AN INTRODUCTION TO THE THEORY OF VALUED FIELDS

ASHVIN A. SWAMINATHAN

Abstract. In this article, we discuss the theory of valued fields, a subject that is fundamental to many subdisciplines of modern mathematics, most notably class field theory. We begin by introducing the basic definitions and properties of absolute values and their associated algebraic objects. Then, after discussing completions of valued fields and normed vector spaces, we apply the theory of absolute values to study finite extensions of number fields. We conclude our discussion with a proof of Dirichlet's Unit Theorem using the language of adeles and ideles. Throughout the paper, we strive to provide a sense of concreteness by including numerous motivating examples, many of which relate to the field of p-adic numbers.

Contents

1. Motivations and Definitions . . . 2
1.1. A Historical Perspective . . . 2
1.2. Absolute Values . . . 3
1.3. Topology . . . 6
2. Types of Absolute Values . . . 8
2.1. Non-archimedean Absolute Values . . . 8
2.2. Discrete Absolute Values . . . 11
3. Completions and Finite Extensions . . . 13
3.1. Completions . . . 14
3.2. Finite Extensions . . . 18
4. Number Fields . . . 23
4.1. An Archimedean Aside . . . 24
4.2. The Non-archimedean Case . . . 27
5. A Glimpse of Class Field Theory . . . 29
5.1. Restricted Topological Products . . . 29
5.2. Adeles and Ideles . . . 32
5.3. Dirichlet's Unit Theorem . . . 38
6. Appendix: Auxiliary Theorems . . . 41
Acknowledgements . . . 43
References . . . 43

This Junior Paper was composed in partial fulfillment of the requirements for the degree of *Artium Baccalaureus* in Mathematics at Harvard College. The author hereby affirms his awareness of the standards of the Harvard College Honor Code.

1. Motivations and Definitions

1.1. **A Historical Perspective.** The theory of absolute values on fields was originally developed as a means of generalizing the work of German mathematician Kurt Hensel on p-adic numbers. Hensel was interested in comparing the ring $\mathbb{Z}$ of rational integers and the ring $\mathbb{C}[x]$ of polynomials in one variable over $\mathbb{C}$. Specifically, he observed that there is an analogy between prime ideals of $\mathbb{Z}$, which are precisely those ideals of the form (p) where p is a prime number, and prime ideals of $\mathbb{C}[x]$, which are precisely those ideals of the form $(x - \alpha)$ where $\alpha \in \mathbb{C}$. For example, one important similarity between the rings $\mathbb{Z}$ and $\mathbb{C}[x]$ is that they are both unique factorization domains; i.e. given an element of either ring, one can uniquely express it as a product of primes (up to multiplication by unit). Moreover, each positive integer has a unique base-p expression for every prime number p, just like every $f \in \mathbb{C}[x]$ can be uniquely expressed as a polynomial in $x - \alpha$ for every $\alpha \in \mathbb{C}$. In light of these similarities, Hensel took this analogy one step further by asking the following question: since for every rational function $f \in \mathbb{C}(x)$ and $\alpha \in \mathbb{C}$ we can expand f in terms of $x - \alpha$ by means of its Laurent series

$$f(x) = \sum_{n \geq N} a_n (x - \alpha)^n,$$

where $N \in \mathbb{Z}$ is the order of f at α, does a similar expansion exist for a rational number in terms of a given prime p?

In his 1904 paper entitled "Neue Grundlagen der Arithmetik," Hensel answered this question in the affirmative. Indeed, given a prime p, we can formally write every rational number $q \in \mathbb{Q}$ as a finite-tailed "Laurent series" in p with coefficients in $\{0, \dots, p-1\}$ as follows. If $q = 0$, there is nothing to do, so suppose $q > 0$. Write $q = p^k \cdot \frac{a}{b}$, where the fraction $\frac{a}{b}$ is in lowest terms and each of a and b is coprime to p. Then, to find the Laurent series expansion of q, we need only find the p-adic expansion of $\frac{a}{b}$ and multiply the result by p^k. The first digit r_1 of the Laurent series expansion of $\frac{a}{b}$ is obtained by long division: we find the unique number $r_1 \in \{0, \dots, p-1\}$ such that $\frac{a}{b} - r_1$, when written as a fraction in lowest terms, has numerator divisible by p. The remaining digits of the Laurent series expansion of $\frac{a}{b}$ are given by the Laurent series expansion of $\frac{1}{p} \cdot \left(\frac{a}{b} - r_1\right)$. (Notice that this algorithm simply returns the base-p expansion of q when $q \in \mathbb{Z}_{\geq 0}$.) Now, observe that we can write the number -1 as the formal power series

$$-1 = (p-1) + (p-1) \cdot p + (p-1) \cdot p^2 + \cdots = \sum_{n \geq 0} (p-1) p^n, \tag{1}$$

so if $q < 0$, then we obtain an expansion of q as a Laurent series in p by multiplying the series expansion of the positive rational number $-q$ with the series expansion of -1 given by (1). This formal expression of $q \in \mathbb{Q}$ as a

Laurent series in p with coefficients in $\{0, \ldots, p-1\}$ is known as the p-adic expansion of the number q.

Given that the p-adic expansion, as formulated above, is purely formal, one can ask whether an arbitrary formal Laurent series

$$\sum_{n \geq N} a_n p^n \tag{2}$$

satisfying $a_n \in \{0, \ldots, p-1\}$ for all n represents a rational number. The answer to the corresponding question for the field $\mathbb{C}(x)$ is "no," as can be seen by noting that the power series

$$\sum_{n \geq 0} \frac{(-1)^{2n+1}}{(2n+1)!}$$

is a finite-tailed Laurent series in $x - 0$ but corresponds to the function $\sin x$, which is not manifestly not rational: the zero locus of $\sin x$ is an infinite discrete subset of $\mathbb{C}$. One surmises that that an analogous result holds for p-adic expansions, and this is indeed the case: if $p > 2$, then by taking a_n to be such that $\sum_{i=0}^{n} a_i p^i$ is a root of the equation $x^2 \equiv 2 \pmod{p^n}$ for all $n \geq 0$, the power series (2) can be thought of as a root of the polynomial $x^2 - 2$, and the rational numbers certainly do not contain a square root of 2 (when $p = 2$, a similar trick works if we replace the polynomial $x^2 - 2$ with $x^2 - x + 1$). Furthermore, we observe (without proof) that one can formally add, multiply, and divide finite-tailed Laurent series, so the set of p-adic series of the form (2) forms a field that is a proper extension of the field $\mathbb{Q}$ of rational numbers. We shall denote this field by $\mathbb{Q}_p$, the field of p-adic numbers.

Our construction of the field $\mathbb{Q}_p$, however explicit, is somewhat *ad hoc* and perhaps unsatisfying. Thus far, all we know about $\mathbb{Q}_p$ is that its elements are formal Laurent series, most of which do not appear to converge in the conventional sense (whereas the convergence of Laurent series expansions of complex functions is well-understood). The reason why we omitted the proofs of basic facts about $\mathbb{Q}_p$ in the previous paragraph, such as the well-definedness of the field operations, is that they are quite frankly tedious. For example, if we are to multiply two p-adic numbers, we must not only multiply out all of the terms, but also adjust the coefficients of the resulting series to ensure that they lie in $\{0, \ldots, p-1\}$. It is with the view of developing a more natural and systematic construction of the fields $\mathbb{Q}_p$ of p-adic numbers that mathematicians introduced the theory of valuations.

1.2. **Absolute Values.** In order to achieve a suitable notion of convergence for a p-adic expansion, we must find some way to quantify the "size" of the terms in such an expansion. On the field $\mathbb{Q}$ of rational numbers, we are already familiar with one way of measuring the size of a number, namely by taking the standard absolute value, which (for reasons that will be revealed later) we shall denote by $| - |_\infty$. The standard absolute value, as one readily recalls, is defined by

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

and satisfies three important properties: positive-definiteness ($|x|_\infty \geq 0$, with equality precisely when $x = 0$), multiplicativity ($|xy|_\infty = |x|_\infty \cdot |y|_\infty$), and the triangle inequality ($|x + y|_\infty \leq |x|_\infty + |y|_\infty$). This notion of absolute value can be generalized to an arbitrary field as follows:

Definition 1. An absolute value on a field k is a function $| - |_v : k \to \mathbb{R}_{\geq 0}$ that satisfies the following three properties:

(1) Positive-definiteness: $|x|_v = 0$ if and only if $x = 0$.
(2) Multiplicativity: $|xy|_v = |x|_v \cdot |y|_v$.
(3) "Modified" Triangle Inequality: There exists a constant $C \in \mathbb{R}_{\geq 1}$ such that $|1 + x|_v \leq C$ if $|x|_v \leq 1$. (In this case, observe that $|x + y|_v \leq C \cdot \max\{|x|_v, |y|_v\}$ for all $x, y \in k$.)

The field k, together with the absolute value $| - |_v$, is known as a valued field.

Remark. Suppose $|-|_v$ is an absolute value on a field k, and let S be the set of all $C \in \mathbb{R}_{\geq 1}$ such that $| - |_v$ satisfies the modified triangle inequality with the constant C. Then clearly $|-|_v$ satisfies the modified triangle inequality with $\inf S \in \mathbb{R}_{\geq 1}$; we call this minimal constant the Artin constant associated to $| - |_v$.

The first two of the above properties are exactly the same as the corresponding properties of the standard absolute value $|-|_\infty$, but the third is visibly different. The reason for requiring a "modified" triangle inequality is to ensure that any positive power of an absolute value is still an absolute value. For instance, the absolute value $| - |_\infty^2$ (defined by $|x|_\infty^2 = |x|_\infty \cdot |x|_\infty$), fails to satisfy the triangle inequality, but it does satisfy the modified triangle inequality with $C = 4$. More generally, we have that for any absolute value $|-|_v$ with Artin constant $C \in \mathbb{R}_{\geq 1}$, the function $| - |_v^m : k \to \mathbb{R}_{\geq 0}$ defined in the obvious way is also an absolute value when $m > 0$, with Artin constant $C^m \in \mathbb{R}_{\geq 1}$.

A number of properties of absolute values can be deduced rather quickly from Definition 1. Indeed, if k is a field equipped with an absolute value $| - |_v$, then one readily checks that the following facts hold:

Lemma 2. *We have $|1|_v = 1$ and $\left|\frac{1}{x}\right|_v = \frac{1}{|x|_v}$ for $x \in k^\times$. Since 1 is the only root of unity in $\mathbb{R}_{\geq 0}$, we have $|x|_v = 1$ for all $x \in k$ such that $x^n = 1$ for some $n \in \mathbb{Z}$. It follows that $| - x|_v = |x|_v$ for all $x \in k$.*

Since Definition 1 gives a notion of absolute value that works over any field, one might ask whether every field has an absolute value in the first place. But this is clear: any field k is equipped with the trivial absolute value, whose value at 0 is 0 and whose value at $x \in k^\times$ is 1. In the case where k is a finite field, every $x \in k^\times$ is a root of unity, so Lemma 2 implies that

Corollary 3. *The only absolute value on a finite field is the trivial one.*

Many properties of absolute values that will be of interest to us will hold for the absolute value $|-|_v^m$, where $m > 0$, if they hold for the absolute value $|-|_v$. Thus, it makes sense to declare two absolute values $|-|_v$ and $|-|_{v'}$ equivalent if there exists $m \in \mathbb{R}_{>0}$ such that $|-|_{v'} = |-|_v^m$. One readily checks that this gives an equivalence relation on the set of absolute values; an equivalence class of absolute values is known as a place. It is natural to wonder whether every place contains an absolute value that satisfies the ordinary triangle inequality. Fortunately, this is indeed the case:

Lemma 4. *If $|-|_v$ is an absolute value on a field k, then there exists an equivalent absolute value $|-|_{v'}$ on k that satisfies the ordinary triangle inequality.*

Proof. Suppose $|-|_v$ has Artin constant $C \in \mathbb{R}_{\geq 1}$. Let $|-|_{v'} = |-|_v^m$, where $m = \log_2 C$. Then $|-|_{v'}$ is equivalent to $|-|_v$, and we claim that $|-|_{v'}$ satisfies the triangle inequality. By construction, $|-|_{v'}$ has Artin constant 2, so $|x+y|_{v'} \leq 2 \cdot \max\{|x|_{v'}, |y|_{v'}\}$ for all $x, y \in k$. It follows by induction that

$$\left|\sum_{i=1}^{2^r} x_i\right|_{v'} \leq 2^r \cdot \max\{|x_i|_{v'} : 1 \leq i \leq 2^r\}. \tag{3}$$

Now, notice that for any $n \in \mathbb{Z}_{\geq 0}$ we have

$$|x+y|_{v'}^n = |(x+y)^n|_{v'} = \left|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\right|_{v'} \leq 2(n+1) \sum_{i=0}^{n} \left|\binom{n}{i}\right|_{v'} \cdot |x^i|_{v'} \cdot |y^{n-i}|_{v'},$$

where the final inequality above is obtained by performing the following trick: let 2^r be the smallest power of 2 greater than $n+1$, add $2^r - (n+1)$ zero terms to the sum, applying the bound (3), and use the fact that $2^r \leq 2(n+1)$. This same trick tells us that $\left|\binom{n}{i}\right|_{v'} \leq 2\binom{n}{i}$, so we deduce that

$$|x+y|_{v'}^n \leq 4(n+1) \sum_{i=0}^{n} \binom{n}{i} \cdot |x^i|_{v'} \cdot |y^{n-i}|_{v'} = 4(n+1) \cdot (|x|_{v'} + |y|_{v'})^n.$$

Taking n^{th} roots on both sides, sending $n \to \infty$, and using the well-known fact that $\lim_{n\to\infty} \sqrt[n]{n} = 1$, we find that $|x+y|_{v'} \leq |x|_{v'} + |y|_{v'}$. Thus, the absolute value $|-|_{v'}$ satisfies the triangle inequality, as desired. ♠

Remark. The main tactic employed in the proof of Lemma 4 (namely, estimating n^{th} powers, taking n^{th} roots, and sending $n \to \infty$) is a fairly common one in the theory of valuations, and we will certainly encounter it in the future. We have now shown that every place contains an absolute value that satisfies the triangle inequality, so for the most part, it will suffice to restrict our attention to such absolute values.

Thus far, we have only discussed two examples of absolute values, namely the standard and trivial ones, so to conclude this subsection, let us consider a more interesting example, that of the p-adic norm:

Example 5. One of our objectives in generalizing absolute values was to develop a notion of "size" for rational numbers, with respect to which p-adic expansions would converge. We would like the p-adic "size" of a rational number q to somehow reflect the number of factors of p that are present in the numerator or denominator when q is expressed in lowest terms. In this light, we make the following definition:

Definition 6. The p-adic norm is the function $|-|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ that sends $0 \mapsto 0$ and assigns to $q \in \mathbb{Q}^\times$ the value p^{-a}, where a is the unique integer such that $q = p^a \cdot \frac{r}{s}$, with $r, s \in \mathbb{Z}$ both coprime to p.

One readily checks that the p-adic norm is indeed an absolute value with Artin constant $C = 1$. It may seem strange that we defined the p-adic norm in such a way that it grows inversely to the number of factors of p in the numerator. However, recall that we want p-adic expansions to converge with respect to the p-adic norm. For this to happen, the size of a number containing a large positive power of p in its factorization needs must be small. Thus, Definition 6 is in fact quite natural. ♣

1.3. **Topology.** Recall that the standard absolute value on $\mathbb{Q}$ induces a metric $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_{\geq 0}$, defined by $d(a, b) = |a - b|_\infty$. Then, using this metric, we can define a topology (known as the metric topology) on $\mathbb{Q}$ by designating the balls $B(a, r) = \{b \in \mathbb{Q} : d(a, b) < r\}$ for $a \in \mathbb{Q}$ and $r > 0$ to be open. One might ask whether it is possible to use our general theory of absolute values to define metrics and topologies on arbitrary fields. To this end, let $|-|_v$ be an absolute value on a field k. It follows from Definition 1 and Lemma 2 that if $|-|_v$ satisfies the ordinary triangle inequality, then the function $d : k \times k \to \mathbb{R}_{\geq 0}$ defined by $d(a, b) = |a - b|_v$ is a well-defined metric on k (indeed, it satisfies positive-definiteness, symmetry, and the triangle inequality).

The only issue with the above construction is that it requires $|-|_v$ to satisfy the triangle inequality, which not all absolute values do. Observe, however, that even if $|-|_v$ does not satisfy the triangle inequality, we can still use $|-|_v$ to directly define a topology on k. Indeed, we make the following definition:

Definition 7. The topology induced by an absolute value $|-|_v$ on a field k is generated by the basis of open balls $B_v(a, d) = \{b \in k : |b - a|_v < d\}$ for $a \in k$ and $d \in \mathbb{R}_{>0}$.

We asserted in the previous subsection that equivalent absolute values have similar properties, so one might hope that the topological structure given by Definition 7 is invariant under equivalence. In the next lemma, we prove an even stronger version of this statement:

Lemma 8. *Two absolute values $|-|_v$ and $|-|_{v'}$ on a field k are equivalent if and only if they induce the same topology on k.*

Proof. First suppose $|-|_v$ and $|-|_{v'}$ are equivalent; then, there exists $m \in \mathbb{R}_{>0}$ such that $|-|_{v'} = |-|_v^m$. Take $a \in k$ and $d \in \mathbb{R}_{>0}$, and notice that

$$x \in B_v(a,d) \Leftrightarrow \frac{|x-a|_v}{d} < 1 \Leftrightarrow \frac{|x-a|_{v'}}{d^m} < 1 \Leftrightarrow x \in B_{v'}(a, d^m).$$

It follows that every open ball in the topology induced by $|-|_v$ is an open ball in the topology induced by $|-|_{v'}$, and vice versa. Thus, $|-|_v$ and $|-|_{v'}$ induce the same topologies on k.

