THE IDELIC APPROACH TO NUMBER THEORY

TOM WESTON

1. Introduction

In classical algebraic number theory one embeds a number field into the cartesian product of its completions at its archimedean absolute values. This embedding is very useful in the proofs of several fundamental theorems. However, it was noticed by Chevalley and Weil that the situation was improved somewhat if the number field is embedded in the cartesian product of its completions at *all* of its absolute values. With a few additional restrictions, these objects are known as the *adeles*, and the units of this ring are called the *ideles.*

When considering the adeles and ideles, it is their topology as much as their algebraic structure that is of interest. Many important results in number theory translate into simple statements about the topologies of the adeles and ideles. For example, the finiteness of the ideal class group and the Dirichlet unit theorem are equivalent to a certain quotient of the ideles being compact and discrete.

We will begin by reviewing the construction of local fields, first algebraically and then topologically. We will then prove the basic global results combining all of the local data, namely the product formula and the approximation theorem. Next we will define the adeles and the ideles and prove their basic topological properties. We will then define the idele class group, and relate it to the usual ideal class group. We will conclude with proofs of the finiteness of the ideal class group and the Dirichlet unit theorem, using idelic methods.

I have tried in this paper to emphasize the topological details in these constructions, and hopefully have not ignored any important points. We will assume some familiarity with number fields, at the level of [3, Chapter 1], [4, Chapters 1-3] or [8, Chapter 1].

We fix the following notation throughout this paper: we let k be a number field (that is, a finite extension of $\mathbb{Q}$) of degree n over $\mathbb{Q}$. We let $\mathfrak{o}_k$ be the ring of integers of k. If $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}_k$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$, we write $e_\mathfrak{p}$ for the ramification degree and $f_\mathfrak{p}$ for the inertial degree of $\mathfrak{p}$ over p. That is, $e_\mathfrak{p}$ is the largest power of $\mathfrak{p}$ dividing $p\mathfrak{o}_k$, and $f_\mathfrak{p}$ is the degree of the residue field extension $\mathfrak{o}_k/\mathfrak{p}$ over $\mathbb{Z}/(p)$. If the prime $\mathfrak{p}$ is clear from context, then we will just write $e = e_\mathfrak{p}$ and $f = f_\mathfrak{p}$.

Part 1. Classical Algebraic Number Theory

2. Local Fields : Algebraic Description

Recall that the local ring $\mathfrak{o}_\mathfrak{p} \subseteq k$ is a discrete valuation ring. Let π be a uniformizing element of $\mathfrak{o}_\mathfrak{p}$; that is, π generates the unique non-zero prime ideal $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$ of $\mathfrak{o}_\mathfrak{p}$. Then any $\alpha \in k^*$ can be written as $\alpha = u\pi^m$ for a unique integer m and some unit u of $\mathfrak{o}_\mathfrak{p}^*$. We say that this m is the $\mathfrak{p}$-*adic valuation* $v_\mathfrak{p}(\alpha)$ of α. Setting

$v_{\mathfrak{p}}(0) = \infty$, we have defined a discrete valuation

$$v = v_{\mathfrak{p}} : k \to \mathbb{Z} \cup \{\infty\},$$

which is easily checked to satisfy the usual properties of a discrete valuation:

(1) $v_{\mathfrak{p}}(\alpha\beta) = v_{\mathfrak{p}}(\alpha) + v_{\mathfrak{p}}(\beta)$ for all $\alpha, \beta \in k$;
(2) $v_{\mathfrak{p}}(\alpha + \beta) \geq \min\{v_{\mathfrak{p}}(\alpha), v_{\mathfrak{p}}(\beta)\}$ for all $\alpha, \beta \in k$;
(3) $v_{\mathfrak{p}}(\alpha) = \infty$ if and only if $\alpha = 0$.

We use the standard conventions for arithmetic with ∞, including $\infty \cdot 0 = \infty$. $\mathfrak{o}_{\mathfrak{p}}$ is precisely the set of elements of k with nonnegative valuation; the units $\mathfrak{o}_{\mathfrak{p}}^*$ are precisely the elements of k^* with valuation 0. We also have

$$\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{o}_{\mathfrak{p}} = (\mathfrak{o}_k/\mathfrak{p})_{\mathfrak{p}\mathfrak{o}_k/\mathfrak{p}} = (\mathfrak{o}_k/\mathfrak{p})_{(0)} = \mathfrak{o}_k/\mathfrak{p}$$

since $\mathfrak{o}_k/\mathfrak{p}$ is already a field.

Note that $p = u\pi^e$ for some unit $u \in \mathfrak{o}_{\mathfrak{p}}^*$, so that

$$v_{\mathfrak{p}}(p) = e,$$

where e is the ramification degree of $\mathfrak{p}$.

We will now construct the completion of $\mathfrak{o}_{\mathfrak{p}}$. Let $A_m = \mathfrak{o}_{\mathfrak{p}}/(\pi^m)$. Then we have natural maps

$$\varphi_m : A_m \to A_{m-1}$$

given by simply considering a residue class modulo π^m modulo π^{m-1}. The A_m form an inverse system, and we define the $\mathfrak{p}$-*adic integers* $\mathfrak{o}_v$ to be the inverse limit of the A_m. That is, $\mathfrak{o}_v$ is the subset of elements $(a_1, a_2, \ldots)$ of the infinite product

$$\prod_{m=1}^{\infty} A_m$$

such that

$$\varphi_m(a_m) = a_{m-1}$$

for all m. It is easy to see that if (a_m) and (b_m) lie in $\mathfrak{o}_v$, then so do $(a_m + b_m)$ and $(a_m b_m)$, so $\mathfrak{o}_v$ inherits a ring structure from $\prod_{m=1}^{\infty} A_m$.

Note that we have natural inclusions

$$\mathfrak{o}_k \hookrightarrow \mathfrak{o}_{\mathfrak{p}} \hookrightarrow \mathfrak{o}_v$$

given by sending $\alpha \in \mathfrak{o}_{\mathfrak{p}}$ to $(\bar{\alpha}, \bar{\alpha}, \ldots) \in \mathfrak{o}_v$. These are clearly ring homomorphisms, so $\mathfrak{o}_k$ and $\mathfrak{o}_{\mathfrak{p}}$, are naturally subrings of $\mathfrak{o}_v$.

We would like to have a better way to think of elements of $\mathfrak{o}_v$. To do this, first fix representatives $0 = c_0, \ldots, c_{p^f-1} \in \mathfrak{o}_{\mathfrak{p}}$ of the residue classes in the finite field $\mathfrak{o}_{\mathfrak{p}}/(\pi) \cong \mathfrak{o}_k/\mathfrak{p}$. (In the case where $\mathfrak{o}_{\mathfrak{p}}/(\pi) = \mathbb{F}_p$ we have the standard representatives $0, 1, \ldots, p-1$, but in general there are no such obvious choices.) Now, take any element $a = (a_m)$ of $\mathfrak{o}_v$. There is then a unique c_{i_0} such that

$$a_1 \equiv c_{i_0} \pmod{\pi}.$$

Next consider $a - c_{i_0} = (a_m - c_{i_0}) \in \mathfrak{o}_v$, The first coordinate of $a - c_{i_0}$ will be 0, and thus divisible by π. It follows from the compatibility of the $(a_m - c_{i_0})$ under

the φ_m that each $a_m - c_{i_0}$ is then divisible by π. Thus, we can write

$$\begin{aligned} a - c_{i_0} &= (a_m - c_{i_0}) \\ &= (\pi a'_m) \\ &= \pi(a'_m) \\ &= \pi a' \end{aligned}$$

for some $a' = (a'_m)$ in $\mathfrak{o}_v$. Repeating this procedure, we can write

$$a' - c_{i_1} = \pi a''$$

for some unique c_{i_1} and some $a'' \in \mathfrak{o}_v$.

Continuing this and combining all of the terms, we have

$$\begin{aligned} a &= c_{i_0} + (a - c_{i_0}) \\ &= c_{i_0} + \pi a' \\ &= c_{i_0} + \pi\left(c_{i_1} + (a' - c_{i_1})\right) \\ &= c_{i_0} + c_{i_1}\pi + \pi\big(\pi(c_{i_2} + (a'' - c_{i_2}))\big) \\ &= c_{i_0} + c_{i_1}\pi + c_{i_2}\pi^2 + \cdots \end{aligned}$$

for some uniquely determined $c_{i_0}, c_{i_1}, c_{i_2}, \ldots$, each chosen from our fixed set of representatives. Further, it is clear that any such expression

$$\sum_{m=0}^{\infty} c_{i_m}\pi^m$$

corresponds to some $a = (a_m) \in \mathfrak{o}_v$ by setting

$$a_m \equiv c_{i_0} + c_{i_1}\pi + \cdots + c_{i_{m-1}}\pi^{m-1} \pmod{\pi^m}.$$

Thus, we can think of the elements of $\mathfrak{o}_v$ as some sort of infinite power series in the uniformizing element π, with coefficients chosen from representatives of the finite field $\mathfrak{o}_\mathfrak{p}/(\pi) = \mathfrak{o}_k/\mathfrak{p}$. We will think of the c_{i_m} as the digits of $x \in \mathfrak{o}_v$.

