeta function, we can find a function g_χ and constants a and b, depending on χ and k, such that

$$\zeta(g_\chi,\chi,s) = ba^s. \tag{28}$$

6 Conclusion

It is our hope that the current article have introduced the reader to the power of the adeles and ideles and their usefulness in different areas of number theory. As we have seen they may be used to directly simplify the proofs of several fundamental theorems such as the Class number theorem and Dirichlet's Unit theorem. Although adeles and ideles are not directly used in the proof of Mordell-Weil theorem presented in this paper, their relevance for the field of Elliptic curves is great. [Bump], [Gelbart] and [Lang] show how ideles are a common modern method to study the relation between automorphic forms and algebraic number theory. As we have seen in our brief discussion of the Iwasawa-Tate method the abstractness of the ideles is very useful for deriving

[6] Tate's theorem actually determines that the poles at these points are simple with residues $-\kappa f(0)$ and $\kappa\hat{f}(0)$, where κ is a constant depending only on the number field k that involves the class number, the discriminant and the conductor of k. See [Lang].

the functional equations and the complex continuation of different zeta functions that are of interest to number theorists.

Since the current article hardly does justice to the amazing applications of the adeles and ideles method in modern number theory we strongly encourage the readers interested to learn more about the subject to read the referred literature.

7 Acknowledgements

I would like to take the opportunity to thank my mentor Evan Jenkins for his great guidance and help that allowed me to prepare this project. I would like to thank Takashi Suzuki for suggesting the theme of my research and also helping me through the difficult parts of the subject. I would like to thank Prof. Paul Sally for being an outstanding tutor during this program in particular and during my college experience in general. I would like to thank Prof. Peter May for reviewing the current article and making many excellent suggestions for its improvement. Finally, I would like to thank the REU committee at the Department of Mathematics at The University of Chicago for their hard work in organizing this wonderful program.

References

[Weil] Weil, André, *Basic Number Theory*, Springer-Verlag, Berlin, (1974).

[Lang] Lang, Serge, *Algebraic Number Theory*,2nd ed., Springer, New York, (1994).

[Bump] Bump, Daniel, *Automorphic Forms and Representations*, Cambridge University Press, Cambridge, (1997).

[Gelbart] Gelbart, Stephen S., *Automorphic Forms on Adele Groups*, Princeton University Press, Princeton, (1975).

[Iwasawa] Iwasawa, Kenkichi, Local Class Field Theory, Oxford University Press, 1986.

[Silverman-Tate] Silverman, J. H., Tate, J., *Rational Points on Elliptic Curves*, Springer, New York, (1992).

[Ireland] Ireland, K., Rozen, M., *A Classical Introduction to Modern Number Theory*, 2^{nd} ed., Springer-Verlag, New York, (1990).

[Taylor] Frölich, A., Taylor, M. J., *Algebraic Number Theory*, Cambridge University Press, Cambridge, (1991).

[Thorne] Thorne, F., *Tate's Thesis*, lecture notes, Department of Mathematics, University of Wisconsin, Madison, Wisconsin, (2000).