Now suppose $|-|_v$ and $|-|_{v'}$ induce the same topology on k. Observe that for $x \in k$, we have $|x|_v < 1$ if and only if the sequence $\{x^n\}_{n \in \mathbb{Z}_{>0}}$ converges to 0, which happens if and only if $|x|_{v'} < 1$. Taking reciprocals yields that $|x|_v > 1$ if and only if $|x|_{v'} > 1$, from which we deduce that $|x|_v = 1$ if and only if $|x|_{v'} = 1$. Now let $y, z \in k^\times$ and $m, n \in \mathbb{Z}$; we have just shown that $|y^m z^n|_v \lesseqgtr 1$ if and only if $|y^m z^n|_{v'} \lesseqgtr 1$. Taking logarithms and rearranging, we have

$$n \cdot \frac{\log|z|_v}{\log|y|_v} \lesseqgtr -m \Leftrightarrow n \cdot \frac{\log|z|_{v'}}{\log|y|_{v'}} \lesseqgtr -m.$$

Since the above holds for all $m, n \in \mathbb{Z}$, it follows that $\frac{\log|y|_{v'}}{\log|y|_v} = \frac{\log|z|_{v'}}{\log|z|_v}$ for all $y, z \in k^\times$, from which we conclude that $|-|_v$ and $|-|_{v'}$ are equivalent. ♠

Observe that Lemmas 4 and 8 together tell us that we can always replace an absolute value with one that satisfies the triangle inequality, and hence gives rise to a metric, without altering the topological structure of our field. The topology induced by an absolute value also plays well with the field operations, in the following sense:

Lemma 9. *Let $|-|_v$ be an absolute value on a field k. Then k is a topological field in the topology induced by $|-|_v$; i.e. the operations of addition, multiplication, and inversion are continuous.*

Proof. We may assume that $|-|_v$ satisfies the triangle inequality. Then for $x, y, \varepsilon_1, \varepsilon_2 \in k$, we have that $|x + \varepsilon_1 + y + \varepsilon_2|_v \leq |x+y|_v + |\varepsilon_1|_v + |\varepsilon_2|_v$ and that $|x+y|_v \leq |x + \varepsilon_1 + y + \varepsilon_2|_v + |\varepsilon_1|_v + |\varepsilon_2|_v$. Thus, by taking $\varepsilon_1, \varepsilon_2$ so that $|\varepsilon_1|_v + |\varepsilon_2|_v$ is sufficiently small, we can make $|x + \varepsilon_1 + y + \varepsilon_2|_v$ arbitrarily close to $|x+y|_v$, implying that addition is continuous. The proofs for multiplication and inversion are similar, so we omit them. ♠

2. Types of Absolute Values

In this section, we give definitions for and prove basic properties of two important properties that an absolute value can have, namely non-archimedean-ness and discreteness. Absolute values satisfying one or both of these properties are fundamental to the theory of valued fields.

2.1. Non-archimedean Absolute Values.

To begin with, recall from Example 5, where we discussed the p-adic norm, that there are absolute values (in addition to the trivial one) with Artin constant $C = 1$. Such absolute values are given a special name:

Definition 10. An absolute value $|-|_v$ on a field k is said to be non-archimedean if it has Artin constant $C = 1$ (in this case, the modified triangle inequality is known as the ultra-metric inequality). Otherwise, it is said to be archimedean.

In general, it may not be easy to check whether an absolute value is non-archimedean directly from Definition 10. The following result provides a somewhat simpler test for this property:

Lemma 11. *An absolute value $| - |_v$ on a field k is non-archimedean if and only if $|n|_v \leq 1$ for all $n = \sum_{i=1}^{n} 1 \in k$.*

Proof. The forward direction is an obvious consequence of the ultra-metric inequality. For the reverse direction, we apply the tactic used in the proof of Lemma 4. Take $x \in k$ with $|x|_v \leq 1$. Then for any $n \in \mathbb{Z}_{n\geq 0}$, we have

$$|1 + x|_v^n \leq \sum_{i=0}^{n} \left| \binom{n}{i} \right|_v \cdot |x|^i \leq n + 1.$$

Taking n^{th} roots and sending $n \to \infty$ yields that $|1 + x|_v \leq 1$, so $| - |_v$ satisfies the ultra-metric inequality and is therefore non-archimedean. ♠

Remark. The result of Lemma 11 gives justification to the terminology "non-archimedean." Recall that the archimedean property on $\mathbb{Q}$ states that for every $x, y \in \mathbb{Q}$ with $x > 0$, then there exists $n \in \mathbb{Z}_{>0}$ such that $nx > y$. We can rewrite this inequality in terms of absolute values as $|nx|_\infty > |y|_\infty$, and taking $x = y = 1$, we see that $|n|_\infty > 1$ for some positive integer n. This is, as we might hope, exactly the opposite of the non-archimedean condition given by Lemma 11.

Corollary 12. *If k is a field of finite characteristic p, then every absolute value on k is non-archimedean.*

Proof. Let $| - |_v$ be an absolute value on k. The additive subgroup $A \subset k$ generated by 1 is a copy of the finite field $\mathbb{F}_p$ of order p, so by Corollary 3, $|x|_v = 1$ for all nonzero $x \in A$. That $| - |_v$ is non-archimedean follows immediately from Lemma 11. ♠

Because of the ultra-metric inequality, the geometry of a field equipped with a non-archimedean absolute value is really quite strange, as is evidenced by the following two lemmas:

Lemma 13. *Let $|-|_v$ be a non-archimedean absolute value on a field k. If $|x|_v < |y|_v$, then $|x+y|_v = |y|_v$. In particular, every triangle in k is isosceles with respect to the metric given by $|-|_v$.*

Proof. The ultra-metric inequality tells us that $|x+y|_v \leq |y|_v$ and that

$$|y|_v = |(x+y)-x|_v \leq \max\{|x+y|_v, |x|_v\}.$$

Since $|y|_v \not\leq |x|_v$, we have $|y|_v \leq |x+y|_v \leq |y|_v$, which implies the first statement in the lemma. For the second statement, let $x, y, z \in k$. Then $x - z = (x-y) + (y-z)$, so by the first statement, we have that $|x-z|_v = \max\{|x-y|_v, |y-z|_v\}$. It follows that the triangle with vertices x, y, z is isosceles. ♠

Example 14. We return to the case of the p-adic norm $|-|_p$ from Example 5. We already know that $|-|_p$ satisfies the ultra-metric inequality, so it gives a non-archimedean absolute value on $\mathbb{Q}$. Suppose $x, y \in \mathbb{Z}$, and express them as $x = p^m r$ and $y = p^n s$, where $r, s \in \mathbb{Z}$ are both coprime to p. We may assume without loss of generality that $m \leq n$, in which case the largest factor of p dividing $x+y$ is p^m, so $|x+y|_v = |x|_v$, as we know should be true from Lemma 13. ♣

Lemma 15. *Let $|-|_v$ be a non-archimedean absolute value on a field k. For any $x, y \in k$ and $r \in \mathbb{R}_{>0}$ such that $|x-y|_v \geq r$, we have $B_v(x,r) \cap B_v(y,r) = \varnothing$. In particular, every open ball in k is closed.*

Proof. By the ultra-metric inequality, for any $z \in B_v(x,r) \cap B_v(y,r)$, we have

$$r \leq |x-y|_v = |(x-z)+(z-y)|_v \leq \max\{|x-z|_v, |z-y|_v\} < r,$$

which is a contradiction (the second-to-last inequality is in fact an equality by Lemma 13, but we do not need this fact for the present proof). Thus, $B_v(x,r) \cap B_v(y,r) = \varnothing$ for all $x, y \in k$, which is the first statement in the lemma. For the second statement, take $x \in k$, $r \in \mathbb{R}_{>0}$, and $y \in k \setminus B_v(x,r)$. Observe that $|x-y|_v \geq r$, so by the first statement, we have that $B_v(x,r) \cap B_v(y,r) = \varnothing$. We have thus exhibited an open neighborhood of y disjoint from $B_v(x,r)$, which implies that $k \setminus B_v(x,r)$ is open, so $B_v(x,r)$ is closed. ♠

The next proposition, which follows from Lemma 15, states that the topology induced on a field by a non-archimedean absolute value is about as ill-behaved as it could possibly be:

Proposition 16. *Let $|-|_v$ be a non-archimedean absolute value on a field k. Then k is totally disconnected with respect to the topology induced by $|-|_v$.*

Proof. Suppose $U \subset k$ is a subset containing at least two distinct elements, call them x, y. Take $r \in (0, |x-y|_v]$, and consider the sets $A = B(x,r) \cap U$ and $C = U \setminus B(x,r)$. Clearly, we have that $A \cap C = \varnothing$ and $A \cup C = U$. Moreover, because A is closed in U by Lemma 15, we have that C is open in U. But since A is also open in U, we have that $U = A \sqcup C$ constitutes a separation of U into two disjoint open subsets. Because our choice of U was arbitrary, we have that k is totally disconnected, as desired. $\spadesuit$

Now that we have dwelled for long enough about the strange geometric properties of a field equipped with a non-archimedean absolute value, we shall proceed to discuss some of the truly amazing properties that such fields have.

We begin by observing that if $|-|_v$ is a non-archimedean absolute value on a field k, then the closed ball $\mathcal{O}_v = \{x \in k : |x|_v \leq 1\}$ is in fact a subring of k, called the valuation ring associated to $|-|_v$. Indeed, notice that $1 \in \mathcal{O}_v$ because $|1|_v = 1$; moreover, if $x, y \in \mathcal{O}_v$, then $|x+y|_v \leq \max\{|x|_v, |y|_v\} \leq 1$, so $x + y \in \mathcal{O}_v$, and $|xy|_v = |x|_v \cdot |y|_v \leq 1$, so $xy \in \mathcal{O}_v$. By the same argument, one checks that the subset $\mathfrak{p}_v = \{x \in k : |x| < 1\} \subset \mathcal{O}_v$ is an ideal, called the valuation ideal associated to $|-|_v$. The ideal $\mathfrak{p}_v$ is maximal because every element in $\mathcal{O}_v \setminus \mathfrak{p}_v$ has absolute value 1 and is therefore a unit (note that the units in $\mathcal{O}_v$ are precisely those elements $x \in \mathcal{O}_v$ with $|x|_v = 1$; the set of all units in $\mathcal{O}_v$ is denoted by $\mathcal{O}_v^\times$). Since every proper ideal of $\mathcal{O}_v$ is contained in $\mathfrak{p}_v$, we have that $\mathcal{O}_v$ is a local ring with unique maximal ideal $\mathfrak{p}_v$, and the quotient ring $\kappa_v = \mathcal{O}_v/\mathfrak{p}_v$ is a field, called the residue field associated to $|-|_v$. Just as with the topology induced by an absolute value, the valuation ring, valuation ideal, and residue field are invariant under equivalence:

Lemma 17. *Let $|-|_v$ and $|-|_{v'}$ be non-archimedean absolute values on a field k. If $|-|_v$ and $|-|_{v'}$ are equivalent, then $\mathcal{O}_v = \mathcal{O}_{v'}$, $\mathfrak{p}_v = \mathfrak{p}_{v'}$, and $\kappa_v = \kappa_{v'}$. On the other hand, if $\mathcal{O}_v = \mathcal{O}_{v'}$, then $|-|_v$ and $|-|_{v'}$ are equivalent.*

Proof. For the forward direction, recall from the proof of Lemma 8 that $|x|_v \overset{<}{\underset{>}{=}} 1$ if and only if $|x|_v' \overset{<}{\underset{>}{=}} 1$ for all $x \in k$. It immediately follows that $\mathcal{O}_v = \mathcal{O}_{v'}$ and $\mathfrak{p}_v = \mathfrak{p}_{v'}$, so $\kappa_v = \kappa_{v'}$ as well. For the reverse direction, suppose $\mathcal{O}_v = \mathcal{O}_{v'}$. Notice that $\mathfrak{p}_v = \mathfrak{p}_{v'}$, because $\mathcal{O}_v \setminus \mathfrak{p}_v = \mathcal{O}_{v'} \setminus \mathfrak{p}_{v'}$: the property of having absolute value 1 is equivalent to being a unit in the ring $\mathcal{O}_v = \mathcal{O}_{v'}$. It follows that $|x|_v \overset{<}{\underset{>}{=}} 1$ if and only if $|x|_v' \overset{<}{\underset{>}{=}} 1$ for all $x \in k$. The remainder of the proof is identical to that of Lemma 8. $\spadesuit$

The next lemma gives some insight into the relationship between the valuation ring $\mathcal{O}_v$ and the field k:

Lemma 18. *Let $|-|_v$ be a non-archimedean absolute value on a field k. Then k is the fraction field of $\mathcal{O}_v$, and $\mathcal{O}_v$ is integrally closed in k.*

Proof. The first statement is obvious: Every $x \in k^\times$ satisfies either $x \in \mathcal{O}_v$ or $\frac{1}{x} \in \mathcal{O}_v$. For the second statement, let $x \in k$ be integral over $\mathcal{O}_v$. Then there exist $a_0, \dots, a_{n-1} \in \mathcal{O}_v$ such that

$$x^n = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0.$$

If $x \notin \mathcal{O}_v$, then $\frac{1}{x} \in \mathcal{O}_v$. Multiplying the above equality through by $\left(\frac{1}{x}\right)^{n-1}$ yields that

$$x = a_{n-1} + a_{n-2}\left(\tfrac{1}{x}\right) + \cdots + a_1\left(\tfrac{1}{x}\right)^{n-2} + a_0\left(\tfrac{1}{x}\right)^{n-1} \in \mathcal{O}_v,$$

a contradiction implying that $x \in \mathcal{O}_v$. ♠

2.2. **Discrete Absolute Values.** We shall now discuss another important property of absolute values. For any absolute value $|-|_v$ on a field k, we have that $|x|_v \in \mathbb{R}_{>0}$ for $x \in k^\times$, or equivalently, $\log|x| \in \mathbb{R}$ for $x \in k^\times$. But recall from Example 5 that for the p-adic norm $|-|_p$, we have something much stronger: $\log_p |x|_p \in \mathbb{Z} \subset \mathbb{R}$ for all $x \in \mathbb{Q}$. Absolute values whose logarithms take values in a discrete subgroup of $\mathbb{R}$ are given a special name:

Definition 19. An absolute value $|-|_v$ on a field k is said to be discrete if $\{\log|x|_v : x \in k^\times\} \subset \mathbb{R}$ is a discrete subgroup. Equivalently, $|-|_v$ is discrete if there exists $\delta > 0$ such that $|x|_v \in (1-\delta, 1+\delta) \Rightarrow |x|_v = 1$.

Absolute values that are both discrete and non-archimedean are of significant importance to the theory of valued fields. We will now discuss the properties of the valuation rings associated to such absolute values. We begin with the following characterization:

Lemma 20. *A non-archimedean absolute value is discrete if and only if its valuation ideal is principal.*

Proof. Let $|-|_v$ be a non-archimedean absolute value on a field k. First suppose $|-|_v$ is discrete. Then by definition, we have that the set $A = \{\log|a|_v : a \in k\}$ is a nontrivial discrete subgroup of $\mathbb{R}$. Thus, A is a free abelian group of rank 1 and is generated by its least positive element α. Let $\widetilde{\alpha} \in k$ be such that $\alpha = \log|\widetilde{\alpha}|_v$. Since $\alpha > 0$, we have that $|\widetilde{\alpha}|_v > 1$, so $\left|\frac{1}{\widetilde{\alpha}}\right|_v < 1$. We claim that $\mathfrak{p}_v$ is generated by $\frac{1}{\widetilde{\alpha}}$. We already showed that $\left|\frac{1}{\widetilde{\alpha}}\right|_v < 1$, so $\frac{1}{\widetilde{\alpha}} \in \mathfrak{p}_v$. Now if $\beta \in \mathfrak{p}_v$, we have that $|\beta|_v \leq \left|\frac{1}{\widetilde{\alpha}}\right|_v$, since α is the least positive element of A. Thus, $|\beta\widetilde{\alpha}|_v = |\beta|_v \cdot |\widetilde{\alpha}|_v \leq 1$, so $\beta\widetilde{\alpha} \in \mathcal{O}_v$, which implies that $\beta \in (\widetilde{\alpha})$. It follows that $\mathfrak{p}_v = (\widetilde{\alpha})$.

Now suppose $\mathfrak{p}_v$ is principal and generated by π. To show that $|-|_v$ is discrete, it suffices to show that there exists $\delta > 0$ such that for all $a \in k$ satisfying $|a|_v \in (1-\delta, 1+\delta)$ we have $|a|_v = 1$. Clearly any $\delta > 0$ satisfies $|a|_v \in (1-\delta, 1+\delta)$ if $|a|_v = 1$. If $|a|_v < 1$, then $a \in \mathfrak{p}_v$, so $a = r\pi$ for some $r \in \mathcal{O}_v$. Taking absolute values, we have that $|a|_v = |r|_v \cdot |\pi|_v \leq |\pi|_v$.

If $|a|_v > 1$, then $\left|\frac{1}{a}\right|_v < 1$, so $\left|\frac{1}{a}\right|_v \leq |\pi|_v$, which implies that $|a|_v \geq \frac{1}{|\pi|_v}$. Let $\delta = \max\left\{\frac{1}{|\pi|_v} - 1, 1 - |\pi|_v\right\}$. Then $|a|_v \neq 1$ implies that $1 + \delta \leq |a|_v$ or $1 - \delta \geq |a|_v$. Taking the contrapositive, we have that $|a|_v = 1$ for all $a \in k$ satisfying $|a|_v \in (1 - \delta, 1 + \delta)$. It follows that $|-|_v$ is discrete. ♠

Since equivalent absolute values give rise to the same valuation ring, we deduce from Lemma 20 that the property of being discrete is invariant under equivalence. The valuation ring associated to a discrete, non-archimedean absolute value is known as a discrete valuation ring (DVR). The following proposition gives a number of conditions that are necessary and sufficient for a ring to be a DVR:

Proposition 21. *Let R be a Noetherian local domain of Krull dimension* 1*, and let $\mathfrak{m} \subset R$ be its unique maximal ideal. Then, the following are equivalent:*

(1) R is a DVR.
(2) R is integrally closed in its field of fractions (i.e. R is Dedekind).
(3) $\mathfrak{m}$ is principal.
(4) Every nonzero proper ideal of R is a power of $\mathfrak{m}$.

Proof. That (1) implies (2) is a consequence of Lemma 18, for DVRs are valuation rings. To see that (3) implies (4), suppose $\mathfrak{m} = (t)$, and let I be any proper nonzero ideal of R. Since R is local, we have that $I \subset \mathfrak{m}$. By Krull's Intersection Theorem (for the statement and proof of this theorem, see Appendix 6), we have that $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$, so the set of all positive integers n satisfying $I \subset \mathfrak{m}^n$ is finite and nonempty; let N be the largest element of this set. Then there exists $x \in I$ such that $x \in \mathfrak{m}^N \setminus \mathfrak{m}^{N+1}$. We can therefore write x as $x = yt^N$ for $y \in R \setminus \mathfrak{m}$. But then y is a unit, so $t^N \in I$, implying that $I = (t^N) = \mathfrak{m}^N$.

It now remains to show that (2) implies (3) and that (4) implies (1); these two steps are a bit more involved. Suppose (2) holds, so that R is integrally closed in its field of fractions k, and take any $x \in R$. Since R is Noetherian, $(x) \supset \mathfrak{m}^n$ for some positive integer n. By taking n to be minimal, we can find $y \in \mathfrak{m}^{n-1} \setminus (x)$. We claim that $\mathfrak{m}$ is generated by $t = \frac{x}{y}$. To prove this claim, notice that $t^{-1}\mathfrak{m}$, which at first glance is just a R-submodule of k, is in fact an ideal of R. If $t^{-1}\mathfrak{m} \neq R$, then $t^{-1}\mathfrak{m} \subset \mathfrak{m}$, which implies that $\mathfrak{m}$ is a finitely-generated R-module with a faithful action of the ring $R[t^{-1}]$. It follows that t^{-1} is integral over R, so since R is integrally closed in k, we have that $t^{-1} \in R$, which contradicts the fact that $y = t^{-1}x \notin (x)$. Thus, we must have that $t^{-1}\mathfrak{m} = R$, so $\mathfrak{m} = (t)$, as claimed.