Writing elements of $\mathfrak{o}_v$ in this form, it is now clear how to extend our discrete valuation $v_\mathfrak{p}$ to $\mathfrak{o}_v$: given any element

$$a = c_{i_0} + c_{i_1}\pi + c_{i_2}\pi^2 + \cdots$$

of $\mathfrak{o}_v$, we define $v_\mathfrak{p}(a) = m$, where π^m is the first power of π with a non-zero coefficient. It is easy to see that $v_\mathfrak{p}$ agrees with our original discrete valuation on the image of $\mathfrak{o}_\mathfrak{p}$ in $\mathfrak{o}_v$, and that it still satisfies the axioms of a discrete valuation. Therefore, $\mathfrak{o}_v$ is a discrete valuation ring. The maximal ideal $\mathfrak{p}_v$ of $\mathfrak{o}_v$ is generated by any element of valuation 1; for example, our original uniformizer π. Thus, $\mathfrak{p}_v = \mathfrak{p}\mathfrak{o}_v$. Further, it is clear from our expansion of elements of $\mathfrak{o}_v$ in terms of π that

$$\mathfrak{o}_v/\mathfrak{p}_v \cong \mathfrak{o}_\mathfrak{p}/\mathfrak{p}\mathfrak{o}_\mathfrak{p} \cong \mathfrak{o}_k/\mathfrak{p},$$

so that all of the residue fields coincide.

The units $\mathfrak{o}_v^*$ of $\mathfrak{o}_v$ are precisely those elements of $\mathfrak{o}_v$ of valuation 0, and the non-units $\mathfrak{p}$ are precisely those elements of $\mathfrak{o}_v$ divisible by π. Since any element of $\mathfrak{o}_v$ can be written as $u\pi^m$ for some $u \in \mathfrak{o}_v^*$ and some nonnegative integer n, the field of fractions of $\mathfrak{o}_v$ is obtained simply by inverting π. We write k_v for this field; then we have

$$k_v = \mathfrak{o}_v[\pi^{-1}].$$

Therefore, elements x of k_v have the form

$$x = \sum_{m=m_0}^{\infty} c_{i_m} \pi^m$$

for some integer m_0. If we require that $c_{i_{m_0}} \neq 0$, then m_0 is just $v_{\mathfrak{p}}(x)$.

Since k is the field of fractions of $\mathfrak{o}_{\mathfrak{p}}$, and $\mathfrak{o}_{\mathfrak{p}}$ embeds in $\mathfrak{o}_v$, k must embed in k_v.

3. Local Fields : Topological Description

We remain in the situation of the preceding section; that is, we have a number field k and a prime $\mathfrak{p}$ of the ring of integers $\mathfrak{o}_k$ lying over a prime p of $\mathbb{Z}$, and we let $v = v_{\mathfrak{p}}$ be the corresponding discrete valuation on k. In this section we will give a topological description of the completion k_v, in terms of the valuation $v_{\mathfrak{p}}$.

First, observe that the valuation v induces a norm $\| \cdot \|_v$ on k by

$$\| \alpha \|_v = p^{-fv(\alpha)}.$$

(We could have set $\| \alpha \|_v = c^{v(\alpha)}$ for any real constant c between 0 and 1; it does not matter for the purposes of this section. However, the choice $c = p^{-f}$ is necessary for the product formula of Section 4. For the moment, note that the residue class ring $\mathfrak{o}_{\mathfrak{p}}/(\alpha)$ has size $1/\| \alpha \|_v$, so this choice of c has at least something recommending it.) It follows immediately from the axioms of a discrete valuation that $\| \cdot \|_v$ satisfies the axioms of a norm :

(1) $\| \alpha\beta \|_v = \| \alpha \|_v \| \beta \|_v$ for all $\alpha, \beta \in k$;
(2) $\| \alpha + \beta \|_v \leq \| \alpha \|_v + \| \beta \|_v$ for all $\alpha, \beta \in k$.

In fact, $\| \cdot \|_v$ satisfies the stronger axiom

(3) $\| \alpha + \beta \|_v \leq \min\{\| \alpha \|_v, \| \beta \|_v\}$ for all $\alpha, \beta \in k$.

For this reason we call $\| \cdot \|_v$ a *non-archimedean* norm.

We can now in the usual way use $\| \cdot \|_v$ to give us a metric on k, defined by

$$d_v(\alpha, \beta) = \| \alpha - \beta \|_v \ .$$

This then gives us a topology on k. One can now define the completion of k with respect to v to be the usual completion of a metric space, in terms of equivalence classes of Cauchy sequences. This in fact gives rise to exactly the field k_v we constructed in Section 2. We will not go through the construction here; for a detailed exposition of it, see [2, Chapter 1, Section 4]. We will instead show that our algebraically constructed field of Section 2 has the necessary topological properties.

Note that we can use the discrete valuation on our field k_v of Section 2 to define a metric on it, which will agree with the metric defined above on the subfield k. We will show that under this topology k_v is a complete, locally compact topological ring, with compact subsets $\mathfrak{o}_v$ and $\mathfrak{o}_v^*$.

Let us describe the basic open sets on k_v; these are simply the open balls

$$B(x, r) = \{y \in k_v; \| x - y \|_v < r\}.$$

First, note that since our metric takes on only a discrete set of values, for any r there is some small ε so that

$$B(x, r) = \overline{B(x, r - \varepsilon)},$$

if ε is chosen small enough so that the metric does not take on any values between $r-\varepsilon$ and r. Thus every basic open set is also closed. (Of course, it does not follow that *every* open set is also closed.)

Next, let us consider in more detail the open balls around $0 \in k_v$. It is enough to consider the balls

$$B(0, p^{-fs})$$

for integral s, since these are the only values the metric takes. An element y of k_v satisfies $\| y - 0 \|_v < p^{-fs}$ if and only if $v_{\mathfrak{p}}(y) > s$; that is, if and only if y has the form

$$\sum_{m=s+1}^{\infty} c_{i_m} \pi^m.$$

Thus, the ball $B(0, p^{-fs})$ consists precisely of those y which have coefficients 0 up to (and including) the coefficient of π^s. In the same way, for any $x \in k_v$, the ball $B(x, p^{-fs})$ consists of those $y \in k_v$ agreeing with x up to (and including) the coefficient of π^s.

In particular, we see that

$$\mathfrak{o}_v = B(0, p^f)$$

and

$$\mathfrak{p}_v = B(0, 1)$$

are open and closed subsets of k_v. Then

$$\mathfrak{o}_v^* = \mathfrak{o}_v - \mathfrak{p}_v$$

is open and closed as well.

We can actually describe the induced topology on $\mathfrak{o}_v$ in a different way. Recall that we defined $\mathfrak{o}_v$ to be a subset of an infinite product

$$\prod_{m=1}^{\infty} A_m.$$

Each set A_m is finite, and we give it the discrete topology. We then give $\prod_{m=1}^{\infty} A_m$ the product topology, and $\mathfrak{o}_v$ the topology it inherits as a subspace.

Let us now try to describe the basic open sets in this topology. They have the form

$$\prod_{m=1}^{\infty} B_m \cap \mathfrak{o}_v$$

where B_m is any subset of A_m, and $B_m = A_m$ for all but finitely many m. Equivalently, they are the sets of the form

$$\left(\prod_{m=1}^{m_0} B_m \times \prod_{m > m_0} A_m \right) \cap \mathfrak{o}_v \tag{1}$$

for positive integers m_0, where the B_m are any subsets of A_m. Now, consider any set U of the form (1), and pick any point x in it. It is then clear that

$$x \in B(x, p^{-f(m_0-1)}) \subseteq U,$$

so that U is open in the metric topology on $\mathfrak{o}_v$.

Conversely, consider any open ball $B(x, p^{-fs})$ in the metric topology. Such a set is actually of the form (1), taking $m_0 = s+1$ and the first $s+1$ B_m to be a single point. We therefore have established:

Proposition 3.1. *The two topologies we have defined on $\mathfrak{o}_v$ are the same.*

We are now ready to give the fundamental topological description of k_v.

Theorem 3.2. *k_v is a locally compact, complete topological field, with compact open and closed subsets $\mathfrak{o}_v$ and $\mathfrak{o}_v^*$.*

Proof. To say that k_v is a topological field is to say that addition, negation, multiplication and inversion are all continuous maps. The proofs of these facts are nearly identical to the proofs of the corresponding facts for the real numbers $\mathbb{R}$; in fact, the non-archimedean nature of our norm makes the proofs even easier.