Finally, suppose (4) holds, so that every nonzero proper ideal of R is a power of $\mathfrak{m}$. We first observe that $\mathfrak{m}$ is principal, because if $t \in \mathfrak{m} \setminus \mathfrak{m}^2$, then $(t) = \mathfrak{m}^n$ for some positive integer n, but we must have $n = 1$, implying that $\mathfrak{m} = (t)$. We must now construct a field k and a discrete, non-archimedean absolute value $|-|_v$

such that $R = \mathcal{O}_v$. Let k be the field of fractions of R, and let $|-|_v$ be defined as follows: let $|0|_v = 0$, let $|u|_v = 1$ for all units $u \in R$, and for all other $x \in R$, let $|x|_v = \exp(-n)$, where n is the unique positive integer such that $(x) = \mathfrak{m}^n$. Extend $|-|_v$ to a function on all of k in the obvious way by setting $\left|\frac{x}{y}\right|_v = \frac{|x|_v}{|y|_v}$ for all nonzero $x, y \in R$. One readily checks that $|-|_v$ satisfies positive-definiteness and multiplicativity. To see that the ultra-metric inequality holds, observe that if $(x) = (t^m)$ and $(y) = (t^n)$ where $m \leq n$ are nonnegative integers (here, we are abusing notation slightly by taking the zeroth power of an element to be 1), then $(x + y) \subset (t^m)$, so $|x + y|_v \leq \exp(-m) = \max\{|x|_v, |y|_v\}$, as desired. Observe that by construction we have $|x|_v \leq 1$ if and only if $x \in R$, so $R = \mathcal{O}_v$ and $\mathfrak{m} = \mathfrak{p}_v$. Lastly, to see that $|-|_v$ is discrete, it suffices by Lemma 20 to check that $\mathfrak{p}_v = \mathfrak{m}$ is principal, but we already proved this. ♠

Remark. A generator of the maximal ideal in a DVR is often called a uniformizing parameter, or uniformizer for short.

We conclude this subsection with an example describing the valuation ring of the p-adic norm:

Example 22. Consider the p-adic norm $|-|_p$ on $\mathbb{Q}$. Since $|-|_p$ is non-archimedean, we can compute its valuation ring $\mathcal{O}_p$, valuation ideal $\mathfrak{p}_p$, and residue field κ_p. We claim that $\mathcal{O}_p = \mathbb{Z}_{(p)}$ (the localization of $\mathbb{Z}$ away from the ideal (p)), that $\mathfrak{p}_p = p\mathbb{Z}_{(p)}$, and that $\kappa_p = \mathbb{F}_p$. Indeed, observe that if $x \in \mathbb{Z}_{(p)}$, then we can write $x = \frac{a}{s}$ for $a \in \mathbb{Z}$ and $s \in \mathbb{Z} \setminus (p)$, from which it is easy to see that $|x|_p \leq 1$, with strict inequality when x is divisibly by p; it follows that $\mathcal{O}_p = \mathbb{Z}_{(p)}$ (this is often called the ring of p-adic integers) and $\mathfrak{p}_p = p\mathbb{Z}_{(p)}$. To show that $\kappa_p = \mathbb{F}_p$, we must show that $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{F}_p$, but this follows from the fact that localization is an exact functor.

Note that because $|-|_p$ is discrete, the ring $\mathcal{O}_p = \mathbb{Z}_{(p)}$ is a DVR. This can also be deduced by observing that $\mathbb{Z}$ is both Noetherian and Dedekind, so localizing $\mathbb{Z}$ away from a prime ideal will always yield a DVR. ♣

3. Completions and Finite Extensions

Recall that in Section 1, we showed that the field $\mathbb{Q}_p$ of p-adic numbers is a proper extension of $\mathbb{Q}$ by considering the formal finite-tailed Laurent series

$$\sum_{n\geq 0} a_n p^n,$$

where for each $n \geq 0$ we took a_n to be such that $\sum_{i=0}^n a_i p^i$ is a solution to $f(x) \equiv 0 \pmod{p^n}$, with f being a quadratic polynomial that is irreducible over $\mathbb{Q}$. Notice that the sequence of partial sums $\{\sum_{i=0}^n a_i p^i\}_{n\in\mathbb{N}}$ is Cauchy in the p-adic norm; indeed, $|\sum_{i=m}^n a_i p^i|_p \leq p^{-m}$ for all nonnegative integers $m \leq n$. It follows that $\mathbb{Q}$ is not complete in the metric given by the p-adic norm. In this section, will study the completions of fields with respect to the topologies induced by absolute values. After a brief interlude on characterizing archimedean valued fields, we will use our understanding of completions to study finite extensions of valued fields.

3.1. **Completions.** If an absolute value $|-|_v$ on a field k gives rise to a metric on k, then we could decide whether k is complete or not by simply viewing it as a metric space and appealing to the already-developed theory of completions on metric spaces. However, only absolute values satisfying the triangle inequality give rise to well-defined metrics, so we shall start from scratch. We begin by defining what it means for a valued field to be complete:

Definition 23. We say that a field k is complete with respect to an absolute value $|-|_v$ if it is complete with respect to the topology induced by $|-|_v$ (i.e. for every sequence $\{a_n\}_{n\in\mathbb{N}} \subset k$ such that $|a_n - a_m| \to 0$ as $m, n \to \infty$, there exists $a \in k$ such that $\lim_{n\to\infty} a_n = a$).

Notice that the property of being complete with respect to an absolute value is preserved under equivalence of absolute values (this can be seen either by appealing to Lemma 8 or by directly applying the definition of equivalence). We can therefore replace our absolute values with ones satisfying the triangle inequality, while still keeping our field complete. The following theorem tells us that every valued field can be embedded in a nice way into a complete valued field:

Theorem 24. *Let $|-|_v$ be an absolute value on a field k. There exists a unique field extension $\overline{k}$ of k and absolute value $|-|_{v'}$ on $\overline{k}$ such that $\overline{k}$ is complete with respect to $|-|_{v'}$, such that $|x|_{v'} = |x|_v$ for all $x \in k$, and such that k is dense in $\overline{k}$.*

Proof. We may assume that $|-|_v$ satisfies the triangle inequality, so that k is a metric space with respect to the metric induced by $|-|_v$. Let K be the set of all sequences in k that are Cauchy with respect to $|-|_v$, and observe that K is a ring under the operations of termwise addition and multiplication. Let $M \subset K$ be the set of all sequences in k that are not only Cauchy, but also converge to 0 with respect to $|-|_v$, and observe that M is a maximal ideal of K. Take $\overline{k} = K/M$, notice that k embeds in K/M as the subfield of equivalence classes of constant sequences with values in k, and let $|-|_{v'}$ be defined by continuously extending $|-|_v$ to all of K/M. It is now not difficult to check that $\overline{k}$ satisfies the necessary properties. Indeed, the field $\overline{k}$, viewed as a metric space, is the completion of k with respect to the metric induced by $|-|_v$, and the absolute value $|-|_{v'}$ restricts to $|-|_v$ on the subfield k. Uniqueness follows from the fact that k is dense in $\overline{k}$, so the field operations and absolute value must all continuously extend from k to $\overline{k}$ and are therefore uniquely defined. ♠

By the uniqueness statement of Theorem 24, there is no ambiguity in using the notation $|-|_v$ to denote the absolute value on the completion $\overline{k}$ of a field k with absolute value $|-|_v$, so that is what we will do. The next lemma states that the property of being non-archimedean is preserved by field extensions (and hence by completions):

Lemma 25. *Let $|-|_v$ be an absolute value on a field k, let ℓ be any field extension of k, and let $|-|_{v'}$ be an absolute value on ℓ that extends $|-|_v$. Then $|-|_v$ is non-archimedean if and only if $|-|_{v'}$ is non-archimedean. Moreover, if $|-|_v$ is indeed non-archimedean, we have $\{|x|_v : x \in k\} = \{|x|_v : x \in \overline{k}\}$.*

Proof. By Lemma 11, an absolute value $|-|_v$ is non-archimedean if and only if $|n|_v \leq 1$ for all $n = \sum_{i=1}^{n} 1$. Clearly, this property is preserved by taking field extensions and by restricting to subfields, so we have the first statement. For the second statement, take $y \in \overline{k}^{\times}$. Then there exists $x \in k$ such that $|x-y|_v < |y|_v$, so by Lemma 13 we have $|x|_v = |y|_v$. It follows that $\{|x|_v : x \in k\} \supset \{|x|_v : x \in \overline{k}\}$, and the reverse containment is obvious, so we are done. ♠

Remark. It follows from the second statement Lemma 25 that the property of a non-archimedean absolute value being discrete is preserved under completions.

The following theorem can be viewed as a generalization of the Chinese Remainder Theorem and tells us that inequivalent absolute values are about as independent as possible:

Theorem 26 (Weak Approximation). *Let $|-|_1, \dots, |-|_N$ be a list of nontrivial, inequivalent absolute values, and let k_n denote the completion of k with respect to $|-|_n$. Then the image of k under the diagonal embedding $\Delta : k \hookrightarrow \prod_{n=1}^{N} k_n$ is dense.*

Proof. Fix $\varepsilon > 0$, and take $(y_1, \dots, y_N) \in \prod_{n=1}^{N} k_n$. Choose $(x_1, \dots, x_N) \in k^N \subset \prod_{n=1}^{N} k_n$ such that $|x_n - y_n|_n < \varepsilon$ for all $n \in \{1, \dots, N\}$. Suppose for every $n \in \{1, \dots, N\}$ that there exists $t_n \in k$ such that $|t_n|_n > 1$ but $|t_n|_m < 1$ for all $m \neq n$. Then for all $n \in \{1, \dots, N\}$ we have

$$\lim_{r \to \infty} \frac{t_n^r}{1 + t_n^r} \to \begin{cases} 1 & \text{w.r.t } |-|_n, \\ 0 & \text{w.r.t. } |-|_m \text{ for } m \neq n \end{cases}$$

It follows that for sufficiently large r we have

$$\left| x_m - \sum_{n=1}^{N} \frac{t_n^r}{1 + t_n^r} \cdot x_n \right|_m < \varepsilon \quad \Rightarrow \quad \left| y_m - \sum_{n=1}^{N} \frac{t_n^r}{1 + t_n^r} \cdot x_n \right|_m < 2\varepsilon$$

for every $m \in \{1, \dots, N\}$, in which case we would be done. All that remains is to construct the desired t_n's, for which we will resort to induction. Note that we only need to construct t_1, as the argument will be the same for $t_2, \dots, t_N$. If

$N = 2$, then since $|-|_1$ and $|-|_2$ are inequivalent, there exist $a, b \in k$ such that $|a|_1 < |b|_1$ and $|a|_2 < |b|_2$, so we can take $t_1 = \frac{a}{b}$. If $N \geq 3$, by induction, there exists t_1' such that $|t_1'|_1 > 1$ and $|t_1'|_m < 1$ for all $m \in \{1, \ldots, N-1\}$. Take t_1'' with $|t_1''|_1 > 1$ and $|t_1''|_N < 1$. We may then take t_1 to be given as follows:

$$t_1 = \begin{cases} t_1' & \text{if } |t_1|_N < 1, \\ (t_1')^r \cdot t_1'' & \text{for large enough } r \text{ if } |t_1'|_N = 1, \\ \frac{(t_1')^r}{1+(t_1')^r} \cdot t_1'' & \text{for large enough } r \text{ if } |t_1'|_N > 1 \end{cases}$$

One verifies that the above selection for t_1 works, so we have the theorem. ♠

We will now study the case when our absolute value $|-|_v$ on k is non-archimedean. Let $\overline{\mathcal{O}}_v$, $\overline{\mathfrak{p}}_v$, and $\overline{\kappa}_v$ denote the valuation ring, valuation ideal, and residue field, respectively, of the completion $\overline{k}$. Observe that we have the following commutative square, with the horizontal maps given by projection and the vertical map $\mathcal{O}_v \hookrightarrow \overline{\mathcal{O}}_v$ given by inclusion:

$$\begin{tikzcd}
\mathcal{O}_v \arrow[r, two heads] \arrow[d, hook] & \kappa_v \arrow[d, dashed, "\phi"] \\
\overline{\mathcal{O}}_v \arrow[r, two heads] & \overline{\kappa}_v
\end{tikzcd}$$

The composite map $\mathcal{O}_v \to \overline{\kappa}_v$ (given by going down and then right in the above diagram) clearly has kernel $\mathfrak{p}_v$, so we obtain an injective map $\phi : \kappa_v \to \overline{\kappa}_v$; indeed, any extension of non-archimedean valued fields gives rise to an extension of the corresponding residue fields. We claim that ϕ is also surjective, and hence an isomorphism. To see why this claim holds, take a nonzero $y \in \overline{\mathcal{O}}_v$. Then there exists $x \in k$ such that $|x-y|_v < |y|_v$, so by Lemma 13 we have $|x|_v = |y|_v$, implying that $x \in \mathcal{O}_v$. But $|x-y|_v < |y|_v \leq 1$, so $x - y \in \overline{\mathfrak{p}}_v$. It follows that ϕ takes the class of x in κ_v to the class of y in $\overline{\kappa}_v$. We deduce that ϕ is surjective.

Suppose further that our absolute value $|-|_v$ is discrete. Recall in this case that the valuation ring $\mathcal{O}_v$ is a DVR with principal maximal ideal $\mathfrak{p}_v$, generated by a uniformizer that we shall call π_v. Then by Proposition 21, every $x \in k$ can be expressed as $x = u \cdot \pi_v^n$, where $u \in \mathcal{O}_v^\times$ and $n \in \mathbb{Z}$, with $n \geq 0$ if and only if $x \in \mathcal{O}_v$. The integer n is called the order of x and is independent of the choice of uniformizer π_v.

We can compute $\overline{\mathfrak{p}}_v$ in terms of our uniformizer π_v. Take $y \in \overline{\mathfrak{p}}_v$, and let $\{x_n\}_{n \in \mathbb{N}} \subset k$ be a sequence converging to y. Then Lemma 13 tells us that for sufficiently large n we have $|x_n|_v = |y|_v$, implying that $x_n \in \mathfrak{p}_v$. Thus, π_v divides x_n for sufficiently large n, and so π_v divides y. Since $\pi_v \in \mathfrak{p}_v \subset \overline{\mathfrak{p}}_v$, we conclude that $\overline{\mathfrak{p}}_v = (\pi_v)$, as an ideal of the ring $\overline{\mathcal{O}}_v$. Therefore, $\overline{\mathcal{O}}_v$ is a DVR with principal maximal ideal $\overline{\mathfrak{p}}_v = (\pi_v)$. Again, by Proposition 21, every $y \in \overline{k}$ can be expressed as $y = u \cdot \pi_v^n$, where $u \in \overline{\mathcal{O}_v}^\times$ and $n \in \mathbb{Z}$.

As we might expect, we can express each element of $\overline{\mathcal{O}}_v$ as a power series in π_v with coefficients in $\mathcal{O}_v$. Take $y \in \overline{\mathcal{O}}_v$, and let $S \subset \mathcal{O}_v$ be a system of representatives of κ_v. By definition, there exists a unique $a_0 \in S$ such that $y \equiv a_0 \pmod{\overline{\mathfrak{p}}_v}$, and there exists a unique $a_1 \in S$ such that $\pi_v^{-1}(y - a_0) \equiv a_1$ $(\text{mod } \overline{\mathfrak{p}}_v)$. Continuing in this manner, we obtain a sequence $\{a_n\}_{n \in \mathbb{N}}$ of elements of S such that $y \equiv \sum_{i=0}^{n} a_i \pi_v^i \pmod{\overline{\mathfrak{p}}_v^{n+1}}$ for each $n \in \mathbb{N}$. It follows that up to our choice of representatives S, we can uniquely express any $y \in \overline{\mathcal{O}}_v$ as $y = \sum_{n=0}^{\infty} a_i \pi_v^i$ (the convergence of this series is manifest). We deduce that every $y \in \overline{k}$ can be uniquely expressed as $y = \sum_{n \geq n_0} a_i \pi_v^i$ for some $n_0 \in \mathbb{Z}$, because we can write y as $y = u \cdot \pi_v^{n_0}$ for $u \in \overline{\mathcal{O}}_v$ and write u as $u = \sum_{n=0}^{\infty} a_i \pi_v^i$.

In this case where κ_v is a finite field, we can say something interesting about the topology of the valuation ring $\mathcal{O}_v$:

Proposition 27. *Let $| - |_v$ be a discrete, non-archimedean absolute value on a field k, and suppose k is complete with respect to $| - |_v$. Then $\mathcal{O}_v$ is compact if and only if κ_v is finite.*

Proof. Notice first that $x + \mathfrak{p}_v$ is an open subset of k for any $x \in k$. Let $S \subset \mathcal{O}_v$ be a system of representatives of κ_v. Then $\mathcal{O}_v = \bigsqcup_{a \in S}(a + \mathfrak{p}_v)$, which is a covering of $\mathcal{O}_v$ by open sets. If $\mathcal{O}_v$ is compact, then the covering has a finite subcover, which implies that S must itself be finite. On the other hand, suppose κ_v is finite. To show that $\mathcal{O}_v$ is compact, we need only show that $\mathcal{O}_v$ is totally bounded, because it is complete by assumption. Take $\varepsilon \in \mathbb{R}_{>0}$, and let $n \in \mathbb{N}$ be so large that $|\pi_v|_v^{n+1} < \varepsilon$. Since κ_v is finite, there are only finitely many elements of $\mathcal{O}_v$ having the form $\sum_{i=0}^{n} a_i \pi_v^i$ with $a_i \in S$ for all $i \in \{0, \ldots, n-1\}$. But every element of $\mathcal{O}_v$ is within ε of such an element, because if $a_i \in S$ for all $i \geq n+1$ we have by the ultra-metric inequality that

$$\left| \sum_{i \geq n+1} a_i \pi_v^i \right|_v \leq \sum_{i \geq n+1} |a_i|_v \cdot |\pi_v|_v^i \leq |\pi_v|_v^{n+1} < \varepsilon.$$

It follows that $\mathcal{O}_v$ is complete and totally bounded, hence compact. ♠

It follows from Proposition 27 that k is locally compact, because any translate $x + \mathcal{O}_v$ for $x \in k$ must be compact; such fields are known more generally as local fields. We conclude this section by discussing our results in the all-too-familiar context of the p-adic norm.