Next we will show that $\mathfrak{o}_v$ is compact. This is easy, using our alternate description of the topology on $\mathfrak{o}_v$: each finite set A_m is compact, so by the Tychonoff theorem, $\prod_{m=1}^{\infty} A_m$ is compact. Thus it is enough to show that $\mathfrak{o}_v$ is closed as a subspace of $\prod_{m=1}^{\infty} A_m$. So take $(a_m) \notin \mathfrak{o}_v$. Then there is an m_0 with $\varphi_{m_0}(a_{m_0}) \neq a_{m_0-1}$. Consider the set

$$\{a_1\} \times \{a_2\} \times \cdots \times \{a_{m_0}\} \times \prod_{m>m_0} A_m.$$

This is open in the product topology, and it is disjoint from $\mathfrak{o}_v$ since every point in it has the same incompatible beginning. Thus, the complement of $\mathfrak{o}_v$ is open, so $\mathfrak{o}_v$ is closed, and thus compact.

Since $\mathfrak{o}_v^*$ is a closed subset of the compact set $\mathfrak{o}_v$, it is also compact. In fact, every basic open subset of k_v is compact, since we have a homeomorphism

$$\psi : B(x, p^{-fs}) \to B(0, p^f) = \mathfrak{o}_v$$

given by $\psi(y) = \pi^{-s-1}(y - x)$. ($\psi$ is continuous since k_v is a topological field, and it is easy to see that it is bijective.) This shows that k_v is locally compact. Finally, since k_v is locally compact, it is complete. □

Proposition 3.3. *$\mathfrak{o}_v^*$, $\mathfrak{o}_v$ and k_v are the topological closures of $\mathfrak{o}_k^*$, $\mathfrak{o}_k$ and k respectively.*

Proof. Since we clearly have $\mathfrak{o}_k^* \subseteq \mathfrak{o}_v^*$, $\mathfrak{o}_k \subseteq \mathfrak{o}_v$ and $k \subseteq k_v$ and the larger sets are all closed, it is enough to show that any element of the larger set can be arbitrarily closely approximated by an element of the smaller set. But this is clear; for example, if we pick our representatives c_i to all lie in $\mathfrak{o}_k$ (which we can do since $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}\mathfrak{o}_\mathfrak{p} = \mathfrak{o}_k/\mathfrak{p}$), as well as π, then given $x = \sum_{m=0}^{\infty} c_{i_m}\pi^m \in \mathfrak{o}_v$, the sequence

$$(c_{i_0}, c_{i_0} + c_{i_1}\pi, c_{i_0} + c_{i_1}\pi + c_{i_2}\pi^2, \ldots)$$

of elements of $\mathfrak{o}_k$ converges to x. □

Note that since $\mathfrak{o}_k^* \subseteq \mathfrak{o}_\mathfrak{p}^* \subseteq \mathfrak{o}_v^*$ and $\mathfrak{o}_k \subseteq \mathfrak{o}_\mathfrak{p} \subseteq \mathfrak{o}_v$, we also have $\overline{\mathfrak{o}_\mathfrak{p}^*} = \mathfrak{o}_v^*$ and $\overline{\mathfrak{o}_\mathfrak{p}} = \mathfrak{o}_v$.

4. Global Fields

We will now consider the description of k in terms of local data. Each prime $\mathfrak{p}$ gives rise to a valuation $v_\mathfrak{p}$ on k, and thus to a non-archimedean absolute value $\|\cdot\|_{v_\mathfrak{p}}$ on k. We also have archimedean absolute values arising from the embeddings of k in $\mathbb{C}$. Precisely, if

$$\sigma : k \hookrightarrow \mathbb{C}$$

is an embedding, then we have an absolute value $\|\cdot\|_\sigma$ on k given by

$$\|\alpha\|_\sigma = |\sigma(\alpha)|,$$

where $|\cdot|$ is the usual absolute value on $\mathbb{C}$.

Lemma 4.1. *If σ_1 and σ_2 are two different embeddings of k into $\mathbb{C}$ and $\|\alpha\|_{\sigma_1}=\|\alpha\|_{\sigma_2}$ for all $\alpha \in k$, then $\sigma_1 = \overline{\sigma_2}$.*

Proof. Pick $\alpha \in k$ such that $k = \mathbb{Q}(\alpha)$. Set $\sigma_i(\alpha) = x_i + y_i i$. Then, since $|\sigma_1(\alpha)| = |\sigma_2(\alpha)|$, we have

$$x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Further,

$$\begin{aligned} |\sigma_1(\alpha+1)| &= |\sigma_2(\alpha+1)| \\ |\sigma_1(\alpha)+1| &= |\sigma_2(\alpha)+1| \\ |(x_1+1)+y_1 i| &= |(x_2+1)+y_2 i| \\ x_1^2+2x_1+1+y_1^2 &= x_2^2+2x_2+1+y_2^2. \end{aligned}$$

Combining these two equations, we have

$$2x_1 + 1 = 2x_2 + 1,$$

so that $x_1 = x_2$. Therefore $y_1 = \pm y_2$, and since $\sigma_1 \neq \sigma_2$ we must have $y_1 = -y_2$. Since α generates k over $\mathbb{Q}$, this implies that $\sigma_1 = \overline{\sigma_2}$, as desired. □

Now, if σ is a real embedding of k (meaning that the image of σ lies in $\mathbb{R}$), then $\sigma = \overline{\sigma}$, so we get exactly one absolute value from this embedding. If σ is complex (meaning that the image of σ is strictly larger than $\mathbb{R}$), then σ and $\overline{\sigma}$ are distinct embeddings of k into $\mathbb{C}$, giving rise to the same absolute value. Lemma 4.1 guarantees that this is the only situation in which this can happen. Thus, if k has r_1 real embeddings and r_2 pairs of complex conjugate embeddings, then we have $r_1 + 2r_2 = n$, but we get only $r_1 + r_2$ distinct absolute values.

We define the *canonical set* M_k of k to be the set of all of these absolute values : one non-archimedean absolute value for each prime $\mathfrak{p}$ (normalized as in Section 3), one archimedean absolute value for each real embedding and one archimedean absolute value for each pair of complex conjugate embeddings. We denote by S_∞ the subset of M_k of archimedean valuations. These absolute values are all independent, in the sense that they induce different topologies on k. We will prove this fact later, while proving the approximation theorem.

To simplify notation, we will use v for both embeddings and valuations, so that we can write $\|\cdot\|_v$ for any of the absolute values of M_k, not just the non-archimedean ones. We will also say valuation even when we more properly mean absolute value; in particular, we will often use $v \in M_k$ to mean $\|\cdot\|_v \in M_k$.

Note that if v is a real embedding, then the (topological) completion k_v of k with respect to $\|\cdot\|_v$ is $\mathbb{R}$, since $\mathbb{Q} \subseteq k \subset \mathbb{R}$, and the completion of $\mathbb{Q}$ is $\mathbb{R}$. Similarly, if v is a complex embedding, then the completion k_v of k with respect to $\|\cdot\|_v$ is $\mathbb{C}$. If we let $v_1, \ldots, v_{r_1}$ be the real embeddings and $v_{r_1+1}, \overline{v_{r_1+1}}, \ldots, v_{r_1+r_2}, \overline{v_{r_1+r_2}}$ be the complex embeddings of k, then, thinking of each $\mathbb{C}$ as $\mathbb{R}^2$, we have

$$\prod_{i=1}^{r_1+r_2} k_v = \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=r_1+1}^{r_1+r_2} \mathbb{R}^2 = \mathbb{R}^n.$$

Since k embeds in each k_v, k has a natural embedding in this $\mathbb{R}^n$. It is this embedding which is used classically.

We will now prove the product formula, which is an important relation between the absolute values in M_k. We will need a lemma.

Lemma 4.2. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be the primes of $\mathfrak{o}_k$ lying over $p \in \mathbb{Z}$. Let $v_1, \dots, v_m$ be the corresponding valuations on k, and let v be the p-adic valuation on $\mathbb{Q}$. Then for any $\alpha \in k^*$,*

$$\| N(\alpha) \|_v = \prod_{i=1}^{m} \| \alpha \|_{v_i},$$

where N is the norm from k to $\mathbb{Q}$.