Example 28. In the case of the p-adic norm, we have $\mathcal{O}_p = \mathbb{Z}_{(p)}$, $\mathfrak{p}_p = (p)$, and $\kappa_p = \mathbb{F}_p$, so we can take $S = \{0, \ldots, p-1\}$. Taking p to be our uniformizer, we have proven that

$$\mathbb{Z}_{(p)} = \left\{ \sum_{n=0}^{\infty} a_n p^n : a_n \in \{0, \dots, p-1\} \right\}, \text{ and}$$
$$\overline{\mathbb{Q}} = \left\{ \sum_{n \geq n_0}^{\infty} a_n p^n : a_n \in \{0, \dots, p-1\}, n_0 \in \mathbb{Z} \right\},$$

where by $\overline{\mathbb{Q}}$ we mean the completion of $\mathbb{Q}$ with respect to the p-adic norm. Note that in this case, the residue field is finite, so $\mathbb{Z}_{(p)}$ is compact, and $\overline{\mathbb{Q}}$ is a local field. But recall that we had defined the field $\mathbb{Q}_p$ of p-adic numbers to be the set of all formal finite-tailed Laurent series in p with coefficients in $\{0, \dots, p-1\}$. It follows that $\mathbb{Q}_p$ is none other than the completion of $\mathbb{Q}$ with respect to the p-adic norm. ♣

We have now accomplished what we set out do to; indeed, our motivation for introducing absolute values in the first place was to provide a more natural construction for the field $\mathbb{Q}_p$ of p-adic numbers. But along the way, we have introduced so much theory and opened up so many possibilities for discussion that we simply cannot stop here.

3.2. **Finite Extensions.**

Recall that if $k \hookrightarrow \ell$ is an extension of fields, then we may view ℓ as a k-vector space; in particular, when the extension is finite, ℓ is a finite-dimensional vector space over k. One might hope that we can use this fact to construct absolute values on ℓ given absolute values on k. In this light, we shall now introduce the theory of normed vector spaces to study finite extensions. Recall that the standard way of putting a measure of size on a vector space is to introduce a norm, which is defined as follows:

Definition 29. Let $| - |_v$ be an absolute value on a field k, and let V be a k-vector space. A norm on k is a function $|| - || : V \to \mathbb{R}_{\geq 0}$ that satisfies the following three properties:

1. Positive-definiteness: $||w|| = 0$ if and only if $w = 0$.
2. Scalar Multiplication: $||xw|| = |x|_v \cdot ||w||$ for all $x \in k$ and $w \in V$.
3. Triangle Inequality: $||w + w'|| \leq ||w|| + ||w'||$ for all $w, w' \in V$.

The vector space V, along with the norm $||-||$, is known as a normed vector space.

Notice that norms (see Definition 29) are defined in a way that is very similar to how absolute values are defined (see Definition 1), so it is reasonable to expect that we can use norms to construct absolute values on field extensions. Just as with absolute values that satisfy the triangle inequality, a norm on a vector space V gives rise to a metric on V, defined in the obvious way. Finally, norms have a notion of equivalence just like absolute values do: we say that two norms

$||-||_1$ and $||-||_2$ on a vector space V are equivalent if there exist positive constants $C_1 < C_2$ such that $\frac{||w||_1}{||w||_2} \in [C_1, C_2]$ for all $w \in V \setminus \{0\}$.

The next proposition roughly states that under certain conditions, there is essentially only one norm on a vector space V:

Proposition 30. *Let $|-|_v$ be an absolute value on a field k with respect to which k is complete. If V is a finite-dimensional k-vector space, then any two norms on V are equivalent.*

Proof. We will construct a specific norm $||-||_0$ on V and then prove that any other norm must be equivalent to $||-||_0$. Take a basis $(b_1, \dots, b_n)$ of V, and define $||a_1b_1 + \cdots + a_nb_n||_0 = \max\{|a_i|_v : i \in \{1, \dots, n\}\}$ for all $a_1, \dots, a_n \in k$. It is easy to check that $||-||_0$, as defined, is a norm on V (it clearly satisfies the three defining properties of a norm).

Now let $||-||$ be any norm on V. Clearly we have that

$$\left|\left|\sum_{i=1}^n a_ib_i\right|\right| \leq \sum_{i=1}^n |a_i|_v \cdot ||b_i|| \leq \left(\sum_{i=1}^n ||b_i||\right) \cdot \left|\left|\sum_{i=1}^n a_ib_i\right|\right|_0 .$$

Taking $C_2 = \sum_{i=1}^n ||b_i|| > 0$ yields that $\frac{||w||}{||w||_0} \leq C_2$ for all $w \in V \setminus \{0\}$. Suppose we cannot find a positive constant $C_1 \leq C_2$ such that $\frac{||w||}{||w||_0} \geq C_1$ for all $w \in V \setminus \{0\}$. Then for every positive integer $j > 0$, there exist elements $a'_{1,j}, \dots, a'_{n,j} \in k$ such that

$$0 < \left|\left|\sum_{i=1}^n a'_{i,j}b_i\right|\right| \leq \frac{1}{j} \cdot \left|\left|\sum_{i=1}^n a'_{i,j}b_i\right|\right|_0 .$$

We may assume without loss of generality that $1 = |a'_{1,j}|_v = \max\{|a'_{i,j}|_v : i \in \{1, \dots, n\}\}$ for infinitely many j. It follows that for each $i \in \{2, \dots, n\}$, there exist sequences $\{a_{i,j}\}_{j\in\mathbb{N}}$ such that

$$\lim_{j\to\infty} \left|\left|b_1 + \sum_{i=2}^n a_{i,j}b_i\right|\right| = 0, \quad \text{and} \quad \lim_{j,k\to\infty} \left|\left|\sum_{i=2}^n (a_{i,j} - a_{i,k})b_i\right|\right| = 0. \tag{4}$$

We now proceed by induction. The proposition is obvious in the case when $n = 1$, for then we can take $C_1 = ||b_1||$. Suppose $n \geq 2$, and assume by induction that the proposition holds on the subspace $\text{span}(b_2, \dots, b_n)$. Then (4) implies that $\lim_{j,k\to\infty} |a_{i,j} - a_{i,k}|_v = 0$ for each $i \in \{2, \dots, n\}$. Thus, the sequences $\{a_{i,j}\}_{j\in\mathbb{N}}$ are all Cauchy, so since k is complete, for each $i \in \{2, \dots, n\}$ there exists $c_i \in k$ such that $\lim_{j\to\infty} a_{i,j} = c_i$. But then we have that

$$0 < \left|\left|b_1 + \sum_{i=2}^n c_ib_i\right|\right| \leq \lim_{j\to\infty} \left|\left|b_1 + \sum_{i=2}^n a_{i,j}b_i\right|\right| + \left|\left|\sum_{i=2}^n (c_i - a_{i,j})b_i\right|\right| = 0,$$

which is a contradiction. ♠

Remark. As it happens, the topology of V with respect to the metric induced by $||-||_0$ is none other than the product topology on $V \simeq k^n$, where the identification is given by the choice of basis. To see why, take $a_1, \dots, a_n \in k$. The open ball of radius r centered at $a_1b_1 + \cdots + a_nb_n \in V$ is given by

$$\{c_1b_1 + \cdots + c_nb_n : |c_i - a_i|_v < r \text{ for all } i \in \{1, \dots, n\}\}.$$

It is clear that the above set is simply the product over each factor of k in $V \simeq k^n$ of the open ball of radius r centered at a_i. Thus, every set that is open in the metric topology on V is open in the product topology on $V \simeq k^n$. For the reverse containment, suppose we have an open ball B_i of radius r_i centered at a_i in each factor of k in $V \simeq k^n$. Let $r = \min\{r_i : i \in \{1, \dots, n\}\}$, and for each i, choose a covering $\bigcup_{\alpha_i \in A_i} B_{\alpha_i}$ of B_i by open balls B_{α_i} of radius r such that $B_{\alpha_i} \subset B_i$ for all $\alpha_i \in A_i$. Then we have that

$$\prod_{i=1}^n B_i = \bigcup_{\alpha_1 \in A_1} \cdots \bigcup_{\alpha_n \in A_n} \prod_{i=1}^n B_{\alpha_i},$$

and the set on the right-hand-side of the above equality is clearly open in the metric topology on V.

Also, the proof of Proposition 30 is quite a bit simpler in the case where $|-|_v$ is discrete and non-archimedean with finite residue field κ_v and k is complete with respect to $|-|_v$. For in this case, we can appeal to Proposition 27 and utilize compactness along with the Extreme Value Theorem to obtain the desired bounds C_1 and C_2. In fact, this alternative method of proof works for any locally compact valued field, and hence over the fields $\mathbb{R}$ and $\mathbb{C}$ equipped with the archimedean absolute value (that these fields are locally compact is geometrically obvious).

Proposition 30 has the following important consequence for finite extensions on our field k:

Corollary 31. *Let $|-|_v$ be an absolute value on a field k such that k is complete with respect to $|-|_v$. If $k \hookrightarrow \ell$ is a finite extension, then there exists a unique absolute value $|-|_{v'}$ on ℓ whose restriction to k is $|-|_v$. In particular, setting $[\ell : k] = n$, then we can take $|x|_{v'} = \left|\mathrm{Nm}_{\ell/k}(x)\right|_v^{\frac{1}{n}}$.*

Remark. In the following proof, we will assume that k is locally compact. Note that $|x|_{v'} = \left|\mathrm{Nm}_{\ell/k}(x)\right|_v^{\frac{1}{n}}$ is a well-defined absolute value on ℓ even in the case when k is not locally compact. The proof, however, is somewhat more laborious, and the case when k is locally compact is of particular importance in the theory.

Proof. We deal with uniqueness first. Suppose we have two different absolute values $|-|_{v'}$ and $|-|_{v''}$ whose restriction to k is given by $|-|_v$. Let $c \in \mathbb{R}_{>0}$ be such that $|-|_v^c$, $|-|_{v'}^c$, and $|-|_{v''}^c$ all satisfy the triangle inequality. Then

$|-|_{v'}^c$ and $|-|_{v''}^c$ are norms on ℓ, viewed as a k-vector space, and note that k is still complete with respect to $|-|_v^c$. But by Proposition 30, the norms $|-|_{v'}^c$ and $|-|_{v''}^c$ are equivalent, and hence the absolute values $|-|_{v'}$ and $|-|_{v''}$ must be the same.

For existence, we need to check that $|x|_{v'} = \left|\mathrm{Nm}_{\ell/k}(x)\right|^{\frac{1}{n}}$ is an absolute value on ℓ whose restriction to k is $|-|_v$. Positive-definiteness and multiplicativity follow immediately from the definition of $\mathrm{Nm}_{\ell/k}(x)$ as the determinant of the map of multiplication by x on ℓ, viewed as a k-vector space. We must now show that there exists a constant $C \in \mathbb{R}_{\geq 1}$ such that $|x|_{v'} \leq 1$ implies $|1+x|_{v'} \leq C$. Recall the norm $||-||_0$ defined in the proof of Proposition 30, and put this norm on ℓ, viewed as a k-vector space. One can check that $|-|_{v'}$ is continuous with respect to topology given by $||-||_0$, and in particular, it is continuous on the set $S = \{x \in \ell : ||x||_0 = 1\}$, which is compact because we assumed k to be locally compact. Thus, there exist positive constants $C_1 < C_2$ with $C_1 \leq ||x|| \leq C_2$ for all $x \in S$, so $C_1 \leq \frac{||x||}{||x||_0} \leq C_2$ for all $x \in \ell$. We can then take $C = C_2(||1||_0 + C_1^{-1})$. $\spadesuit$

Corollary 32. *Under the assumptions of Corollary 31, ℓ is complete with respect to $|-|_{v'}$.*

Proof. By Proposition 30, the norm given by $|-|_{v'}$ is equivalent to the norm $||-||_0$ (which we defined in the proof of Proposition 30). As we showed earlier, the topology given by $||-||_0$ is the product topology, so $\ell \simeq k^n$ is the product of n complete metric spaces and is therefore complete. $\spadesuit$

We have just shown that under finite field extensions, absolute values on complete fields extend in a unique way. However, the situation when our base field is not complete is considerably more complicated; in this case, the following theorem tells us that an absolute value can extend in more than one way under a finite field extension:

Theorem 33. *Fix $|-|_v$ an absolute value on a field k, and let $k \hookrightarrow \ell$ be a finite separable extension of degree $[\ell : k] = n$. Then there are at most n extensions of $|-|_v$ to ℓ, which we will denote by $|-|_{v_1}, \dots, |-|_{v_N}$. Furthermore, let $\overline{k}$ denote the completion of k with respect to $|-|_v$, and let ℓ_{v_i} denote the completion of ℓ with respect to $|-|_{v_i}$ for each $i \in \{1, \dots, N\}$. Then*

$$\overline{k} \otimes_k \ell \simeq \bigoplus_{i=1}^{N} \ell_{v_i}.$$

Proof. By the Primitive Element Theorem (which applies because the extension $k \hookrightarrow \ell$ is separable; see Appendix 6 for a statement and proof), we can write $\ell = k(\alpha)$ for some $\alpha \in \ell$. Let $f \in k[x]$ be the minimal polynomial of α over k, and let $N = \deg f$. Then $\ell \simeq k[x]/(f)$, so $\overline{k} \otimes_k \ell \simeq \overline{k}[x]/(f)$. Now suppose f

factors over $\overline{k}$ as $f = \prod_{i=1}^{J} g_i$, where each $g_i \in \overline{k}[x]$ is irreducible and the g_i's are all pairwise distinct (because the extension $k \hookrightarrow \ell$ is separable). Then we have that

$$\overline{k} \otimes_k \ell \simeq \overline{k}[x]/(f) \simeq \bigoplus_{i=1}^{J} \overline{k}[x]/(g_i).$$

Let $\widetilde{\ell}_i = \overline{k}[x]/(g_i)$ for each $i \in \{1, \dots, J\}$. We shall prove that the two sets $\{\widetilde{\ell}_i : i \in \{1, \dots, J\}\}$ and $\{\ell_{v_i} : i \in \{1, \dots, N\}\}$ are one and the same.

Consider the obvious map $\ell \hookrightarrow \overline{k} \otimes_k \ell$ given by $y \mapsto 1 \otimes y$. Postcomposing this map with the projection from $\overline{k} \otimes_k \ell$ onto the factor $\widetilde{\ell}_i$ yields a field extension $\ell \hookrightarrow \widetilde{\ell}_i$ (this map is injective because the map $\ell \hookrightarrow \overline{k} \otimes_k \ell \twoheadrightarrow \widetilde{\ell}_i$ is a composition of ring homomorphisms whose source is a field). Note that the embedding $\ell \hookrightarrow \overline{k} \otimes_k \ell$ is dense because $\ell \simeq k \otimes_k \ell$ and k is dense in $\overline{k}$. It follows that the embedding $\ell \hookrightarrow \widetilde{\ell}_i$ is also dense. But $\widetilde{\ell}_i$ is a finite extension of $\overline{k}$ for each $i \in \{1, \dots, J\}$, so by Corollaries 31 and 32, $\widetilde{\ell}_i$ is complete with respect to a unique absolute value $| - |_{v_{i'}}$ on $\widetilde{\ell}_i$ whose restriction to $\overline{k}$ gives $| - |_v$. We deduce that $\widetilde{\ell}_i$ is the completion of ℓ with respect to $| - |_{v_{i'}}$. It follows that $\{\widetilde{\ell}_i : i \in \{1, \dots, J\}\} \subset \{\ell_{v_i} : i \in \{1, \dots, N\}\}$.

For the reverse containment, suppose an absolute value $| - |_{v'}$ on ℓ is an extension of $| - |_v$ on k. Then by continuity we can extend $| - |_{v'}$ to a multiplicative function on the ring $\overline{k} \otimes_k \ell$, and we can subsequently restrict $| - |_{v'}$ to any of the $\widetilde{\ell}_i$'s. If $|x_i|_{v'} = 0$ for some nonzero $x_i \in \widetilde{\ell}_i$, then the restriction of $| - |_{v'}$ to $\widetilde{\ell}_i$ is identically 0, but otherwise one can check that it does give an absolute value on $\widetilde{\ell}_i$. But $| - |_{v'}$ cannot possibly give an absolute value on more than one of the $\widetilde{\ell}_i$'s, because otherwise by taking $x_i \in \widetilde{\ell}_i^{\times}$ and $x_j \in \widetilde{\ell}_j^{\times}$, we would have that $|x_i|_{v'} \cdot |x_j|_{v'} = 0$ which is a contradiction. It follows that there exists a unique $i \in \{1, \dots, J\}$ for which $| - |_{v'}$ gives an absolute value on $\widetilde{\ell}_i$, and by Corollary 31, $| - |_{v'}$ must restrict to $| - |_{v_{i'}}$ on $\widetilde{\ell}_i$. It follows that $\{\widetilde{\ell}_i : i \in \{1, \dots, J\}\} \supset \{\ell_i : i \in \{1, \dots, N\}\}$. ♠

The next corollary demonstrates how we might use the result of Theorem 33 to compute the trace and norm of a finite extension of valued fields:

Corollary 34. *Retain the setting of Theorem 33. Then for any $\alpha \in \ell$ we have*

$$\mathrm{Tr}_{\ell/k}(\alpha) = \sum_{i=1}^{N} \mathrm{Tr}_{\ell_{v_i}/\overline{k}}(\alpha) \quad \textit{and} \quad \mathrm{Nm}_{\ell/k}(\alpha) = \prod_{i=1}^{N} \mathrm{Nm}_{\ell_{v_i}/\overline{k}}(\alpha).$$

Proof. Since the trace (resp. determinant) of a block-diagonal matrix is the sum (resp. product) of the traces (resp. determinants) of the blocks, to prove the corollary it suffices to show that the trace and determinant maps are preserved under tensoring up from ℓ to $\overline{k} \otimes_k \ell$. Indeed, if $(\omega_1, \dots, \omega_n)$ is a basis of ℓ as a k-vector space, let M_a denote the corresponding matrix of the map $m_a : \ell \to \ell$ of multiplication by a. Then the map $m_a \otimes \mathrm{id} : \ell \otimes_k \overline{k} \to \ell \otimes_k \overline{k}$ has matrix M_a with respect to the basis $(\omega_1 \otimes 1, \dots, \omega_n \otimes 1)$. Since trace and determinant are independent of the choice of basis, the trace and determinant of m_a are equal to the trace and determinant of $m_a \otimes \mathrm{id}$. Thus, we have the corollary. ♠

We will explore what the above-developed theory of absolute values tells us about number fields in the next section.