Proof. By unique factorization of fractional ideals we can write

$$(\alpha) = \prod_{i=1}^{m} \mathfrak{p}_i^{n_i} \times I'$$

for some fractional ideal I' prime to $\mathfrak{p}_1, \dots, \mathfrak{p}_m$. Then $n_i = v_i(\alpha)$, so $\| \alpha \|_{v_i} = p^{-f_i n_i}$, where f_i is the inertial degree of $\mathfrak{p}_i$ over p. Therefore,

$$\prod_{i=1}^{m} \| \alpha \|_{v_i} = p^{-\sum_{i=1}^{m} f_i n_i}.$$

Now, since the norm is multiplicative and $N(\mathfrak{p}_i) = p^{f_i}$, we have

$$N(\alpha) = p^{\sum_{i=1}^{m} f_i n_i} \cdot N(I').$$

$N(I')$ is prime to p, so this has p-adic absolute value

$$p^{-\sum_{i=1}^{m} f_i n_i},$$

which proves the lemma. □

Note that if $\alpha \in k$, then

$$N(\alpha) = \prod_{\sigma : k \hookrightarrow \mathbb{C}} |\sigma(\alpha)| = \prod_{v \in S_\infty, v \text{ real}} \| \alpha \|_v \cdot \prod_{v \in S_\infty, v \text{ complex}} \| \alpha \|_v^2 .$$

If we define $n_v = 1$ for v real (and also, for later use, for v non-archimedean) and $n_v = 2$ for v complex, then this takes the form

$$N(\alpha) = \prod_{v \in S_\infty} \| \alpha \|_v^{n_v} .$$

Theorem 4.3 (The Product Formula)**.** *For all $\alpha \in k^*$,*

$$\prod_{v \in M_k} \| \alpha \|_v^{n_v} = 1.$$

(Note that this infinite product makes sense, since $v(\alpha) = 0$ (and therefore $\| \alpha \|_v = 1$) for all but finitely many $v \in M_k$.)

Proof. We first prove this formula in the case $k = \mathbb{Q}$. In this case it is enough to check it for $\alpha = p$ a prime number, since both sides are multiplicative. But then $\| \alpha \|_{v_q} = 1$ for $q \neq p$, so the only two terms which contribute to the product are $\| \alpha \|_{v_p} = 1/p$ and the standard absolute value $|\alpha| = p$, which multiply to 1. This proves the formula for $k = \mathbb{Q}$.

Now let k be any number field. Then

$$\begin{aligned}\prod_{v\in M_k} \|\alpha\|_v^{n_v} &= \prod_{v\in M_k - S_\infty} \|\alpha\|_v \cdot \prod_{v\in S_\infty} \|\alpha\|_v^{n_v} \\ &= \prod_{\mathfrak{p}} \|\alpha\|_{v_\mathfrak{p}} \cdot N(\alpha) \\ &= \prod_{p}\prod_{\mathfrak{p}|p} \|\alpha\|_{v_\mathfrak{p}} \cdot N(\alpha) \\ &= \prod_{p} \|N(\alpha)\|_{v_p} \cdot N(\alpha) \\ &= \prod_{v\in M_\mathbb{Q}} \|N(\alpha)\|_v \\ &= 1\end{aligned}$$

since we know the product formula for $\mathbb{Q}$. □

We chose the normalization we did on the absolute values $\|\cdot\|_v$ in order to get the product formula to work out.

Next we will need some way to find elements of k satisfying certain local conditions. The standard result along these lines is the approximation theorem. We will prove it through a sequence of lemmas.

Lemma 4.4. *For any distinct $v_1, v_2 \in M_k$, there exists $\alpha \in k$ with $\|\alpha\|_{v_1} > 1$ and $\|\alpha\|_{v_2} < 1$.*

Proof. If both v_1 and v_2 are non-archimedean, say $v_1 = v_{\mathfrak{p}_1}$ and $v_2 = v_{\mathfrak{p}_2}$, then pick $\alpha \in \mathfrak{p}_2 - \mathfrak{p}_1$ and $\beta \in \mathfrak{p}_1 - \mathfrak{p}_2$. (These must exist since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are maximal ideals.) We must have $\|\alpha\|_{v_1} \geq 1$, $\|\alpha\|_{v_2} < 1$, $\|\beta\|_{v_1} < 1$ and $\|\beta\|_{v_2} \geq 1$. If $\|\alpha\|_{v_1} \neq 1$, then α will work; if $\|\beta\|_{v_2} \neq 1$, then β^{-1} will work. If $\|\alpha\|_{v_1} = \|\beta\|_{v_2} = 1$, then $\alpha\beta^{-1}$ will work.

If v_1 is archimedean and v_2 is non-archimedean, say $v_2 = v_\mathfrak{p}$, then any non-zero element of $\mathfrak{p} \cap \mathbb{Z}$ will work. In the opposite case, the inverse of any non-zero element of $\mathfrak{p} \cap \mathbb{Z}$ works.

This leaves the case where both v_1 and v_2 are archimedean. By Lemma 4.1 we know that there is $\alpha \in k$ with $\|\alpha\|_{v_1} \neq \|\alpha\|_{v_2}$. Suppose that $\|\alpha\|_{v_1} > \|\alpha\|_{v_2}$. Pick some rational number r in between. Then α/r will satisfy the conditions of the lemma. If we have the opposite inequality, then r/α will work. □

Corollary 4.5. *Any two distinct $v_1, v_2 \in M_k$ induce different topologies on k.*

Proof. Note that for any absolute value $\|\cdot\|_v$, the ball $B(0,1)$ is precisely the set of $\alpha \in k$ with $\lim_{m\to\infty} \alpha^m = 0$. Thus $B(0,1)$ depends only on the topology, and not on the metric. But by Lemma 4.4, $B_{v_1}(0,1)$ and $B_{v_2}(0,1)$ are different, so v_1 and v_2 must induce different topologies. □

Lemma 4.6. *Let v_1, v_2 be distinct elements of M_k. Suppose $\alpha \in k$ satisfies $\|\alpha\|_{v_1} > 1$ and $\|\alpha\|_{v_2} < 1$. Then the sequence*

$$z_m = \frac{\alpha^m}{1+\alpha^m}$$

converges to 1 with respect to v_1 and converges to 0 with respect to v_2.

Proof. This is intuitively quite clear, since the denominator is dominated by α^m with respect to v_1 and by 1 with respect to v_2. We will leave the details to the reader. □

Lemma 4.7. *For any distinct $v_1, v_2, \dots, v_s \in M_k$, there exists $\alpha \in k$ with $\| \alpha \|_{v_1} > 1$ and $\| \alpha \|_{v_i} < 1$ for $i = 2, \dots, s$.*

Proof. We prove this by induction on s. The case $s = 2$ is Lemma 4.4. Now, suppose we have $\alpha \in k$ with $\| \alpha \|_{v_1} > 1$ and $\| \alpha \|_{v_i} < 1$ for $i = 2, \dots, s-1$. If $\| \alpha \|_{v_s} < 1$, then we are done. If $\| \alpha \|_{v_s} = 1$, then pick $y \in k$ with $\| y \|_{v_1} > 1$ and $\| y \|_{v_s} < 1$. Then for large enough m, $\alpha^m y$ will satisfy the necessary conditions, since $\| \alpha^m \|_{v_i}$ can be made arbitrarily small for $i = 2, \dots, s-1$.

This leaves the case where $\| \alpha \|_{v_s} > 1$. By Lemma 4.6 the sequence

$$z_m = \frac{\alpha^m}{1 + \alpha^m}$$

will converge to 1 with respect to v_1 and v_s, and will converge to 0 with respect to $v_2, \dots, v_{s-1}$. Using Lemma 4.4 to pick $y \in k$ with $\| y \|_{v_1} > 1$ and $\| y \|_{v_s} < 1$, we then see that for sufficiently large m the element $z_m y$ will satisfy the conditions of the lemma. □

Theorem 4.8 (The Approximation Theorem)**.** *For any distinct $v_1, v_2, \dots, v_s \in M_k$, $\alpha_1, \dots, \alpha_s \in k$ and $\varepsilon > 0$ there exists $\alpha \in k$ satisfying*

$$\| \alpha - \alpha_i \|_{v_i} < \varepsilon$$

for all i.

Proof. By Lemma 4.7 we can find $y_i \in k$ with $\| y_i \|_{v_i} > 1$ and $\| y_i \|_{v_j} < 1$ for $j \neq i$. Then using Lemma 4.6 we can find $z_1, \dots, z_s \in k$ with z_i arbitrarily close to 1 with respect to v_i and arbitrarily close to 0 with respect to v_j, $j \neq i$. The element $\alpha = z_1 \alpha_1 + \dots + z_s \alpha_s$ will then satisfy the conditions of the theorem, since

$$\| \alpha - \alpha_i \|_{v_i} \leq \| z_1 \|_{v_i} \| \alpha_1 \|_{v_i} + \dots + \| z_i - 1 \|_{v_i} \| \alpha_i \|_{v_i} + \dots + \| z_s \|_{v_i} \| \alpha_s \|_{v_i}$$

which we can make arbitrarily small. □

Part 2. Adeles and Ideles

5. Adeles

We continue to let k be a number field of degree n over $\mathbb{Q}$. Let M_k be its canonical set of absolute values. In analogy with our embedding of k into $\mathbb{R}^n$ in the previous section, we would like to embed k into the product of its completions k_v at all $v \in M_k$. However, we need to restrict this product somewhat, in order to respect the important property that any $\alpha \in k$ is a $\mathfrak{p}$-adic integer for all but finitely many primes $\mathfrak{p}$ of $\mathfrak{o}_k$.