4. Number Fields

A number field is, by definition, a finite extension of the field $\mathbb{Q}$ of rational numbers. In Section 3.2, we studied finite extensions of valued fields, so to understand number fields, it seems reasonable to start off by asking what our theory of absolute values tells us about $\mathbb{Q}$ itself. The following theorem states that the standard and p-adic absolute values are the only absolute values that we can put on $\mathbb{Q}$:

Theorem 35 (Little Ostrowski). *Let $|-|_v$ be an absolute value on $\mathbb{Q}$. If $|-|_v$ is non-archimedean, then $|-|_v$ is equivalent to a p-adic norm. Otherwise, if $|-|_v$ is archimedean, then $|-|_v$ is equivalent to the standard absolute value.*

Proof. Suppose first $|-|_v$ is non-archimedean. Consider the ideal $I = \{n \in \mathbb{Z} : |n|_v < 1\} \subset \mathbb{Z}$ (which is an ideal because of the ultra-metric inequality and because Lemma 11 tells us that $|n|_v \leq 1$ for all $n \in \mathbb{Z}$), and note by the multiplicativity of absolute values that I must be prime. Writing $I = (p)$ for a prime number p, we see that $|x|_v \lesseqgtr 1$ if and only if $|x|_p \lesseqgtr 1$ for all $x \in \mathbb{Q}$, which implies that $|-|_v$ is equivalent to the p-adic norm.

Now suppose $|-|_v$ is archimedean, and assume that it satisfies the triangle inequality. Given $x, y \in \mathbb{Z}$ with $x \geq 2$ and $y > 0$, we can write y in base-x as $y = \sum_{i=0}^m a_i x^i$, where $a_i \in \{0, \dots, a-1\}$ for all $i \in \{0, \dots, m\}$ and where $m \leq \log_x y$. The triangle inequality tells us that

$$|y|_v \leq (\log_x y + 1) \cdot \max\{|a_i|_v : i \in \{0, \dots, m\}\} \cdot \max\{1, |x|_v^{(\log_x y)}\}.$$

Replace y with z^n; we will apply the trick of taking n^{th} roots and sending $n \to \infty$. Doing so yields that

$$\begin{aligned} |z|_v &\leq \lim_{n \to \infty} (n \log_x z + 1)^{\frac{1}{n}} \cdot (\max\{|a_i|_v : i \in \{0, \dots, m\}\})^{\frac{1}{n}} \cdot \left(\max\{1, |x|_v^{n(\log_x z)}\}\right)^{\frac{1}{n}} \\ &= \max\{1, |x|_v^{(\log_x z)}\}. \end{aligned}$$

Since $|-|_v$ is archimedean, by Lemma 11 there exists $z \in \mathbb{Z}_{>0}$ such that $|z|_v > 1$. It follows that for any $x \in \mathbb{Z}_{\geq 2}$, we have $|x|_v^{(\log_x z)} > 1$, which implies that $|x|_v > 1$

for all $x \in \mathbb{Z}_{\geq 2}$. Thus, we have that

$$|z|_v \leq |x|_v^{(\log_x z)} \leq |z|_v^{(\log_z x)\cdot(\log_x z)} \Rightarrow |z|_v^{\frac{1}{\log z}} = |x|_v^{\frac{1}{\log x}} \Rightarrow \frac{\log |z|_v}{\log |z|_\infty} = \frac{\log |x|_v}{\log |x|_\infty}$$

for all $x, z \in \mathbb{Z}_{\geq 2}$. It then follows that $| - |_v$ is equivalent to the standard absolute value. ♠

Now that we know exactly what absolute values can be put on $\mathbb{Q}$, we can proceed to study absolute values on number fields more generally. Nevertheless, it will be fruitful to pause our discussion of number fields to address a case that we have thus far largely ignored, that of the archimedean absolute value. Following this aside, we will conclude the section by characterizing archimedean and non-archimedean absolute values on number fields.

4.1. **An Archimedean Aside.** In this subsection, we will perform a detailed study of archimedean valued fields. To begin with, we will use Theorem 35 to provide a computation of the Artin constant for any valued field; of course, this is only interesting in the archimedean case.

Theorem 36 (Artin). *Let $| - |_v$ be an absolute value on a field k. Then the Artin constant of $| - |_v$ on k is 1 if $| - |_v$ is non-archimedean and $|2|_v$ if $| - |_v$ is archimedean. In particular, if ℓ is a subfield of k, then the Artin constant of the restriction of $| - |_v$ to ℓ is the same as the Artin constant of $| - |_v$ on k.*

Proof. The second statement will follow immediately once we have proven the first statement. Notice that the first statement is obvious when $| - |_v$ is non-archimedean, because such absolute values have Artin constant 1 by definition. We may therefore restrict our consideration to the case where $| - |_v$ is archimedean. In this case, Corollary 12 tells us that k must have characteristic 0, so k contains a subfield isomorphic to $\mathbb{Q}$. Note that the restriction of $| - |_v$ to $\mathbb{Q}$ must be equivalent to the standard absolute value, since by Lemma 25 the restriction to $\mathbb{Q}$ must be archimedean and by Theorem 35 there is only one archimedean place on $\mathbb{Q}$. Thus, there exists $a > 0$ such that $| - |_v = | - |_\infty^a$ on $\mathbb{Q}$, and if $C \in \mathbb{R}_{\geq 1}$ denotes the Artin constant of $| - |_v$, there exists $b > 0$ such that $C = 2^b$. It suffices to prove that $a = b$, for then $| - |_v$ would have Artin constant $2^a = |2|_\infty^a = |2|_v$, as desired. To prove that $a = b$, we will imitate the argument used to prove Lemma 4.

For $x, y \in k$ and $x_1, \dots, x_m \in k$, the modified triangle inequality tells us that

$$|x + y|_v \leq 2^b \cdot \max\{|x|_v, |y|_v\}, \text{ and}$$
$$|x_1 + \cdots + x_m|_v \leq (2m)^b \cdot \max\{|x_i| : i \in \{1, \dots, m\}\}.$$

It follows that for any $n \in \mathbb{Z}_{\geq 0}$ we have

$$\begin{aligned}|x+y|_v^n = |(x+y)^n|_v &= \left|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\right|_v \\ &\leq (2(n+1))^b \cdot \max\left\{\left|\binom{n}{i}\right|_v \cdot |x^i|_v \cdot |y^{n-i}|_v : i \in \{0,\dots,n\}\right\} \\ &= (2(n+1))^b \cdot \max\left\{\binom{n}{i}^a \cdot |x^i|_v \cdot |y^{n-i}|_v : i \in \{0,\dots,n\}\right\} \\ &\leq (2(n+1))^b \cdot 2^{an} \cdot \big(\max\{|x|_v, |y|_v\}\big)^n,\end{aligned}$$

so taking n^{th} roots and sending $n \to \infty$ as usual tells us that $|x+y|_v \leq 2^a \cdot \max\{|x|_v, |y|_v\}$. It follows that $2^b \leq 2^a$. But $2^a = |1+1|_v \leq 2^b \cdot \max\{|1|_v, |1|_v\} = 2^b$, so $a = b$, which is the desired result. ♠

The next theorem tells us roughly that all archimedean valued fields are subfields of $\mathbb{C}$ and that the only archimedean absolute value is the standard one; our proof relies on many of the main results we have already proven, including Theorems 35 and 36:

Theorem 37 (Big Ostrowski). *Let k be a field equipped with an archimedean absolute value $|-|_v$. Then k is isomorphic to a subfield of $\mathbb{C}$, with absolute value given by the restricting the standard absolute value. In particular, if k is complete with respect to $|-|_v$, then k is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.*

Proof. Recall the setup: we have an archimedean absolute value $|-|_v$ on a field k. Theorem 24 tells us that there exists a completion $\overline{k}$ of k, so it suffices to consider the case where k is complete with respect to $|-|_v$. Now, by Corollary 12, k must have characteristic 0. Thus, k contains a subfield isomorphic to $\mathbb{Q}$, so we can think of k as being an extension of $\mathbb{Q}$.

We claim that we can replace $|-|_v$ with an equivalent absolute value that satisfies the triangle inequality and whose restriction to $\mathbb{Q}$ gives the standard absolute value. As in the proof of Theorem 36, the restriction of $|-|_v$ to $\mathbb{Q}$ must be equivalent to the standard absolute value. We may therefore replace $|-|_v$ with an equivalent absolute value whose restriction to $\mathbb{Q}$ gives the standard absolute value. By Theorem 36, we know that the Artin constant of the restriction of $|-|_v$ to $\mathbb{Q}$ is the same as the Artin constant of $|-|_v$ on k, so since the Artin constant of the standard absolute value is 2, the Artin constant of $|-|_v$ on k is also 2; it follows that $|-|_v$ satisfies the triangle inequality.

Because the completion of $\mathbb{Q}$ under the standard absolute value is $\mathbb{R}$, we see that k contains a subfield isomorphic to $\mathbb{R}$, on which the absolute value $|-|_v$ is simply the standard absolute value. Now, if k has a square root of -1 (call it i), then k contains a subfield isomorphic to $\mathbb{C}$. We claim that $|a+bi|_v = \sqrt{a^2+b^2}$

for all $a, b \in \mathbb{R}$. To prove this claim, write $a + bi = \sqrt{a^2 + b^2}(\cos\theta + i \sin\theta)$ for $\theta \in [0, 2\pi)$. Then by the triangle inequality,

$$\begin{aligned}|(a+bi)^n|_v &= (a^2+b^2)^{\frac{n}{2}} \cdot |\cos n\theta + i\sin n\theta|_v \\ &\leq (a^2+b^2)^{\frac{n}{2}} \cdot \big(|\cos n\theta| + |\sin n\theta|\big) \\ &\leq (a^2+b^2)^{\frac{n}{2}} \cdot \sqrt{2}.\end{aligned}$$

Taking n^{th} roots on both sides and taking the limit as $n \to \infty$, we find that $|a + bi|_v = \sqrt{a^2 + b^2}$. On the other hand, if k does not contain $i = \sqrt{-1}$, then we can adjoin i to k and extend the absolute value $|-|_v$ to $k(i)$ by $|a + bi|_v = \sqrt{|a|_v^2 + |b|_v^2}$ for all $a, b \in k$. It is clear that the extended valuation $|-|_v$ is in fact a valuation and that $k(i)$ is complete with respect to this valuation.

We now observe that regardless of whether k has $i = \sqrt{-1}$, it suffices to show that $k(i) \simeq \mathbb{C}$, for if $i \notin k$ then $k(i) \simeq \mathbb{C} \Rightarrow k \simeq \mathbb{R}$. Suppose we have $x \in k(i)$ such that $x \notin \mathbb{C}$. We will first show that there exists $y \in \mathbb{C}$ such that $|x-y|_v = \alpha := \inf_{z\in\mathbb{C}} |x-z|_v$. Consider the set $A = \{z \in \mathbb{C} : |z|_v \leq |x|_v + \alpha + \varepsilon\}$ for some $\varepsilon > 0$. We have that A is a closed, bounded, and nonempty subset of $\mathbb{C}$ and hence the continuous function $f(z) = |x - z|_v$ attains a minimum value at some $y \in A$, as desired. Let $r = x - y$. We then have that $r \notin \mathbb{C}$ and $\alpha = |r|_v \leq |x - (z + y)|_v = |r - z|_v$ for all $z \in \mathbb{C}$.

Let $z \in \mathbb{C}$ be arbitrary, and observe that we have the following inequalities:

$$\left(\frac{|z|_v^n}{\alpha^n} + 1\right)\alpha^n = |r|_v^n + |z|_v^n \geq |r^n - z^n|_v = \left|\prod_{i=0}^{n-1}(r - \zeta^i z)\right|_v \geq |r - z|_v \cdot \alpha^{n-1}.$$

Dividing through by α^{n-1} yields that

$$|r - z|_v \leq \alpha\left(\frac{|z|_v^n}{\alpha^n} + 1\right).$$

Suppose $|z|_v < \alpha$. Taking the limit as $n \to \infty$ of the above inequality yields that $|r - z|_v \leq \alpha \Rightarrow |r - z|_v = \alpha$. Applying the above reasoning with r replaced by $r - z$, we see that yields that for any $z' \in \mathbb{C}$ with $|z'|_v < \alpha$, we have that $|r - z - z'|_v = \alpha$. It follows by induction that $|r - mz|_v = \alpha$ if $|z|_v < \alpha$. Since every complex number can be written as an integral multiple of a number with absolute value less than α, we have that $|r - z|_v = \alpha$ for all $z \in \mathbb{C}$. But then

$$|z - z'|_v = |z - r + r - z'|_v \leq |z - r|_v + |r - z'|_v = 2\alpha$$

for all $z, z' \in \mathbb{C}$, but this is manifestly not the case, as we could take $z = (2+\varepsilon)\alpha$ and $z' = 0$ for any $\varepsilon > 0$. We have thus obtained a contradiction, so we have showed that $k(i) \subset \mathbb{C}$. It follows that $k(i) \simeq \mathbb{C}$, as desired. ♠

This section was supposed to be about number fields, so we should probably get back to studying number fields more closely. The following corollary applies a number of the results we have proven to characterizing archimedean absolute values on a number field:

Corollary 38. *Let k be a number field of degree $[k:\mathbb{Q}] = n$. Then there are at most n archimedean places on k.*

Proof. Let $|-|_v$ be an archimedean absolute value on k. Combining Lemma 25 and Theorem 35, we deduce that $|-|_v$ must restrict to an absolute value that is equivalent to the standard absolute value on $\mathbb{Q}$. By Theorem 33, there exist at most n absolute values on k that extend the standard absolute value on $\mathbb{Q}$. The corollary follows immediately. ♠

4.2. **The Non-archimedean Case.** As for non-archimedean absolute values on a number field, we can say even more. Let k be a number field, and define $\mathcal{O}'_k$ to be the intersection over all non-archimedean absolute values $|-|_v$ of the valuation rings $\mathcal{O}_v$; i.e. we have

$$\mathcal{O}'_k = \{x \in k : |x|_v \leq 1 \text{ for all non-archimedean } |-|_v\}.$$

It turns out that $\mathcal{O}'_k$ is not as strange a construct as it may seem; indeed the following theorem tells us that $\mathcal{O}'_k$ is none other than the ring of integers of k:

Theorem 39. *Let $\mathcal{O}_k$ denote the integral closure of $\mathbb{Z}$ in k. Then $\mathcal{O}_k = \mathcal{O}'_k$.*

Proof. Since by Lemma 11 $|n|_v \leq 1$ for all non-archimedean absolute values $|-|_v$ and $n \in \mathbb{Z}$, we have that $\mathbb{Z} \subset \mathcal{O}'_k$. Suppose $x \in k$ is integral over $\mathbb{Z}$ (i.e. $x \in \mathcal{O}_k$), and let $|-|_v$ be a non-archimedean absolute value on k. We have that $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ for some integers $a_i \in \mathbb{Z}$. If $|x|_v > 1$, then we have that $|a_ix^i|_v \leq |x|_v^n$ for all i, so by the ultra-metric inequality, we have that

$$0 = |x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0|_v \leq |x|_v^n > 1,$$

which is a contradiction. Thus, we must have that $|x|_v \leq 1$ for all $x \in \mathcal{O}_k$. It follows that $\mathcal{O}_k \subset \mathcal{O}'_k$.

Suppose $x \in \mathcal{O}'_k \setminus \mathcal{O}_k$. If the (unique) factorization of the fractional ideal $(x) \subset k$ into primes $\mathfrak{p}$ is given by

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}(x)},$$

for $e_{\mathfrak{p}}(x) \in \mathbb{Z}$, then we have that $e_{\mathfrak{p}_1}(x) < 0$ for some $\mathfrak{p}_1$, for otherwise $x \in \mathcal{O}_k$. Now, consider the absolute value $|-|_v$ that assigns to each $y \in k$ the number $2^{-e_{\mathfrak{p}_1}(y)}$. One can readily check that v is a non-archimedean absolute value on k, and clearly we have that $|x|_v = 2^{-e_{\mathfrak{p}_1}(x)} > 1$, which contradicts the fact that $x \in \mathcal{O}'_k$. Thus, we have that $\mathcal{O}_k \subset \mathcal{O}'_k$ and $\mathcal{O}'_k \setminus \mathcal{O}_k = \varnothing$, from which we deduce that $\mathcal{O}_k = \mathcal{O}'_k$. ♠

Of course, now that we have proven that $\mathcal{O}_k = \mathcal{O}_k'$, we may unambiguously adhere to the notation $\mathcal{O}_k$. Theorem 39 is remarkable in that it allows us to completely characterize what the non-archimedean absolute values on a number field are, as we shall now see:

Theorem 40. *The set of non-archimedean places on a number field k is in natural bijection with the set of prime ideals in its ring of integers $\mathcal{O}_k$.*

Proof. In the following proof, we shall use Theorem 39 in order to view $\mathcal{O}_k$ as both the ring of integers of k (so as to exploit unique factorization) and as the intersection of valuation rings (so as to utilize properties of absolute values).

Given a prime ideal $\mathfrak{p} \subset \mathcal{O}_k$, let $|-|_{v_\mathfrak{p}}$ be the absolute value defined by $|x|_{v_\mathfrak{p}} = 2^{-e_\mathfrak{p}(x)}$ for all $x \in k$ (one readily checks that $v_\mathfrak{p}$ is a non-archimedean absolute value on k). Given a non-archimedean place on k containing an absolute value $|-|_v$, let $\mathfrak{p}_v$ be the prime ideal of $\mathcal{O}_k$ defined by $\mathfrak{p}_v = \{x \in \mathcal{O}_k : |x|_v < 1\}$. Note that $\mathfrak{p}_v$ is prime for all $|-|_v$ because $\{x \in k : |x| < 1\}$ is prime ideal in the ring $\{x \in k : |x| \leq 1\}$.

We first show that $\mathfrak{p}_{v_\mathfrak{p}} = \mathfrak{p}$ for all prime ideals $\mathfrak{p} \subset \mathcal{O}_k$. If $x \in \mathfrak{p}$, then $e_\mathfrak{p}(x) > 0$, so $|x|_{v_\mathfrak{p}} < 1$, which implies that $x \in \mathfrak{p}_{v_\mathfrak{p}}$. On the other hand, if $x \in \mathfrak{p}_{v_\mathfrak{p}}$, then $|x|_{v_\mathfrak{p}} < 1$, which implies that $e_\mathfrak{p}(x) > 0$, so $x \in \mathfrak{p}$. It follows that $\mathfrak{p}_{v_\mathfrak{p}} = \mathfrak{p}$ for all prime ideals $\mathfrak{p} \subset \mathcal{O}_k$.