We will do this as follows: First, consider the usual direct product

$$\prod_{v \in M_k} k_v.$$

We define the *adeles* A to be the subset of this direct product consisting of $a = (a_v)_{v \in M_k}$ with a_v a $\mathfrak{p}$-adic integer for all but finitely many of the non-archimedean valuations $v_\mathfrak{p}$. (We do not impose any restriction on the components of a_v at

archimedean valuations.) However, we do not give A the subspace topology; we take as our basis of open sets sets of the form

$$\prod_{v \in M_k} U_v$$

where $U_v \subseteq k_v$ is open in k_v for all $v \in M_k$, and $U_v = \mathfrak{o}_v$ for all but finitely many $v \in M_k$. (We will always assume that in any such condition the archimedean absolute values are included in the finite excluded set.) We can write such a set as

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathfrak{o}_v \tag{2}$$

where S is some finite subset of M_k, which we take to include S_∞, and each U_v is an open subset of k_v.

A is said to be the *restricted direct product* of the k_v with respect to the $\mathfrak{o}_v$. A inherits a ring structure from the direct product, so that operations are done componentwise.

Note that we can actually take our basis of open sets to be sets of the form (2) with each U_v a basic open set of k_v. The simplest such sets are the sets

$$A_S = \prod_{v \in S} k_v \times \prod_{v \notin S} \mathfrak{o}_v,$$

where S is some finite subset of M_k containing S_∞. The product $\prod_{v \notin S} \mathfrak{o}_v$ is a product of compact sets, and thus compact by the Tychonoff theorem. A_S is therefore a finite product of locally compact sets, and thus is locally compact. Since any $x \in A$ certainly lies in some A_S (take S to be the finite set of valuations v at which x does not lie in $\mathfrak{o}_v$), it follows that the space A is locally compact. This would not be the case if we had given A the subspace topology.

The sets A_S are actually closed as well; given any $a \notin A_S$, we must either have $a_{v_0} \notin U_{v_0}$ for some $v_0 \in S$, or else $a_{v_0} \notin \mathfrak{o}_{v_0}$ for $v_0 \notin S$. In the first case take a neighborhood of a with v_0-component disjoint from U_{v_0}; in the second, take a neighborhood of a with v_0-component disjoint from $\mathfrak{o}_{v_0}$. This gives us a neighborhood of a disjoint from A_S, so A_S is closed.

Proposition 5.1. *The adeles A are a topological ring.*

Proof. We will show that addition is continuous; negation and multiplication are similar. So, let $f : A \times A \to A$ be defined by $f(a, b) = a + b$. Let U be some basic open set of the form

$$\prod_{v \in S} B(c_v, r_v) \times \prod_{v \notin S} \mathfrak{o}_v$$

where S is some finite subset of M_k containing S_∞. We must show that $f^{-1}(U)$ is open in $A \times A$.

Pick $(a, b) \in f^{-1}(U)$. Then

$$\| a_v + b_v - c_v \|_v < r_v$$

for all $v \in S$. Now, define sets $U_1, U_2 \in A$ by

$$U_1 = \prod_{v \in S} B\left(a_v, \frac{r_v}{4}\right) \times \prod_{v \notin S} \mathfrak{o}_v$$

and

$$U_2 = \prod_{v \in S} B\left(b_v, \frac{r_v}{4}\right) \times \prod_{v \notin S} \mathfrak{o}_v.$$

Then U_1 and U_2 are both open in A, so $U_1 \times U_2$ is open in $A \times A$. The v-component of $f(U_1 \times U_2)$ is just $\mathfrak{o}_v$ for $v \notin S$, and is contained in $B(a_v + b_v, r_v/2)$, which in turn is contained in $B(c_v, r_v)$, for $v \in S$. Thus $(a, b) \in U_1 \times U_2 \subseteq f^{-1}(U)$. Therefore $f^{-1}(U)$ is open, and f is continuous. □

Note that we have a natural embedding of k into A, sending each $\alpha \in k$ to the vector $(\alpha, \alpha, \ldots) \in A$. This is well-defined, since any $\alpha \in k$ is a $\mathfrak{p}$-adic integer for all but finitely many primes $\mathfrak{p}$. We give k the subspace topology.

Proposition 5.2. *k is embedded as a discrete subring of the adeles A.*

Proof. k is a topological subring of A since we have given it the subspace topology. It remains to show that it is discrete. We will show that 0 has a neighborhood disjoint from $k - \{0\}$, and the general case follows by translation.

Define a set $U = \prod_{v \in M_k} U_v$ by taking $U_v = \mathfrak{o}_v$ for all non-archimedean $v \in M_k$, and $U_v = B(0, 1/2)$ for all $v \in S_\infty$. Then U is a basic open neighborhood of 0. Suppose there is a non-zero $\alpha \in U \cap k$. Then $\| \alpha \|_v \leq 1$ for all non-archimedean v, and $\| \alpha \|_v < 1/2$ for all archimedean v. Thus,

$$\prod_{v \in M_k} \| \alpha \|_v^{n_v} < \frac{1}{2}.$$

But this contradicts the product formula, since this product is always 1 for non-zero α. Thus, $U \cap k = 0$, which shows that $\{0\}$ is open in k, and thus that k is discrete. □

We also have embeddings of k_v into A for each $v \in M_k$ given by sending $x \in k_v$ to $(0, \ldots, x, \ldots) \in A$, with the x in the v-component.

Proposition 5.3. *This embeds k_v as a closed subring of A, and the topology k_v inherits as a subspace of A is just the usual topology on k_v.*

Proof. It is clear that k_v inherits its usual topology, since $U_v \times \prod_{v' \in M_k, v' \neq v} \mathfrak{o}_{v'}$ is open in A, and for any basic open set U of A (and thus for any open set of A), $U \cap k_v$ will be an open set of k_v.

It remains to show that k_v is closed in A. So take $a \in A - k_v$. Then there is some $v' \neq v$ with $a_{v'} \neq 0$. The open set

$$B\left(a_v, \frac{\| a_v \|_v}{2}\right) \times \prod_{v'' \in M_k - S_\infty, v'' \neq v'} \mathfrak{o}_{v''} \times \prod_{v'' \in S_\infty} k_{v''}$$

will then be an open neighborhood of a disjoint from k_v. Thus k_v is closed in A. □

Note that the embedding $k_v \hookrightarrow A$ induces an embedding $k \hookrightarrow A$, inducing the v-adic topology on k. Thus, in A we have copies of k with each of our topologies from M_k, together with a copy of k with the discrete topology.

Of course, A is not an integral domain. The units A^* are the elements $a = (a_v)$ with $a_v \in k_v^*$ for all $v \in M_k$, and with $a_v \in \mathfrak{o}_v^*$ for all but finitely many $v \in M_k$. (If there are infinitely many $a_v \notin \mathfrak{o}_v^*$, then the inverse $a^{-1} = (a_v^{-1})$ is not an adele.) Such an element is called an *idele*. Unfortunately, the ideles are not a topological

(multiplicative) subgroup of A, since inversion is not continuous. We will leave the demonstration of this to the reader.

Since k is an additive subgroup of A, it makes sense to consider the quotient A/k as a topological group in the quotient topology. We will show that A/k is compact. We will first need a lemma.

Lemma 5.4.

$$k + A_{S_\infty} = A,$$

in the sense that any adele can be written as a sum of an element of k and an element in the basic open set A_{S_∞}.

Proof. This means precisely that for any adele a, there is some $\alpha \in k$ such that $a - \alpha \in \mathfrak{o}_v$ for all non-archimedean $v \in M_k$, since A_{S_∞} is just the set

$$\prod_{v \in S_\infty} k_v \times \prod_{v \notin S_\infty} \mathfrak{o}_v.$$

We find such an α as follows: First, find an integer $c \in \mathbb{Z}$ such that $ca \in \mathfrak{o}_v$ for all $v \notin S_\infty$. We can do this since $a_v \in \mathfrak{o}_v$ for all but finitely many $v \notin S_\infty$, so we can just take some c highly divisible by the finitely many primes of $\mathbb{Z}$ lying under the $\mathfrak{p}$ with $a_v \notin \mathfrak{o}_{v_p}$.

Let S be the set of primes of $\mathfrak{o}_k$ dividing $c\mathfrak{o}_k$; this is finite, but may be larger than the set of primes with $a_{v_\mathfrak{p}} \notin \mathfrak{o}_{v_p}$, since more than one prime of $\mathfrak{o}_k$ can divide $p \in \mathbb{Z}$. Now, by the approximation theorem we can find $\alpha \in \mathfrak{o}_k$ with

$$\alpha \equiv ca_v \pmod{\mathfrak{p}^m}$$

for all $\mathfrak{p} \in S$ and some large m.

I claim that $a - \alpha/c$ satisfies the conditions of the lemma. First, if $\mathfrak{p} \notin S$, then c is in $\mathfrak{o}_v^*$, so $\alpha/c \in \mathfrak{o}_v$ and $a_v - \alpha/c$ will still be in $\mathfrak{o}_v$. If $\mathfrak{p} \in S$, then so long as we took m larger than the power of $\mathfrak{p}$ dividing c, $a_v - \alpha/c$ will still be in $\mathfrak{o}_v$. This completes the proof. □

Theorem 5.5. *The group A/k is compact.*

Proof. First, recall that we had an embedding

$$k \hookrightarrow \prod_{v \in S_\infty} k_v = \mathbb{R}^n.$$

Under this embedding the integers $\mathfrak{o}_k$ form a lattice. If $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{o}_k$, then the images of the α_i in $\mathbb{R}^n$ will still be linearly independent. (This is because the computation to check this is essentially just the computation of the discriminant, which is non-zero; for details, see [9, Chapter 8].) This shows that this lattice has rank n.

Let $P \in \mathbb{R}^n$ be a fundamental parallelotope for the lattice $\mathfrak{o}_k$. Then, since the lattice $\mathfrak{o}_k$ has the same rank as the dimension of the space $\mathbb{R}^n$, P is bounded, and therefore $\overline{P}$ is compact. Also, note that

$$A_{S_\infty} = \prod_{v \notin S_\infty} \mathfrak{o}_v \times \mathbb{R}^n.$$

Now, given any $a \in A$, we first take $\alpha \in k$ such that $a - \alpha \in A_{S_\infty}$. Next we take some $\beta \in \mathfrak{o}_k$ such that

$$a - \alpha - \beta \in \prod_{v \notin S_\infty} \mathfrak{o}_v \times \overline{P}.$$

We can do this since P is a fundamental domain for $\mathfrak{o}_k$. Call this set Q. It is a product of compact sets, and thus is compact. Therefore translation by the element $-(\alpha+\beta) \in k$ takes a into a compact set. Therefore $A/k = Q/(k \cap Q)$, which is a quotient of a compact space and thus is compact. □

6. Ideles

Recall that we defined the ideles to be the units A^* of the adele ring A. However, as we observed, inversion is not continuous on A^* with this topology. So A^* is not a topological group, at least when viewed as a subspace of A. To remedy this we will give A^* a different topology, which we can describe in two different ways.

The first is in analogy with the restricted direct product topology on A. We define the *ideles* J to be the subset of the direct product

$$\prod_{v \in M_k} k_v^*$$

consisting of those elements for which all but finitely many components lie in $\mathfrak{o}_v^*$. That is, $a = (a_v) \in J$ if and only if $a_v \in \mathfrak{o}_v^*$ for all but finitely many non-archimedean valuations v. (Again, we impose no restriction on the values a takes on at archimedean v.) Then, as sets, J is just the units A^* of A. However, we take for a basis of open sets of J the sets of the form

$$\prod_{v \in M_k} U_v$$

where $U_v \subseteq k_v^*$ is open in k_v^*, and $U_v = \mathfrak{o}_v^*$ for all but finitely many non-archimedean valuations v. (We give k_v^* the topology it inherits as a subspace of k_v.) As with the adeles, we can write such a set as

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathfrak{o}_v^* \tag{3}$$

where S is some finite subset of M_k containing S_∞, and U_v is open in k_v^* for each $v \in S$. As with the adeles, we can actually take our basis to consist of sets of the form (3) with each U_v a basic open set of k_v^*.

There is another way to define this topology. First, consider the product set $A \times A$, with the product topology. We then have a map

$$\varphi : J \to A \times A$$

given by $\varphi(a) = (a, a^{-1})$. We claim that this is a topological embedding. It is clear that φ is injective, so we must only show that it is bicontinuous.

First, note that if

$$U = \left(\prod_{v \in S} U_v \times \prod_{v \notin S} \mathfrak{o}_v, \prod_{v \in S} U_v' \times \prod_{v \notin S} \mathfrak{o}_v \right)$$

is a basic open set in $A \times A$ (we can take the same set S in each factor simply by taking some of the U_v and U_v' to be all of $\mathfrak{o}_v$), then

$$U \cap \varphi(J) = \left(\prod_{v \in S} \left(U_v \cap (U_v')^{-1} \right) \times \prod_{v \notin S} \mathfrak{o}_v^*, \prod_{v \in S} \left(U_v^{-1} \cap (U_v')^{-1} \right) \times \prod_{v \notin S} \mathfrak{o}_v^* \right).$$

This is the image of

$$\prod_{v\in S}\left(U_v\cap(U_v')^{-1}\right)\times\prod_{v\notin S}\mathfrak{o}_v^*,$$

which is open in J since inversion is continuous in each k_v^*. This implies immediately that φ is bicontinuous.

With both of these descriptions of the topology on J in hand, it is now easy to prove the basic facts about its topology. First, as with the adeles, we define sets

$$J_S=\prod_{v\in S}k_v^*\times\prod_{v\notin S}\mathfrak{o}_v^*$$

where S is some finite subset of M_k containing S_∞. Then J_S is open and locally compact, so J is locally compact. As in the adelic case, J_S is also closed, as is easy to see.

Proposition 6.1. *J is a topological group.*

Proof. Viewing J as embedded in $A\times A$, it is clear that inversion is continuous, since it is just the natural map reversing the order of the direct product. It is also clear that multiplication is continuous, since the map from $A\times A\times A\times A$ given by

$$(a_1,a_2,a_3,a_4)\mapsto(a_1a_3,a_2a_4)$$

is continuous, and this restricts to give precisely multiplication in J. □

We have natural embeddings $k^*\hookrightarrow k_v^*\hookrightarrow J$, along the v-component, and $k^*\hookrightarrow J$ along the diagonal. An element of k^* viewed as an idele in this second way is called a *principal idele*.

Proposition 6.2. *k^* is embedded along the diagonal in J as a discrete subgroup.*

Proof. This is essentially the same as the proof for the adeles, taking neighborhoods $B(1,1/2)$ for the archimedean valuations and using the product formula to derive a contradiction about $\alpha-1$ for $\alpha\in k$. □

Proposition 6.3. *k_v^* is embedded as a closed subgroup of J.*

Proof. This again is essentially the same as the adelic case. □

Summarizing, we have shown that the ideles J are a locally compact topological group, containing k^* as a discrete subgroup along the diagonal, and in the v-adic topology for each v inside of $k_v^*\hookrightarrow J$.

7. The Idele Class Group

The ideles possess two important natural homomorphisms into other multiplicative groups. The first is a map

$$\|\cdot\|:J\to\mathbb{R}^+$$

defined by

$$\|a\|=\prod_{v\in M_k}\|a_v\|_v^{n_v}\ .$$

This makes sense, since for any idele a all but finitely many of the terms in the product are 1. This map is also continuous; to show this, we must show that the preimage of an open interval $(b_0,b_1)\subseteq\mathbb{R}^+$ is open in J. So take any $a\in J$ with

$\| a \| \in (b_0, b_1)$. Pick one archimedean valuation v_0, let S be the set of valuations at which a is not in $\mathfrak{o}_v^*$, and consider the open sets

$$U_r = \prod_{v \in S, v \neq v_0} B(a_v, 1) \times \prod_{v \notin S} \mathfrak{o}_v^* \times B(a_{v_0}, r)$$

where we let r vary. Then these open sets contain a, and we can make r sufficiently small to force $\| U_r \|$ to lie in (b_0, b_1). This shows that $\| \cdot \|$ is continuous.

Since $\{1\}$ is closed in $\mathbb{R}^+$, the kernel of $\| \cdot \|$ (which is just the preimage of $\{1\}$) is closed in J. We denote this by J^0. Note that the product formula shows that $k^* \subseteq J^0$, and is a discrete subgroup.

The second natural homomorphism is given as follows: Let $\mathcal{I}$ be the multiplicative group of fractional ideals of k, and let $\mathcal{P}$ be the subgroup of principal ideals. We define a map

$$J \to \mathcal{I}$$

by associating to $a \in J$ the fractional ideal

$$\prod_{v_\mathfrak{p} \in M_k - S_\infty} \mathfrak{p}^{v_\mathfrak{p}(a_v)},$$

which we will denote (a). This is a fractional ideal, since only finitely many of the $v_\mathfrak{p}(a_v)$ are non-zero. This is clearly surjective, with kernel J_{S_∞}. Further, if $\alpha \in k^* \subseteq J$, then (α) is just the usual principal ideal generated by α. Thus $(k^*) \subseteq \mathcal{P}$, so that we obtain an induced surjective homomorphism from J/k^* to the ideal class group $\mathcal{I}/\mathcal{P}$. We call J/k^* the *idele class group*, and write it as C. It contains the closed subgroup $C^0 = J^0/k^*$.