We now show that $|-|_{v_{\mathfrak{p}_v}}$ is equivalent to $|-|_v$ for all non-archimedean absolute values $|-|_v$. It suffices to show that $|-|_{v_{\mathfrak{p}_v}}$ and $|-|_v$ give rise to the same valuation ring. If $|x|_v < 1$, then $x \in \mathfrak{p}_v$, so $e_{\mathfrak{p}_v}(x) > 0$, which implies that $|x|_{v_{\mathfrak{p}_v}} < 1$. On the other hand, if $|x|_{v_{\mathfrak{p}_v}} < 1$, then $e_{\mathfrak{p}_v}(x) > 0$, which implies that $x \in \mathfrak{p}_v$, so $|x|_v < 1$. It now remains to show that $|x|_v = 1$ if and only if $|x|_{v_{\mathfrak{p}_v}} = 1$. If $|x|_v = 1$ and $|x|_{v_{\mathfrak{p}_v}} > 1$, then $|1/x|_{v_{\mathfrak{p}_v}} < 1$, implying that $|1/x|_v < 1$, which is a contradiction, so $|x|_{v_{\mathfrak{p}_v}} = 1$. On the other hand if $|x|_{v_{\mathfrak{p}_v}} = 1$ and $|x|_v > 1$, then $|1/x|_v < 1$, so we have that $|1/x|_{v_{\mathfrak{p}_v}} < 1$, a contradiction implying that $|x|_v = 1$. It follows that $|-|_v$ is equivalent to $|-|_{v_{\mathfrak{p}_v}}$. ♠

Remark. From the proof of Theorem 40, we see that the non-archimedean places on a number field are represented by what one might call the $\mathfrak{p}$-adic absolute values $|-|_{v_\mathfrak{p}}$, which are the natural analogues of the p-adic absolute values on $\mathbb{Q}$. In this light, Theorem 40, along with Corollary 38, may be viewed as a Little Ostrowski Theorem for number fields. Note that the $\mathfrak{p}$-adic absolute values are all discrete and give finite residue fields.

Corollary 41. *Let k be a number field, and take $\alpha \in k^\times$. Then there exist only finitely many places containing an absolute value $|-|_v$ such that $|\alpha|_v \neq 1$.*

Proof. By Corollary 38, there are only finitely many archimedean places on k, so we can ignore them. As for the non-archimedean places, it follows from Theorem 40 that the only non-archimedean absolute values $|-|_v$ with $|\alpha|_v \neq 1$

belong to the places of the $\mathfrak{p}$-adic absolute values for the finitely many prime factors $\mathfrak{p}$ of the ideal (α). Hence, the corollary. ♠

Corollary 41 establishes a property that holds for all but finitely many absolute values on a given number field. In accordance with the jargon of the subject, we shall use the phrase "almost all" to mean "all but finitely many" throughout the remainder of this article.

5. A Glimpse of Class Field Theory

In this section, we will introduce the tools necessary to define adeles and ideles, which were introduced by French mathematician Claude Chevalley as a means of systematizing class field theory, the subdiscipline of mathematics concerned with studying abelian extensions of number fields. We will then use the language of adeles and ideles to give a proof of Dirichlet's Unit Theorem.

5.1. Restricted Topological Products.

The primary tool we shall require to define adeles and ideles is the restricted topological product, which is defined as follows:

Definition 42. Let $\{X_\lambda\}_{\lambda\in\Lambda}$ be a collection of topological spaces indexed by Λ, and take open subsets $U_\lambda \subset X_\lambda$ for almost all $\lambda \in \Lambda$. As a set, the restricted topological product X of the X_λ's with respect to the U_λ's is the subset of $\prod_{\lambda\in\Lambda} X_\lambda$ given by sequences $\{\sigma_\lambda\}_{\lambda\in\Lambda}$ satisfying $\sigma_\lambda \in X_\lambda$ for all $\lambda \in \Lambda$ and $\sigma_\lambda \in U_\lambda$ for almost all $\lambda \in \Lambda$. The topology endowed upon X has, as a basis of open sets, the products $\prod_{\lambda\in\Lambda} V_\lambda$, where $V_\lambda \subset X_\lambda$ is open for all $\lambda \in \Lambda$ and $V_\lambda = U_\lambda$ for almost all $\lambda \in \Lambda$.

Observe that the restricted product X remains unaltered if we replace finitely many of the U_λ's with open subsets $U'_\lambda \subset U_\lambda$. Moreover, if $S \subset \Lambda$ is any finite set such that U_λ is defined for all $\lambda \in \Lambda \setminus S$ (we shall call such sets S "good"), then setting $X_S = \prod_{\lambda\in S} X_\lambda \times \prod_{\lambda\in\Lambda\setminus S} U_\lambda \subset X$, we have that $X_S \subset X$ is open, and the subspace topology on X_S induced by X is none other than the product topology. Moreover, the subspaces X_S, where $S \subset \Lambda$ ranges over all good sets, form an open cover of X.

The case that will be of primary interest to us is where the spaces X_λ's are locally compact topological rings and the subspaces U_λ's are compact open subrings. The next lemma sheds some light on what happens, topologically speaking, in this situation:

Lemma 43. *We have the following (unrelated) properties:*

(1) As before, let X be the restricted topological product of locally compact topological spaces X_λ with respect to compact open subsets U_λ. Then X_S is locally compact for any good set $S \subset \Lambda$, so X is also locally compact.

(2) *Suppose that the X_λ's are topological rings and that the U_λ's are subrings. Then X is also a topological ring.*

Proof. For the first statement, that X_S is locally compact for any good set $S \subset \Lambda$ follows immediately from our earlier observation that the subspace topology on X_S is just the product topology. Since the sets X_S form a cover of X, we deduce that X is itself locally compact.

For the second statement, we give X the structure of topological ring in the obvious way by defining the operations of addition and multiplication componentwise. To check continuity of the ring operations, we may pass to a particular open subset X_S, where continuity is clear because X_S is a product of topological rings and bears the product topology. ♠

It may now be somewhat apparent what we intend to do with these restricted topological products. Essentially, we want to take a number field, look at its completions with respect to the absolute values that we can put on it, and construct a restricted topological product out of them. The completions arising from archimedean absolute values are necessarily either $\mathbb{R}$ or $\mathbb{C}$, which are locally compact; the completions arising from non-archimedean ($\mathfrak{p}$-adic) absolute values, all of which are discrete and give finite residue fields, are also locally compact with compact open valuation rings by Proposition 27. But since equivalent absolute values give the same completions, we only want one representative from each place to incorporate into our restricted topological product. In order to specify a distinguished absolute value from each place, we introduce the following definition:

Definition 44. Let $|-|_v$ be an absolute value on a number field k. We say that $|-|_v$ is normalized if:

(1) When $|-|_v$ is archimedean and the completion of k with respect to $|-|_v$ is $\mathbb{R}$, we have $|-|_v = |-|_\infty$.
(2) When $|-|_v$ is archimedean and the completion of k with respect to $|-|_v$ is $\mathbb{C}$, we have $|-|_v = |-|_\infty^2$.
(3) When $|-|_v$ is discrete and non-archimedean with finite residue field, we have $|\pi_v|_v = 1/\#(\kappa_v)$, where π_v is a uniformizer. (Note that $|-|_v$ is specified entirely by its value on π_v.)

Remark. The motivation for the choice of representative made in Definition 44 stems from the theory of Haar measures on locally compact topological groups. We omit a discussion of this subject because, with the exception of Theorem 58, it is not necessary to understand the balance of the present article. For more details on the Haar measure, one could refer to [1].

Example 45. We can now see why we defined the p-adic norm as we did in Definition 6. Notice that $|p|_p = 1/p = 1/\#(\mathbb{F}_p)$, so in fact the p-adic norm was chosen from its place of equivalent absolute values to be the normalized one. ♣

We shall now investigate how normalized absolute values play with finite extensions. The next lemma tells us what happens in the case when our base field k is complete:

Lemma 46. *Retain the setting of Corollary 31, and suppose $|-|_v$ is a normalized absolute value. The normalized absolute value $|-|_{\widetilde{v}}$ on ℓ whose restriction to k belongs to the place of $|-|_v$ is given by $|-|_{\widetilde{v}} = |\operatorname{Nm}_{\ell/k}(x)|_v$.*

Proof. By Corollary 31, we know that $|-|_{\widetilde{v}} = |\operatorname{Nm}_{\ell/k}(x)|_v^m$ for some $m \in \mathbb{R}_{>0}$, so we need only show that $m = 1$. In the archimedean case, this is obvious: the only nontrivial situation is when $k = \mathbb{R}$ and $\ell = \mathbb{C}$, but then $\operatorname{Nm}_{\ell/k}(x) = |x|_\infty^2$, as desired. Now suppose $|-|_v$ is discrete and non-archimedean with finite residue field κ_v. We claim that $|-|_{\widetilde{v}}$ is also discrete and non-archimedean with finite residue field $\kappa_{\widetilde{v}}$. The only tricky property to check here is that $\kappa_{\widetilde{v}}$ is finite, but this follows from the fact that a finite-dimensional normed vector space over a local field is locally compact.

Let π_v be a uniformizer for $|-|_v$, and let $\pi_{\widetilde{v}}$ be a uniformizer for $|-|_{\widetilde{v}}$. Then there exists a unit $u \in \ell$ and an integer e such that $\pi_v = u \cdot \pi_{\widetilde{v}}^e$, implying that $|\pi_v|_{\widetilde{v}} = 1/\#(\kappa_{\widetilde{v}})^e$; note that $e > 0$ because $|-|_{\widetilde{v}}$ is equivalent to an extension of $|-|_v$. But we also know that $|\pi_v|_{\widetilde{v}} = |\operatorname{Nm}_{\ell/k}(\pi_v)|_v^m = |\pi_v^n|_v^m = 1/\#(\kappa_v)^{mn}$, so to prove the corollary it suffices to show that $[\kappa_{\widetilde{v}} : \kappa_v] = n/e$. The proof of this is somewhat involved and extraneous to the development of the present article; we refer the reader to [1] or [4]. ♠

We can use Lemma 46 to prove the following product formula for number fields, which will come handy in the next subsection:

Theorem 47 (Product Formula)**.** *Let k be a number field, and take $x \in k^\times$. Let Λ_k denote the set of all nontrivial normalized absolute values on k. Then $\prod_{\lambda \in \Lambda_k} |x|_\lambda = 1$.*

Proof. The product formula clearly holds when $k = \mathbb{Q}$. Indeed, by Example 45, the normalized non-archimedean absolute values are just the p-adic norms, so the product over non-archimedean absolute values gives a factor of $1/x$, and the single archimedean absolute value gives a factor of x. Now suppose k is a finite extension of $\mathbb{Q}$. We write $\lambda \mid \mu$ for absolute values $|-|_\lambda$ on k and μ on $\mathbb{Q}$ if the restriction of λ to $\mathbb{Q}$ is given by μ. Furthermore, let k_λ be the completion of k with respect to $|-|_\lambda$ and $\mathbb{Q}_\mu$ be the completion of $\mathbb{Q}$ with respect to $|-|_\mu$. With this notation, we have the following:

$$\prod_{\lambda \in \Lambda_k} |x|_\lambda = \prod_{\mu \in \Lambda_{\mathbb{Q}}} \prod_{\substack{\lambda \in \Lambda_k \\ \lambda \mid \mu}} |x|_\lambda = \prod_{\mu \in \Lambda_{\mathbb{Q}}} \prod_{\substack{\lambda \in \Lambda_k \\ \lambda \mid \mu}} |\operatorname{Nm}_{k_\lambda/\mathbb{Q}_\mu}(x)|_\mu = \prod_{\mu \in \Lambda_{\mathbb{Q}}} |\operatorname{Nm}_{k/\mathbb{Q}}(x)|_\mu = 1,$$

where the second equality is Lemma 46 and the third equality is Corollary 34. Thus, we have the theorem. ♠

Finally, the following theorem will also be very useful in the next subsection:

Theorem 48. *Let $k \hookrightarrow \ell$ be a finite extension of number fields having degree $[\ell : k] = n$. For a normalized absolute value $|-|_v$ on k, let the extensions of $|-|_v$ to ℓ be denoted by $|-|_{v_1}, \dots, |-|_{v_N}$ (by Theorem 33, $N \leq n$). Furthermore, let $\overline{k}$ denote the completion of k with respect to $|-|_v$, and let ℓ_{v_i} denote the completion of ℓ with respect to $|-|_{v_i}$ for each $i \in \{1, \dots, N\}$. If $(\omega_1, \dots, \omega_n)$ is a basis of ℓ as a k-vector space, then for almost all choices of the normalized absolute value $|-|_v$, we have*

$$\bigoplus_{i=1}^{n} \omega_i \mathcal{O}_v \simeq \bigoplus_{i=1}^{N} \mathcal{O}_{v_i}, \tag{5}$$

where $\mathcal{O}_v$ is the valuation ring associated to the completion $\overline{k}$ and where the identification given by the isomorphism from Theorem 33.

Remark. The following proof requires an understanding of discriminants; see [5] for the related definitions and properties.

Proof. By Corollary 41, for almost all $|-|_v$ we have $|\omega_i|_{v_j} \leq 1$ for all $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, N\}$. Thus, for almost all $|-|_v$, the left-hand-side of (5) includes via the isomorphism of Theorem 33 into the right-hand-side. For the reverse inclusion, it suffices to work with the elements of the right-hand-side coming from ℓ (via the diagonal embedding), because they are dense by Theorem 26. Given $a = \sum_{i=1}^n c_i \omega_i \in \ell \cap \bigoplus_{i=1}^N \mathcal{O}_{v_i}$ with $c_i \in k$ for all $i \in \{1, \dots, n\}$, the discriminant $\operatorname{disc}(\omega_1, \dots, \omega_{m-1}, a, \omega_{m+1}, \dots, \omega_n)$ is an element of $\mathcal{O}_v$ for almost all $|-|_v$, because ω_i is integral over $\mathcal{O}_v$ for almost all $|-|_v$. Moreover, we have that

$$\operatorname{disc}(\omega_1, \dots, \omega_{m-1}, a, \omega_{m+1}, \dots, \omega_n) = c_m^2 \cdot \operatorname{disc}(\omega_1, \dots, \omega_n).$$

Notice that for almost all $|-|_v$ we have $\operatorname{disc}(\omega_1, \dots, \omega_n) \in \mathcal{O}_v^\times$; combining this result with the above equality yields that $c_m \in \mathcal{O}_v$ for all $m \in \{1, \dots, n\}$. It follows that the right-hand-side of (5) is included in the left-hand-side via the isomorphism of Theorem 33. ♠

5.2. **Adeles and Ideles.** We may now define the adele ring associated to a number field. Let k be a number field, and let Λ_k be the set of nontrivial normalized absolute values on k. Further, let k_λ denote the completion of k with respect to the absolute value $|-|_\lambda$ for each $\lambda \in \Lambda_k$. Notice that we have the open subset $\mathcal{O}_\lambda \subset k_\lambda$ whenever $|-|_\lambda$ is non-archimedean and that by Corollary 38 there are only finitely many archimedean absolute values in Λ. This leads us to the following definition:

Definition 49. The adele ring $\mathbb{A}_k$ associated to k is the restricted topological product of the k_λ's with respect to the $\mathcal{O}_\lambda$'s. The elements of $\mathbb{A}_k$ are known simply as adeles.

To illustrate what an adele ring might look like, we provide the following example, to which will we later return:

Example 50. The adele ring $\mathbb{A}_{\mathbb{Q}}$ of the field $\mathbb{Q}$ of rational numbers is the restricted topological product of $\mathbb{R}$ and the the fields $\mathbb{Q}_p$ of p-adic numbers with respect to all of the $\mathbb{Z}_{(p)}$'s. It is the set of sequences $(x_\infty, x_2, x_3, x_5, \dots, x_p, \dots)$ such that $x_\infty \in \mathbb{R}$, $x_p \in \mathbb{Q}_p$ for all p, and $x_p \in \mathbb{Z}_{(p)}$ for almost all p. ♣

By Lemma 46, $\mathbb{A}_k$ is a locally compact topological ring with componentwise operations of addition and multiplication. Observe that $\mathbb{A}_k$ also has the structure of k-vector space; indeed, if we multiply each component of an adele $\{x_\lambda\}_{\lambda \in \Lambda_k}$ by a constant $c \in k$, we know by Corollary 41 that $|c|_\lambda = 1$ for all but finitely many $\lambda \in \Lambda_k$, so all but finitely many of the cx_λ's will be elements of the $\mathcal{O}_\lambda$'s.

With our understanding (Theorems 33 and 48) of how normalized absolute values play with finite extensions, we should be able to determine the adele ring of a finite field extension from the adele ring of the base field. The next lemma tells us that to do so, we simply need to extend scalars from k to ℓ:

Lemma 51. *Let $k \hookrightarrow \ell$ be a finite extension of number fields. Then we have $\mathbb{A}_\ell \simeq \mathbb{A}_k \otimes_k \ell$.*

Proof. We retain the notation employed in Theorem 48. Let $[\ell : k] = n$, and take a basis $(\omega_1, \dots, \omega_n)$ of ℓ as a k-vector space. By Theorems 33 and 48, we have the following commutative diagram for almost all λ:

$$\begin{tikzcd}
\bigoplus_{i=1}^n \omega_i k_\lambda \arrow[r, "\sim"] & k_\lambda \otimes_k \ell \arrow[r, "\sim"] & \bigoplus_{i=1}^N \ell_{\lambda_i} \\
\bigoplus_{i=1}^n \omega_i \mathcal{O}_\lambda \arrow[u, hook] \arrow[rr, "\sim"'] & & \bigoplus_{i=1}^N \mathcal{O}_{\lambda_i} \arrow[u, hook]
\end{tikzcd}$$

Taking the restricted topological product along the left-hand-side yields $\mathbb{A}_k \otimes_k \ell$, and taking the restricted topological product along the right-hand-side yields $\mathbb{A}_\ell$. The desired isomorphism follows. ♠

Remark. It follows from Lemma 51 that the additive group $\mathbb{A}_\ell^+$ is simply the direct sum of N copies of the additive group $\mathbb{A}_k^+$.

Notice that the base field k embeds diagonally as constant sequences into the adele ring $\mathbb{A}_k$ via the map $x \mapsto \{x\}_{\lambda \in \Lambda}$ (we shall denote this adele simply by x for ease of notation), which is well-defined by Corollary 41; such adeles are called principal and form a subring, and k-vector subspace, of $\mathbb{A}_k$. This diagonal embedding is compatible with the isomorphism given in Lemma 51, in the sense that we have the following commutative square:

$$\begin{tikzcd}
k \otimes_k \ell \arrow[r, hook] & \mathbb{A}_k \otimes_k \ell \\
\ell \arrow[r, hook] \arrow[u, "\wr"] & \mathbb{A}_\ell \arrow[u, "\wr"']
\end{tikzcd}$$

The next theorem tells us, among other things, about the topology of k, viewed as a subspace of the adele ring $\mathbb{A}_k$:

Theorem 52. *The subspace topology on k induced by the topology on $\mathbb{A}_k$ is discrete. Moreover, $\mathbb{A}_k^+/k^+$ is compact.*

Proof. We claim that it suffices to consider the case where $k = \mathbb{Q}$. Indeed, by looking at the commutative square above, we see that ℓ and $\mathbb{A}_\ell$ are direct sums of copies of k and $\mathbb{A}_k$, respectively, so proving that k is discrete in $\mathbb{A}_k$ and that $\mathbb{A}_k^+/k^+$ is compact automatically gives us the analogous results for ℓ and $\mathbb{A}_\ell$.

To show that $\mathbb{Q}$ is discrete in $\mathbb{A}_\mathbb{Q}$, it suffices to find an open set $U \subset \mathbb{A}_\mathbb{Q}$ such that $U \cap \mathbb{Q} = \{0\}$. We shall take U to be defined by

$$U = \{\{x_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} \in \mathbb{A}_\mathbb{Q} : |x_\infty|_\infty < 1 \text{ and } |x_p|_p \leq 1 \text{ for all } p\}.$$

It is clear that $0 \in U$. Moreover, if $x \in U \cap \mathbb{Q}$, then the condition that $|x|_p \leq 1$ for all p implies that $x \in \mathbb{Z}$, and the condition that $|x|_\infty < 1$ further implies that $x = 0$. Thus, $U \cap \mathbb{Q} = \{0\}$, as desired.

To show that $\mathbb{A}_\mathbb{Q}^+/\mathbb{Q}^+$ is compact, it suffices to construct a compact set $V \subset \mathbb{A}_\mathbb{Q}$ such that the composite map $V \hookrightarrow \mathbb{A}_\mathbb{Q}^+ \twoheadrightarrow \mathbb{A}_\mathbb{Q}^+/\mathbb{Q}^+$ is surjective. We shall take V to be defined by

$$V = \{\{x_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} \in \mathbb{A}_\mathbb{Q} : |x_\infty|_\infty \leq 1/2 \text{ and } |x_p|_p \leq 1 \text{ for all } p\}.$$

That V is compact is clear, since it is the product of compact sets. It remains to show that V maps surjectively onto $\mathbb{A}_\mathbb{Q}^+/\mathbb{Q}^+$, for which we will show that every adele $\{x_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} \in \mathbb{A}_\mathbb{Q}$ can be expressed as $\{x_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} = y + \{z_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}}$, where $y \in \mathbb{Q}$ and $\{z_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} \in V$. Note that $|x_p|_p \leq 1$ for almost all p by the definition of an adele. For the finitely many other primes p, let the fractional part of x_p be denoted by $b_p = a_p/p^{n_p}$, where $y_p \in \mathbb{Z}$ and $n_p \in \mathbb{Z}_{>0}$. Because $|b_p|_q \leq 1$ for all primes $q \neq p$, we have that $y' = \sum b_p \in \mathbb{Q}$ satisfies $|x_p - y'|_p \leq 1$ for all primes p. We may then adjust y' by an integer to obtain $y \in \mathbb{Q}$ so that $|x_\infty - y|_\infty \leq 1/2$ and $|x_p - y|_p \leq 1$ for all primes p. It follows that $\{x_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} = y + \{z_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}}$, where $y \in \mathbb{Q}$ and $\{z_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} = \{x_\lambda\}_{\lambda \in \Lambda_\mathbb{Q}} - y \in V$, which is the desired result. ♠

We have said a fair bit about the additive structure of the adele ring, so we will now turn our attention to studying its multiplicative structure. To begin with, the group of units in the adele ring are given a special name:

Definition 53. The idele group $\mathbb{A}_k^\times$ associated to k is the group of units in $\mathbb{A}_k$; i.e. we have

$$\mathbb{A}_k^\times = \{\{x_\lambda\}_{\lambda \in \Lambda_k} \in \mathbb{A}_k : x_\lambda \in k_\lambda^\times \text{ and } x_\lambda \in \mathcal{O}_\lambda^\times \text{ for almost all } \lambda \in \Lambda_k\}.$$

The elements of $\mathbb{A}_k^\times$ are known simply as ideles.

At first glance, one might suppose it appropriate to endow the idele group $\mathbb{A}_k^\times$ with the subspace topology induced by $\mathbb{A}_k$, but this choice of topology is problematic: indeed, the inversion map $x \mapsto 1/x$ fails to be continuous in this topology. In order to correct for this issue, we shall regard $\mathbb{A}_k^\times$ as a subset of $\mathbb{A}_k \times \mathbb{A}_k$ via the embedding $x \mapsto (x, 1/x)$, and we shall give $\mathbb{A}_k^\times$ the subspace topology induced by the product topology on $\mathbb{A}_k \times \mathbb{A}_k$. One readily checks that the multiplication and inversion operations, as well as the inclusion map $\mathbb{A}_k^\times \hookrightarrow \mathbb{A}_k$, are continuous with respect to this topology.

Since the adele ring was defined as a restricted topological product and was topologized accordingly, it is natural to ask whether something similar can be said about the idele group. The next lemma answers this question in the affirmative:

Lemma 54. *As a topological group, the idele group $\mathbb{A}_k^\times$ is the restricted topological product of the $k_\lambda^\times$'s with respect to the $\mathcal{O}_\lambda^\times$'s.*

Proof. We will first specify the desired map $f : \mathbb{A}_k^\times \to R$, where R is the restricted topological product of the $k_\lambda^\times$ with respect to the $\mathcal{O}_\lambda^\times$. The map f will evidently be a bijective map of sets, and R will thus inherit a group structure from $\mathbb{A}_k^\times$ so that f, f^{-1} are both homomorphisms of groups. Finally, we will show that f is both open and continuous.

Take $\{x_\lambda\}_{\lambda \in \Lambda_k} \in \mathbb{A}_k^\times$, and let f be the map that sends this idele to the element $\{x_\lambda\}_{\lambda \in \Lambda_k}$ of R. Clearly, f is a well-defined map of sets $f : \mathbb{A}_k^\times \to R$, and it is obviously a bijection, for the inverse map takes $\{x_\lambda\}_{\lambda \in \Lambda_k} \in R$ back to $\{x_\lambda\}_{\lambda \in \Lambda_k} \in \mathbb{A}_k^\times$. For $\{\alpha_\lambda\}_{\lambda \in \Lambda_k}, \{\beta_\lambda\}_{\lambda \in \Lambda_k} \in R$, we take $\{\alpha_\lambda\}_{\lambda \in \Lambda_k} \cdot \{\beta_\lambda\}_{\lambda \in \Lambda_k} = \{\alpha_\lambda \beta_\lambda\}_{\lambda \in \Lambda_k} \in R$, and this defines a group law on R whose identity element is $\{1\}_{\lambda \in \Lambda_k}$. It is then evident that the maps f, f^{-1} are compatible with the group structures on $\mathbb{A}_k^\times$ and R.

Recall that we have an embedding $\mathbb{A}_k^\times \hookrightarrow \mathbb{A}_k \times \mathbb{A}_k$ given by the map $\{x_\lambda\}_{\lambda \in \Lambda_k} \mapsto \big(\{x_\lambda\}_{\lambda \in \Lambda_k}, \{1/x_\lambda\}_{\lambda \in \Lambda_k}\big)$. The topology on $\mathbb{A}_k^\times$ is the corresponding subset topology on the product topology on $\mathbb{A}_k \times \mathbb{A}_k$. Thus, the open subsets $W \subset \mathbb{A}_k^\times$ satisfying $W = \{\{x_\lambda\}_{\lambda \in \Lambda_k} \in U \cap \mathbb{A}_k^\times : \{1/x_\lambda\}_{\lambda \in \Lambda_k} \in V\}$, for open subsets $U, V \subset \mathbb{A}_k$ in the basis of the topology on $\mathbb{A}_k$, form a basis of the topology on $\mathbb{A}_k^\times$.

To show that f is open, it suffices to show that $f(W)$ is open for all such W. So pick such a W, and let its corresponding sets $U, V \subset \mathbb{A}_k$ be given by

$$U = \prod_{\lambda \notin S} \mathcal{O}_\lambda \times \prod_{\lambda \in S} U_\lambda \text{ and } V = \prod_{\lambda \notin S} \mathcal{O}_\lambda \times \prod_{\lambda \in S} V_\lambda,$$

where $S \subset \Lambda_k$ is a finite set, and $U_\lambda, V_\lambda \subset k_\lambda$ are open subsets for all $\lambda \in S$. Now, taking $g_\lambda : k_\lambda^\times \to k_\lambda^\times$ to be the continuous function defined by $g_\lambda(x) = 1/x$, notice that we have the equality

$$W = \prod_{\lambda \notin S} \mathcal{O}_\lambda^\times \times \prod_{\lambda \in S} U_\lambda \cap g_\lambda^{-1}(V_\lambda) \cap k^\times.$$

It is now evident that $f(W)$ is open, because $g_\lambda^{-1}(V_\lambda)$ is open for all $\lambda \in S$.

To show that f is continuous, it suffices to show that $f^{-1}(U)$ is open for all open sets U in a basis of the topology on R. By the definition of the restricted product, we can take

$$U = \prod_{\lambda \notin S} \mathcal{O}_\lambda^\times \times \prod_{\lambda \in S} U_\lambda,$$

where $S \subset \Lambda_k$ is a finite set, and $U_\lambda \subset k_\lambda^\times$ is an open subset for all $\lambda \in S$. Indeed, we have that $f^{-1}(U) = \mathbb{A}_k^\times \cap (V \times W)$, where $V, W \subset \mathbb{A}_k$ are open subsets defined as follows:

$$V = \prod_{\lambda \notin S} \mathcal{O}_\lambda \times \prod_{\lambda \in S} U_\lambda \cup \{0\} \text{ and } W = \prod_{\lambda \notin S} \mathcal{O}_\lambda \times \prod_{\lambda \in S} k_\lambda.$$

We have thus shown that $f^{-1}(U)$ is open in the idele topology, so f is continuous, which is the desired result. ♠

From the embedding $k \hookrightarrow \mathbb{A}_k$ it is easy to see that we obtain an embedding $k^\times \hookrightarrow \mathbb{A}_k^\times$. Furthermore, $k^\times$ is in fact discrete in $\mathbb{A}_k^\times$, because the composite map $k^\times \hookrightarrow \mathbb{A}_k^\times \hookrightarrow \mathbb{A}_k \times \mathbb{A}_k$ embeds $k^\times$ as a discrete subset of $\mathbb{A}_k^\times \times \mathbb{A}_k^\times$ by Theorem 52.

Recall from Theorem 47 that we obtain the value 1 when we take the product over all normalized absolute values of the absolute value of a particular element. One can perform a similar operation on an idele, as we will now demonstrate:

Definition 55. The content map $c : \mathbb{A}_k^\times \to \mathbb{R}_{>0}$ sends $\{x_\lambda\}_{\lambda \in \Lambda_k} \in \mathbb{A}_k^\times$ to $\prod_{\lambda \in \Lambda_k} |x_\lambda|_\lambda$.

Note that the content map is well-defined because for almost all $\lambda \in \Lambda_k$ we have $|x_\lambda|_\lambda = 1$ by the definition of an idele; it is also clearly a homomorphism of multiplicative groups, and the presence of archimedean absolute values ensures that it is surjective. We now show that the content map is well-behaved topologically:

Lemma 56. *The content map $c : \mathbb{A}_k^\times \to \mathbb{R}_{>0}$ is continuous.*

Proof. To show that c is continuous, it suffices to show that the preimage of any open interval $(a, b) \subset \mathbb{R}_{>0}$ is open. So pick $(a, b) \subset \mathbb{R}_{>0}$, and let $\{x_\lambda\}_{\lambda \in \Lambda_k} \in \mathbb{A}_k^\times$ such that $c(\{x_\lambda\}_{\lambda \in \Lambda_k}) \in (a, b)$. Let $S \subset \Lambda_k$ be the finite set for which $x_\lambda \notin \mathcal{O}_\lambda^\times$. Choose small intervals $I_\lambda \subset \mathbb{R}$ for each $\lambda \in S$ such that $|x_\lambda|_\lambda \in I_\lambda$ and $\{\prod_\lambda x_\lambda : x_\lambda \in I_\lambda\} \subset (a, b)$, and for each such $\lambda \in S$, let $U_\lambda \subset k_\lambda^\times$ be the open subset of

k_λ whose image under the absolute value $|-|_\lambda$ is I_λ (notice that the U_λ's are open because absolute values are continuous). Then the open set

$$U = \prod_{\lambda \notin S} \mathcal{O}_\lambda^\times \times \prod_{\lambda \in S} U_v$$

is an open neighborhood of $\{x_\lambda\}_{\lambda\in\Lambda_k}$ whose image under c lies within (a,b). It follows that $c^{-1}((a,b))$ is open in $\mathbb{A}_k^\times$, so c is continuous. ♠

The ideles with content equal to 1 form the kernel of the content map and are of particular importance to the theory. We shall denote by $\mathbb{A}_k^1 \subset \mathbb{A}_k^\times$ the subgroup of content-1 ideles; Theorem 47 tells us that $k^\times \subset \mathbb{A}_k^1$. The space $\mathbb{A}_k^1$ sits as a subspace of both the adele ring $\mathbb{A}_k$ and the idele group $\mathbb{A}_k^\times$, so it is natural to try and compare the topologies inherited by $\mathbb{A}_k^1$ from $\mathbb{A}_k$ and $\mathbb{A}_k^\times$. The next lemma tells us that they are one and the same:

Lemma 57. *The subspace topology on $\mathbb{A}_k^1$ induced by the topology on $\mathbb{A}_k$ is the same as that induced by the topology on $\mathbb{A}_k^\times$.*

Proof. Take a content-1 idele $\{x_\lambda\}_{\lambda\in\Lambda_k} \in \mathbb{A}_k^1$, choose a finite set $S \subset \Lambda_k$ containing all of the archimedean absolute values and those absolute values $|-|_v$ for which $|x_v|_v \neq 1$, and let $\varepsilon > 0$. Let $U \subset \mathbb{A}_k$ be the open set defined by

$$U = \{\{y_\lambda\}_{\lambda\in\Lambda_k} \in \mathbb{A}_k : |y_\lambda - x_\lambda|_\lambda < \varepsilon \text{ for } \lambda \in S \text{ and } |y_\lambda|_\lambda \le 1 \text{ for } \lambda \in \Lambda_k \setminus S\},$$

and let $U' \subset \mathbb{A}_k^\times$ be the open set defined by

$$U' = \{\{y_\lambda\}_{\lambda\in\Lambda_k} \in \mathbb{A}_k^\times : |y_\lambda - x_\lambda|_\lambda < \varepsilon \text{ for } \lambda \in S \text{ and } |y_\lambda|_\lambda = 1 \text{ for } \lambda \in \Lambda_k \setminus S\}.$$

Then $U \cap \mathbb{A}_k^1 = U' \cap \mathbb{A}_k^1$ for sufficiently small ε, and this yields the lemma. ♠

Just as we showed that $\mathbb{A}_k^+/k^+$ is compact in Theorem 52, we can ask whether something similar holds for $\mathbb{A}_k^1/k^\times$. The following theorem gives an answer to this question:

Theorem 58. *We have that $\mathbb{A}_k^1/k^\times$ is compact.*

Proof. We can use the same general strategy used to prove Theorem 52. We want to find a compact set $W \subset \mathbb{A}_k$ such that $W \cap \mathbb{A}_k^1$ maps surjectively onto $\mathbb{A}_k^1/k^\times$ (note that we are using Lemma 57 here). Using the theory of Haar measures, one can show that there exists a constant $C \in \mathbb{R}_{>0}$ such that for any adele $\{x_\lambda\}_{\lambda\in\Lambda_k}$ with $\prod_{\lambda\in\Lambda_k} |x_\lambda|_\lambda > C$, there exists a principal adele $a \in k^\times$ with $|a|_\lambda \le |x_\lambda|_\lambda$ for all $\lambda \in \Lambda_k$. We take W to be the set of adeles $\{z_\lambda\}_{\lambda\in\Lambda_k} \in \mathbb{A}_k$ with $|x_\lambda|_\lambda \le |x_\lambda|_\lambda$ for all $\lambda \in \Lambda_k$. For any content-1 idele $\{y_\lambda\}_{\lambda\in\Lambda_k} \in \mathbb{A}_k^1$, there exists $a \in k^\times$ with $|a|_\lambda \le |y_\lambda^{-1} x_\lambda|_\lambda$ for all $\lambda \in \Lambda_k$. Then $|a y_\lambda|_\lambda \le |x_\lambda|_\lambda$ for all $\lambda \in \Lambda_k$, so $\{a\}_{\lambda\in\Lambda_k} \cdot \{y_\lambda\}_{\lambda\in\Lambda_k} \in W$, implying that the map $W \cap \mathbb{A}_k^1 \to \mathbb{A}_k^1/k^\times$ is surjective, as desired. ♠

To conclude this subsection, we will apply the above-developed theory to prove the finiteness of the ideal class group. We start with the definition of the ideal group:

Definition 59. Let k be a number field. The ideal group I_k associated to k is the free abelian group on the set of normalized non-archimedean absolute values on k, and it bears the discrete topology.

We should justify why it makes sense to call I_k the ideal group, for it is not immediately clear what it has to do with ideals. But notice that we have a bijective correspondence between the ideal group I_k introduced in Definition 59 and the group of nonzero fractional ideals of $\mathcal{O}_k$ which pairs an absolute value $|-|_\lambda$ with the ideal $\mathfrak{p}_\lambda \cap \mathcal{O}_k$. We also want to relate I_k to the theory of adeles and ideles; to do so, notice further that we have a continuous map $\pi : \mathbb{A}_k^\times \to I_k$ sending an idele $\{x_\lambda\}_{\lambda \in \Lambda_k} \in \mathbb{A}_k^\times$ to $\sum_{\lambda \in \Lambda_k} \operatorname{ord}_\lambda(x_\lambda) \cdot \lambda$, where $\operatorname{ord}_\lambda(x_\lambda) = -\log_2 |x_\lambda|_{v_{\mathfrak{p}_\lambda}}$ (see the proof of Theorem 40 for the notation). The image of $k^\times$ under π clearly corresponds to the principal fractional ideals of $\mathcal{O}_k$, so we make the following definition:

Definition 60. Let k be a number field. The principal ideal group P_k associated to k is the subgroup of I_k given by $\pi(k^\times)$. The ideal class group is I_k/P_k.

We can now prove that the ideal class group is finite:

Theorem 61. *Let k be a number field. The ideal class group I_k/P_k is finite.*

Proof. The map π restricted to $\mathbb{A}_k^1$ surjects onto I_k because of the archimedean place. Thus, the induced map $\mathbb{A}_k^1/k^\times \to I_k/P_k$ is surjective, so by Theorem 58, we have that I_k/P_k is compact. But I_k/P_k has the discrete topology and must be finite as it is both compact and discrete. ♠

5.3. **Dirichlet's Unit Theorem.** In this final subsection, we shall introduce the setting for and provide a proof of Dirichlet's Unit Theorem, which was first proven by the German mathematician Peter Dirichlet and later generalized by German mathematician Helmut Hasse. The theorem concerns the structure of the group of units in the ring of integers of a number field, and is stated in general form as follows:

Theorem 62 (Dirichlet's Unit Theorem, generalized). *Let k be a number field, and let S be a finite set of normalized absolute values on k containing all archimedean absolute values. Then the S-unit group $\mathcal{O}_S^\times$ defined by*

$$\mathcal{O}_S = \{x \in k : |x|_\lambda \leq 1 \text{ for all } \lambda \in \Lambda_k \setminus S\}$$

has the following structure:

$$\mathcal{O}_S^\times \simeq \mathbb{Z}^{\#(S)-1} \oplus U,$$

where U is the group of roots of unity in $k^\times$.