Since the kernel of the map $J \to \mathcal{I}/\mathcal{P}$ is $k^* J_{S_\infty}$, we have an isomorphism

$$J/k^* J_{S_\infty} \cong \mathcal{I}/\mathcal{P}.$$

Thus we have expressed the ideal class group as a quotient of the ideles.

We can generalize this construction somewhat. For any finite subset S of M_k containing S_∞, we will call

$$k_S = J_S \cap k^*$$

the *S-units* of k. It is clear that this coincides with the usual notion of S-units, which are those elements of k^* which are units in each $\mathfrak{o}_v$ for $v \notin S$. k_{S_∞} is just the global units $\mathfrak{o}_k^*$. Since k^* is a discrete subgroup of J, k_S is a discrete subgroup of J_S. We call the quotient J_S/k_S the group of *S-idele classes*, and denote it by C_S. We set $J_S^0 = J_S \cap J^0$, and $C_S^0 = J_S^0/k_S$.

For each such S, we have a natural inclusion

$$C_S \hookrightarrow C$$

embedding C_S as an open and closed subgroup of C, since J_S is open and closed in J. Similarly, the natural inclusion

$$C_S^0 \hookrightarrow C^0$$

embeds C_S^0 as an open and closed subgroup of C^0.

We return to the ideal map defined above. We had a surjective map

$$C \to \mathcal{I}/\mathcal{P}$$

with kernel C_{S_∞}. Even if we restrict this map to C^0 it is still surjective, since if I is a fractional ideal and a an idele with $(a) = I$, we can modify a at one of the

archimedean valuations to get some $a' \in J^0$ with $(a') = I$. The kernel of this map is just $C^0_{S_\infty}$, so we have an isomorphism

$$C^0/C^0_{S_\infty} \cong \mathcal{I}/\mathcal{P}.$$

We must now show that C^0 is compact and discrete. This will turn out to be equivalent to the finiteness of the ideal class group of k and the Dirichlet unit theorem. We will first need a stronger approximation theorem, which we will prove in the next section.

8. Another Approximation Theorem

In order to prove the compactness of the idele class group we will need to exhibit elements of k satisfying conditions at all $v \in M_k$. The approximation theorem is not strong enough to deal with this situation, so we will need to prove a new result.

Given any idele a, we define the set $L(a) \subseteq k$ to be the set of all $\alpha \in k$ satisfying

$$\| \alpha \|_v \leq \| a_v \|_v$$

for all $v \in M_k$. We write $\lambda(a)$ for the order of $L(a)$. We wish to show if $\| a \|$ is sufficiently large, then $L(a)$ is non-zero.

First, note that for any $\alpha \in k^*$ $L(a)$ and $L(\alpha a)$ are in canonical bijection, by

$$x \mapsto \alpha x.$$

Thus, $\lambda(a) = \lambda(\alpha a)$.

Theorem 8.1. *Let k be a number field. Then there is a constant c_0, depending only on k, such that for any idele a,*

$$\lambda(a) \geq c_0 \| a \| .$$

Proof. Let n be the degree of k over $\mathbb{Q}$, and pick an integral basis $\omega_1, \ldots, \omega_n$ for $\mathfrak{o}_k$. Set

$$c_1 = n \sup_{v \in S_\infty, i} \{\| \omega_i \|_v\}.$$

Now, by the approximation theorem we can find $\alpha \in k^*$ satisfying

$$\frac{c_1}{\| a \|_v} \leq \alpha \leq \frac{2c_1}{\| a \|_v}$$

for all $v \in S_\infty$. We can also pick an integer $m \in \mathbb{Z}$ such that

$$\| m\alpha a \|_v \leq 1$$

for all $v \in M_k - S_\infty$, by taking m highly divisible by the prime numbers corresponding to the finitely many valuations v for which $\| \alpha a \|_v > 1$. Now, for all $v \in S_\infty$, we have

$$mc_1 \leq \| m\alpha a \|_v \leq 2mc_1.$$

Since $\lambda(m\alpha a) = \lambda(a)$ and $\| m\alpha a \| = \| a \|$, we may replace a by $m\alpha a$. This allows us to assume that

$$\| a \|_v \leq 1$$

for all $v \in M_k - S_\infty$, and that there is some rational integer m for which

$$mc_1 \leq \| a \|_v \leq 2mc_1$$

for all $v \in S_\infty$.

Now, let Λ be the set of elements of $\mathfrak{o}_k$ of the form

$$b_1\omega_1 + \cdots + b_n\omega_n$$

with $b_i \in \mathbb{Z}$ and $0 \leq b_i \leq m$. Then Λ contains $(m+1)^n > m^n$ elements. Now, by our normalization above, the fractional ideal (a) associated to the idele a is actually an ideal, so it makes sense to consider the quotient map

$$\mathfrak{o}_k \to \mathfrak{o}_k/(a).$$

The image has size $N(a)$, so there must be a subset $\Lambda' \subseteq \Lambda$ containing at least

$$\frac{m^n}{N(a)}$$

elements of Λ, all mapping to the same class in $\mathfrak{o}_k/(a)$.

Fix some $x \in \Lambda'$, and pick any other $y \in \Lambda'$. Then

$$x \equiv y \pmod{(a)},$$

so that

$$\| x - y \|_v \leq \| a_v \|_v$$

for all non-archimedean valuations v. If v is an archimedean valuation, then

$$\begin{aligned} \| x - y \|_v &= \| b_{x1}\omega_1 + \cdots + b_{xn}\omega_n - b_{y1}\omega_1 - \cdots - b_{yn}\omega_n \|_v \\ &= \| (b_{x1} - b_{y1})\omega_1 + \cdots + (b_{xn} - b_{yn})\omega_n \|_v \\ &\leq m \| \omega_1 \|_v + \cdots + m \| \omega_n \|_v \\ &\leq mc_1 \\ &\leq \| a_v \|_v . \end{aligned}$$

Thus $x - y \in L(a)$. Therefore,

$$\lambda(a) \geq \frac{m^n}{N(a)}.$$

However, we also have

$$m^n \geq 2^{-n} c_1^{-n} \prod_{v \in S_\infty} \| a_v \|_v^{n_v} .$$

Finally, since

$$\| a \| = \prod_{v \in M_k - S_\infty} \| a_v \|_v \cdot \prod_{v \in S_\infty} \| a_v \|_v^{n_v} = N(a)^{-1} \prod_{v \in S_\infty} \| a_v \|_v^{n_v},$$

we have

$$\lambda(a) \geq 2^{-n} c_1^{-n} \| a \| .$$

This proves the theorem, with $c_0 = 2^{-n} c_1^{-n}$. □

In fact, it is possible to get a much more precise statement. If we let r_1 be the number of real embeddings of k, r_2 the number of complex embeddings of k and D_k the absolute value of the discriminant of k, then

$$\lambda(a) \approx \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{D_k}} \| a \| .$$

See [3, Chapter 5, Section 2, Theorem 1].

9. The Compactness of the Idele Class Group

We are now in a position to prove the compactness of the idele class group. We will need a lemma. Throughout this section we let c_0 be the constant of Theorem 8.1.

Lemma 9.1. *Let a be an idele with $\| a \| \geq 2/c_0$. Then there exists $\alpha \in k^*$ such that*

$$1 \leq \| \alpha a_v \|_v \leq \| a \|$$

for all $v \in M_k$.

Proof. By Theorem 8.1 there is some non-zero β in $L(a)$. This β satisfies $\| \beta \|_v \leq \| a_v \|_v$ for all v, so if we set $\alpha = \beta^{-1}$, then

$$1 \leq \| \alpha a_v \|_v$$

for all $v \in M_k$. Also, we have

$$\| \alpha a_v \|_v = \frac{\prod_{v' \in M_k} \| \alpha a_v \|_v}{\prod_{v' \in M_k, v' \neq v} \| \alpha a_v \|_v} \leq \frac{\| a \|}{1} = \| a \|,$$

which completes the proof. □

Theorem 9.2. *C^0 is compact.*

Proof. Let $\psi : J \to \mathbb{R}^+$ be defined by $\psi(a) = \| a \|$. For any $\alpha \in k^*$ we have $\psi(\alpha) = 1$, so we get a well defined map

$$\psi : C \to R^+.$$

The kernel of this map is C^0. Now, note that for any $\rho \in \mathbb{R}^+$, $\psi^{-1}(\rho)$ is homeomorphic to C^0. To see this, let a_ρ be any idele with $\| a_\rho \| = \rho$. (We can always find such an a_ρ by adjusting the archimedean valuations.) Then we have $\psi^{-1}(\rho) = a_\rho C^0$, and this is a homeomorphism since J is a topological group. Thus, it will suffice to show that $\psi^{-1}(\rho)$ is compact for some $\rho \in \mathbb{R}^+$.

Fix some ρ with $\rho > 2/c_0$, and pick some $a \in \psi^{-1}(\rho)$. Then by Lemma 9.1 there is some $\alpha_a \in k^*$ with

$$1 \leq \| \alpha_a a_v \|_v \leq \rho$$

for all $v \in M_k$. However, since a non-archimedean valuation $v_\mathfrak{p}$ takes on no values between 1 and $N\mathfrak{p}$, and only finitely many primes $\mathfrak{p}$ have $N\mathfrak{p} \leq \rho$, we must have

$$\| \alpha_a a_v \|_{v_\mathfrak{p}} = 1$$

for all but finitely many primes $\mathfrak{p}$, independent of a. Thus there is some finite set S of valuations (including S_∞) such that

$$\begin{aligned} 1 \leq \| \alpha_a a_v \|_v &\leq \rho, \qquad v \in S \\ \| \alpha_a a_v \|_v &= 1, \qquad v \notin S. \end{aligned}$$

Define

$$T = \prod_{v \in S} \left(\overline{B(0,\rho)} - B(0,1) \right) \times \prod_{v \notin S} \mathfrak{o}_v^*.$$

Then by the Tychonoff theorem T is compact, since each factor is. Further, by what we have shown above, T maps onto $\psi^{-1}(\rho)$ under the quotient map

$$J \to C.$$

(This is because we can always modify an element of $\psi^{-1}(\rho)$ by an element of k^* to get it in T.) The image of T is compact, so $\psi^{-1}(\rho)$ is a closed subset of a compact space, and thus compact. This completes the proof. □

Corollary 9.3. *C_S^0 is compact for any finite set S containing S_∞.*

Proof. C_S^0 is a closed subset of the compact space C^0, and thus is compact. □

10. Applications to Algebraic Number Theory

The finiteness of the ideal class group is now an immediate corollary of everything we have done.

Theorem 10.1. *For any number field k, the ideal class group $\mathcal{I}/\mathcal{P}$ is finite.*

Proof. Recall that we had a group isomorphism

$$C^0/C^0_{S_\infty} \cong \mathcal{I}/\mathcal{P}.$$

The space $C^0/C^0_{S_\infty}$ is a quotient of a compact space, and thus compact. Also, $C^0_{S_\infty}$ is an open subgroup of C^0, so this quotient is also discrete. (This is because each coset of $C^0_{S_\infty}$, which become points in $C^0/C^0_{S_\infty}$, is open.) Thus, the space $C^0/C^0_{S_\infty}$ is compact and discrete, and thus finite. Therefore $\mathcal{I}/\mathcal{P}$ is finite as well. □

The Dirichlet unit theorem will require a preliminary result.

Lemma 10.2. *Any discrete subgroup Λ of $\mathbb{R}^s$ is free abelian, of rank $\dim \mathbb{R}\Lambda$. (Here $\mathbb{R}\Lambda$ is the $\mathbb{R}$-vector space spanned by Λ.)*

Proof. We prove this by induction on the dimension of $\dim \mathbb{R}\Lambda$. If $\dim \mathbb{R}\Lambda = 1$, then, since Λ is discrete, there must be some $\lambda \in \Lambda$ closest to 0. It is then clear that $\Lambda = \mathbb{Z}\lambda$, since otherwise we could construct an element of Λ closer to 0 than λ.

Now, suppose $\dim \Lambda = m$. Let $\lambda_1, \dots, \lambda_m$ be a $\mathbb{R}$-basis for $\mathbb{R}\Lambda$. If Λ_0 is the subgroup of Λ spanned by $\lambda_1, \dots, \lambda_{m-1}$, then by the induction hypothesis

$$\Lambda_0 = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_{m-1}.$$

Now, consider the set Λ' of $\lambda \in \Lambda$ of the form

$$\lambda = a_1\lambda_1 + \cdots + a_m\lambda_m,$$

with $0 \leq a_i < 1$ for $i = 1, \dots, m-1$, and $0 \leq a_m \leq 1$. (We do not require that the a_i be integers.) This is a bounded subset of a discrete set, so it is finite. Pick $\lambda' \in \Lambda'$ with minimal non-zero coefficient of λ_m, say

$$\lambda' = a_1'\lambda_1 + \cdots + a_m'\lambda_m.$$

Now, if λ is any element of Λ, then we can find some integer t such that the coefficient a_m of λ_m in $\lambda - t\lambda'$ satisfies $0 \leq a_m < a_m'$. We can then further modify $\lambda - t\lambda'$ by some $\lambda_0 \in \Lambda_0$ to get $\lambda - t\lambda' - \lambda_0 \in \Lambda'$. But since a_m' was the minimal non-zero coefficient of λ_m in Λ', we must have $a_m = 0$. This implies that

$$\lambda - t\lambda' - \lambda_0 = 0,$$

which, together with linear independence, shows that

$$\Lambda = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_m,$$

as desired. □

Theorem 10.3 (Dirichlet Unit Theorem)**.** *For any set finite set $S \in M_k$ of size s, containing S_∞, the S-units k_S have rank $s-1$.*

Proof. Let $v_1, \ldots, v_s$ be the elements of S, ordered so that v_s is archimedean. We define a group homomorphism

$$\log : J_S \to R^s$$

by

$$\log(a) = (\log \| a_{v_1} \|_{v_1}^{n_{v_1}}, \ldots, \log \| a_{v_s} \|_{v_s}^{n_{v_s}}).$$

This is continuous since it is continuous in each coordinate. Since any $a \in J_S^0$ has $\| a \| = 1$, and $\| a_v \|_v = 1$ for $v \notin S$, the image of J_S^0 under this mapping lies in the hyperplane

$$x_1 + \cdots + x_s = 0,$$

where $x_1, \ldots, x_s$ are the usual coordinates on $\mathbb{R}^s$. Call this hyperplane H. Note that J_S^0 generates H over $\mathbb{R}$, since $\log(J_S^0)$ contains the $s-1$ linearly independent vectors

$$\begin{gathered}(c_1, 0, 0, \ldots, 0, -c_1) \\ (0, c_2, 0, \ldots, 0, -c_2) \\ \vdots \\ (0, 0, 0, \ldots, c_{s-1}, -c_{s-1}),\end{gathered}$$

where the c_i are some non-zero constants depending on v_i.

Now, consider the S-units $k_S = k^* \cap J_S^0$. The set $\log(k_S)$ is in fact discrete. To see this, note that the elements of $\log(k_S)$ in any bounded region of $\mathbb{R}^s$ have bounded archimedean absolute values, which in turn bounds the coefficients of the polynomials of these elements over $\mathbb{Z}$. Since the degree is bounded by $[k : \mathbb{Q}]$, there are only finitely many such polynomials having bounded coefficients. Therefore only finitely many elements of k can map into any bounded region of $\mathbb{R}^s$, so $\log(k_S)$ is discrete. Thus, by Lemma 10.2, $\log(k_S)$ is a free abelian group. Note that the kernel of $\log|_{k_S}$ is just the roots of unity of k (since any algebraic integer which always has archimedean absolute value 1 is a root of unity, by an argument similar to the one just given), so it will be enough to show that $\log(k_S)$ has rank $s-1$.

Let W be the subspace of H generated by $\log(k_S)$. Then we have an induced continuous homomorphism

$$\log : J_S^0/k_S = C_S^0 \to H/W.$$

The image of this map generates H/W as an $\mathbb{R}$-vector space, since J_S^0 generates H. The image is also the image of the compact set C_S^0, and thus compact. But if H/W is non-trivial it has no non-trivial compact subgroups (it is just $\mathbb{R}^n$ for some n), so we must have $H/W = 0$, and $H = W$. Thus $\log(k_S)$ generates all of H, so it has rank $s-1$. □

Corollary 10.4. *The group of global units of a number field k is isomorphic to*

$$W \times \mathbb{Z}^{r_1 + r_2 - 1},$$

where W is the subgroup of roots of unity, r_1 is the number of real embeddings of k and r_2 is the number of complex embeddings of k.

Proof. We simply take $S = S_\infty$ in the preceding theorem. □

References

[1] J.W.S. Cassels and A. Fröhlich, ed., *Algebraic Number Theory*. Academic Press, London, 1967.
[2] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer-Verlag, New York, 1984.
[3] Serge Lang, *Algebraic Number Theory*. Springer-Verlag, New York, 1994.
[4] Daniel Marcus, *Number Fields*. Springer-Verlag, New York, 1977.
[5] Hideyuki Matsumura, *Commutative Ring Theory*. Cambridge Unversity Press, Cambridge, Great Britain, 1986.
[6] James R. Munkres, *Topology : A First Course*. Prentice Hall, Englewood Cliffs, New Jersey, 1975.
[7] Jean-Pierre Serre, *A Course in Arithmetic*. Springer-Verlag, New York, 1973.
[8] Jnean-Pierre Serre, *Local Fields*. Springer-Verlag, New York, 1979.
[9] Ian Stewart and David Tall, *Algebraic Number Theory*. Chapman and Hall, London, 1987.