Before we prove Theorem 62, we must make a few observations. For any positive real numbers $a \leq b$, let $X(a,b) \subset \mathcal{O}_S$ be the set defined by $X(a,b) = \{x \in \mathcal{O}_S : |x|_v \in [a,b] \text{ for all } v \in S\}$. We claim that $X(a,b)$ is finite for all choices of $a \leq b$. Indeed, let $W(a,b) \subset \mathbb{A}_k^\times$ be the (compact) set of all ideles $(x_v)_v$ such that $|x_v|_v \in [a,b]$ for all $v \in S$ and $|x_v|_v = 1$ otherwise. The ideles $(x_v)_v$ in $\mathbb{A}_k^\times$ for which $x_v = x_w$ for all v, w are precisely the ideles that lie in the image $k^\times$ under the diagonal embedding, so we have that $X(a,b) = W(a,b) \cap k^\times$. Since $W(a,b)$ is compact and $k^\times \hookrightarrow \mathbb{A}_k^\times$ is discrete, we have that $X(a,b)$ is finite.

Now let x be a root of unity in k. We know by the definition of a absolute value that $|x|_v = 1$ for all absolute values v. If we let $U \subset k^\times$ be the multiplicative, abelian subgroup of $k^\times$ defined by $U = \{x \in k^\times : |x|_v = 1 \text{ for all } v\}$, then by taking $a = b = 1$, we see by the previous paragraph that $U \subset X(1,1)$ for any choice of a set S of absolute values containing all archimedean absolute values, so in fact U is finite. Thus, every element of U has finite order and is hence a root of unity. We have thus shown that U is the group of roots of unity in $k^\times$.

We are now in position to provide a proof of Dirichlet's Unit Theorem:

Proof of Theorem 62. Let $s = \#(S) - 1$, and let $J \subset \mathbb{A}_k^\times$ be defined by $J = \{(\alpha_v)_v : |\alpha_v|_v = 1 \text{ for all } v \notin S\}$. Let $J_1 = J \cap \mathbb{A}_k^1$, those elements of J with content 1. Then since J is open in $\mathbb{A}_k^\times$, we have that J_1 is open in $\mathbb{A}_k^1$ (which has the subspace topology). We then have that $J_1/\mathcal{O}_S^\times = J_1/(J_1 \cap k^\times)$ is open in $\mathbb{A}_k^1/k^\times$, and in fact $J_1/\mathcal{O}_S^\times$ is also closed because it is a subgroup of $\mathbb{A}_k^1/k^\times$, and all subgroups of topological groups are closed. We therefore have that $J_1/\mathcal{O}_S^\times$ is compact. We now consider the map $\phi : J \to \mathbb{R}^s$ defined by

$$\phi((\alpha_v)_v) = \big(\log|\alpha_{v_1}|_{v_1}, \ldots, \log|\alpha_{v_s}|_{v_s}\big),$$

where $S = \{v_1, \ldots, v_s\}$. Observe that the map ϕ is both continuous and surjective, and notice that $\ker\phi \cap \mathcal{O}_S^\times = U$. We now claim that $\operatorname{im}(\phi|_{\mathcal{O}_S^\times})$ is a discrete subgroup of $\mathbb{R}^s$. To see why this is the case, we simply observe that the set $X(1/2, 2)$ is finite (by the argument in the first paragraph of this solution). Moreover, notice that $\operatorname{im}(\phi|_{J_1}) = \{(r_1, \ldots, r_s) : \sum_{i=1}^s r_i = 0\}$ and is thus an $(s-1)$-dimensional vector subspace of $\mathbb{R}^s$. Since we have that $J_1/\mathcal{O}_S^\times$ is compact, we deduce that $\phi(J_1)/\phi(\mathcal{O}_S^\times)$ is compact. We therefore have that $\operatorname{im}(\phi|_{\mathcal{O}_S^\times})$ is free on $s-1$ generators and being discrete, it is thus isomorphic to $\mathbb{Z}^{s-1}$. We conclude that $\mathcal{O}_S^\times \simeq \mathbb{Z}^{s-1} \oplus U$, which is the desired result. ♠

As a final example, we will compute the idele class group, which is a sort of generalization of the ideal class group, of the field $\mathbb{Q}$ of rational numbers.

Example 63. Recall that we studied the quotient group $\mathbb{A}_k^+/k^+$ in Theorem 52, and we also studied the quotient group $\mathbb{A}_k^1/k^\times$ in Theorem 58. One might ask what we can say about the analogous quotient group $\mathbb{A}_k^\times/k^\times$, which is known as the idele class group of the field k. Idele class groups are very important constructions in class field theory, but for now, we shall content ourselves with determining the idele class group of $\mathbb{Q}$. Specifically, we shall prove that

$$\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \simeq (0,\infty) \times \prod_p \mathbb{Z}_p^{\times}.$$

For each $x \in \mathbb{Q}_p^{\times}$, we can take its p-adic norm $|x|_p \in \langle p \rangle$, and then the number $x \cdot |x|_p$ has p-adic norm 1, so $x \cdot |x|_p \in \mathbb{Z}_p^{\times}$. In this way, we obtain a canonical isomorphism for each rational prime p:

$$\mathbb{Q}_p^{\times} \simeq \langle p \rangle \times \mathbb{Z}_p^{\times},$$

where $\langle p \rangle$ is the free abelian group of rank 1 generated by p, and the map is given by $x \mapsto (|x|_p, x \cdot |x|_p)$. Now, the idele group of $\mathbb{Q}$ is given by

$$\mathbb{A}_{\mathbb{Q}}^{\times} \simeq \mathbb{R}^{\times} \times {\prod_p}' \mathbb{Q}_p^{\times},$$

where the primed products above are restricted with respect to the rings $\mathbb{Z}_p^{\times}$. First notice that we may identify $\mathbb{R}^{\times}$ with $\{\pm 1\} \times (0,\infty)$. Next, observe that we may identify $\langle p \rangle$ with $\mathbb{Z}$. We then have that

$$\mathbb{A}_{\mathbb{Q}}^{\times} \simeq \{\pm 1\} \times (0,\infty) \times {\prod_p}' \mathbb{Q}_p^{\times} \simeq \{\pm 1\} \times (0,\infty) \times \prod_p \mathbb{Z}_p^{\times} \times \bigoplus_p \mathbb{Z},$$

by expanding out the definition of restricted product. We now claim that there is a canonical isomorphism $\mathbb{Q}^{\times} \simeq \{\pm 1\} \times \bigoplus_p \mathbb{Z}$. Indeed, given a rational number $x \in \mathbb{Q}^{\times}$, we can uniquely express x as

$$x = \pm \prod_p p^{e_p}$$

for a unique choice of sign ± and unique exponents $e_p \in \mathbb{Z}$ such that $e_p = 0$ for all but finitely many p. The desired isomorphism $\mathbb{Q}^{\times} \simeq \{\pm 1\} \times \bigoplus_p \mathbb{Z}$ is then given by sending x to its sign along with the list of e_p's. Combining our results, we have that

$$\mathbb{A}_{\mathbb{Q}}^{\times} \simeq \{\pm 1\} \times (0,\infty) \times \prod_p \mathbb{Z}_p^{\times} \times \bigoplus_p \mathbb{Z} \simeq \mathbb{Q}^{\times}(0,\infty) \times \prod_p \mathbb{Z}_p^{\times}.$$

Taking the quotient by $\mathbb{Q}^{\times}$, we find that

$$\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \simeq (0,\infty) \times \prod_p \mathbb{Z}_p^{\times},$$

which is the desired identification. ♣

6. Appendix: Auxiliary Theorems

In this appendix, we present statements and proofs of a few important auxiliary theorems from commutative algebra that are employed in this article. The next two results (primary decomposition and Nakayama's Lemma) are key implements used in proving Krull's Intersection Theorem, which was in turn used in the proof of Proposition 21. However, they are also quite interesting and useful in their own right.

Theorem 64 (Primary Decomposition)**.** *Let A be a ring, and let M be a Noetherian A-module. Then every A-submodule $N \subset M$ has a decomposition $N = \bigcap_k Q_k$, where the Q_k are primary A-submodules of M, meaning that $Q_k \neq M$ and for any $a \in A$ and $m \in M$ such that $am \in Q_k$, either $m \in Q_k$ or $a \in \sqrt{\mathrm{Ann}_A(M/Q)}$.*

Proof. We will first show that if $Q \subset M$ is primary, then $\mathfrak{p} = \sqrt{\mathrm{Ann}_A(M/Q)} \subset A$ is a prime ideal, in which case we will say that Q is $\mathfrak{p}$-primary. If $Q \subset M$ is primary, then suppose $ab \in \sqrt{\mathrm{Ann}_A(M/Q)}$. Then $a^n b^n m \in Q$ for all $m \in M$. If $a \notin \sqrt{\mathrm{Ann}_A(M/Q)}$, then we have that $a^{n-1}b^n m \in Q$ for all $m \in M$ since Q is primary. Repeating this argument n times, we find that $b^n m \in Q$ for all $m \in M$. If $b \notin \sqrt{\mathrm{Ann}_A(M/Q)}$, then by the same reasoning, we have that $m \in Q$ for all $m \in M$, which is a contradiction because $Q \neq M$. Thus, at least one of a or b must be in $\sqrt{\mathrm{Ann}_A(M/Q)}$, so $\sqrt{\mathrm{Ann}_A(M/Q)}$ is a prime ideal.

We will next show that if $Q \subset M$ is irreducible, then Q is primary. Let Q be an irreducible submodule of M. Observe that we may replace the pair (M, Q) with $(M/Q, 0)$, because Q is an irreducible submodule of M if and only if 0 is an irreducible submodule of M/Q, and Q is a primary submodule of M if and only if 0 is a primary submodule of M/Q. Thus, we can assume $Q = 0$. We must show that if $am = 0$ for some $a \in A$ and $m \in M$, then $m = 0$ or $a \in \sqrt{\mathrm{Ann}_A(M)}$. Let $x \in A$ be arbitrary, and consider the ascending chain of submodules $M_x \subset M_{x^2} \subset M_{x^3} \subset \dots$, where $M_{x^i} \subset M$ is the submodule defined by $M_{x^i} = \{m \in M : x^i m = 0\}$ for each positive integer i. Since M is Noetherian, this chain must terminate, so we have that $M_{x^{i+1}} = M_{x^i}$ for all $i \geq N$ for some positive integer N. We claim that $M_x \cap x^N M = 0$. Indeed, if $x^N m \in M_x$, then $x^{N+1}m = 0$, so $m \in M_{x^{N+1}} = M_{x^N}$, so $x^N m = 0$. Since 0 is irreducible, we have that $M_x = 0$, in which case $xm = 0 \Rightarrow m = 0$, or $x^N M = 0$, in which case $xm = 0 \Rightarrow x \in \sqrt{\mathrm{Ann}(M)}$, as desired.

We will now show that any submodule $N \subset M$ can be written as a finite intersection of irreducible submodules. Consider the set S of submodules of M that cannot be expressed as a finite intersection of irreducible submodules. Since M is Noetherian, if S is nonempty, we may choose a maximal element N of S. Clearly N is not irreducible, so we have that $N = N_1 \cap N_2$ for some submodules $N_1, N_2 \supsetneq N$. But neither N_1 nor N_2 is an element of S, so we can express each of N_1, N_2 as a finite intersection of irreducible submodules, which implies that $N = N_1 \cap N_2$ can also be expressed as a finite intersection of irreducible submodules, a contradiction implying that $S = \varnothing$. We conclude that every submodule of M can be expressed as a finite intersection of irreducible submodules. The theorem then follows by combining the above results. ♠

Proposition 65 (Nakayama's Lemma)**.** *Let R be a commutative ring, let M be a finitely-generated A-module, and let $I \subset A$ be an ideal such that $IM = M$. Then, there exists $a \equiv 1 \pmod{I}$ such that $aM = 0$.*

Proof. Clearly if M is generated by 0 elements, then $M = 0$, and the desired value of a is simply $a = 1$. We now induct upon the number n of generators of M. Suppose M is generated by $m_1, \dots, m_n$. Since $IM = M$, there exist $a_1, \dots, a_n \in I$ such that

$$m_1 = a_1 m_1 + \cdots + a_n m_n \Rightarrow (1 - a_1)m_1 = a_2 m_2 + \cdots + a_n m_n.$$

It follows that the A-module $(1-a_1)M$ is generated by $n-1$ elements. Moreover, we have that $I((1-a_1)M) = (1-a_1)M$ since $IM = M$. By induction, there exists $b \equiv 1 \pmod{I}$ such that $b(1-a_1)M = 0$. Simply taking $a = b(1-a_1)$ yields the desired result. ♠

Corollary 66 (Nakayama's Lemma for local rings)**.** *If A is a local ring with unique maximal ideal $\mathfrak{m}$, then for any finitely-generated A-module M, we have $M = 0$ if $\mathfrak{m}M = M$.*

Theorem 67 (Krull's Intersection Theorem)**.** *If A is a local Noetherian ring with maximal ideal $\mathfrak{m}$, then $\mathfrak{m}_\infty := \bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$.*

Proof. Let $\mathfrak{m}\mathfrak{m}_\infty = \bigcap_{k=1}^{N} \mathfrak{q}_k$ be a primary ideal decomposition, which exists because A is Noetherian. We claim that $\mathfrak{q}_k \supset \mathfrak{m}_\infty$ for all $k \in \{1, \dots, N\}$. Take $k \in \{1, \dots, N\}$, and consider the ideal $\sqrt{\mathfrak{q}_k}$ (which is prime because $\mathfrak{q}_k$ is primary). First, suppose $\sqrt{\mathfrak{q}_k} = \mathfrak{m}$. Since A is Noetherian, we have that $\mathfrak{q}_k \supset \mathfrak{m}^n$ for some positive integer n. Thus, we have that $\mathfrak{q}_k \supset \mathfrak{m}^n \supset \mathfrak{m}_\infty$. Now suppose $\sqrt{\mathfrak{q}_k} \neq \mathfrak{m}$. Since $\mathfrak{m}$ is the unique maximal ideal of A, we have that $\sqrt{\mathfrak{q}_k} \subsetneq \mathfrak{m}$. Take $x_k \in \mathfrak{m} \setminus \sqrt{\mathfrak{q}_k}$, and let $y \in \mathfrak{m}_\infty$ be any element. Then $yx_k \in \mathfrak{m}\mathfrak{m}_\infty \subset \mathfrak{q}_k$, so since $\mathfrak{q}_k$ is primary, we have that $y \in \mathfrak{q}_k$ or $x_k \in \sqrt{\mathfrak{q}_k}$. But since $x_k \notin \sqrt{\mathfrak{q}_k}$, we must have that $y \in \mathfrak{q}_k$. Since $y \in \mathfrak{m}_\infty$ was arbitrary, we have that $\mathfrak{m}_\infty \subset \mathfrak{q}_k$. Thus, the claim holds in all cases.

Since $\mathfrak{q}_k \supset \mathfrak{m}_\infty$ for all $k \in \{1, \dots, N\}$, we have that $\mathfrak{m}\mathfrak{m}_\infty = \bigcap_{k=1}^{N} \mathfrak{q}_k \supset \mathfrak{m}_\infty$. But $\mathfrak{m}_\infty \supset \mathfrak{m}\mathfrak{m}_\infty$, so it follows that $\mathfrak{m}_\infty = \mathfrak{m}\mathfrak{m}_\infty$. Because A is Noetherian, we have that $\mathfrak{m}_\infty$ is finitely generated, so since A is local, we have by Nakayama's Lemma that $\mathfrak{m}_\infty = 0$, as desired. ♠

We conclude this appendix with a proof of the Primitive Element Theorem, which was used in the proof of Theorem 33.

Theorem 68 (Primitive Element Theorem)**.** *Let k be a field, and let ℓ be a field extension of k, generated over k by $a_1, a_2, \dots, a_n$, where a_i is algebraic over k for all $i \in \{1, \dots, n\}$ and a_i is separable over k for all $i \in \{2, \dots, n\}$. Then there exists a primitive element $b \in \ell$ such that ℓ is generated over k by b.*

Proof. By induction, it suffices to consider the case where $n = 2$. We shall consider the elements $b_t = a_1 + ta_2 \in \ell$ for $t \in k$ and show that almost all of these elements are primitive. Our method of proof will be completely explicit, so given an extension satisfying the criteria of the theorem, one can follow the argument in order to compute a primitive element.

Let $f, g \in k[x]$ denote the minimal polynomials of a_1, a_2 respectively. Since $0 = f(a_1) = f(b_t - ta_2)$ for any $t \in k$, we have that a_2 is a root of the polynomial $h_t \in k(b_t)[x]$ defined by $h(x) = f(b_t - tx)$. Thus, g and h_t are divisible by the minimal polynomial of a_2 over $k(b_t)$ for all $t \in k$. Suppose g, h_t have a common factor of degree at least 2. We know that g, h_t already have a common root in a_2, and working in an algebraic closure ℓ' of ℓ, we see by the separability of a_2 that there must exist another common root of g, h_t, call it $c_t \in \ell' \setminus \{a_2\}$. Then $f(b_t - tc_t) = f(a_1 + t(a_2 - c_t)) = 0$, and there are clearly only finitely many values of t for which this can happen. For all other values of t, the polynomials g, h_t do not have a common factor of degree at least 2, so the minimal polynomial of a_2 over $k(b_t)$ must be linear, implying that $a_2 \in k(b_t)$, from which it follows that $a_1 \in k(b_t)$ as well. We may then take $b = b_t$. ♠

Acknowledgements

The author thanks Alison Miller for instructing him in the theory of commutative algebra, for suggesting the composition of this expository paper, and for providing useful comments on earlier drafts. Also, the author would like to thank Arul Shankar for his inspiring lectures on class field theory and for motivating the author to study the theory of valued fields in more depth.

References

[1] J. Cassels and A. Fröhlich, editors. *Algebraic Number Theory.* London Mathematical Society, 2010.

[2] D. Dummit and R. Foote. *Abstract Algebra.* John Wiley & sons, 2004.

[3] F. Gouvêa. *p-adic Numbers.* Springer, second edition, 1997.

[4] James S. Milne. Algebraic number theory (v3.06), 2014. Available at `www.jmilne.org/math/`.

[5] P. Samuel. *Algebraic Theory of Numbers.* Dover Publications, 1970.

Department of Mathematics, Harvard College, Cambridge, MA 02138
E-mail address: `aaswaminathan@college.harvard.edu`
URL: `scholar.harvard.edu/ashvin`