SEMINAR ON CLASS FIELD THEORY

MICHAEL BAKER, RAYMOND CHENG, RITVIK RAMKUMAR

3. Review: local theory of number fields

We now turn to the local theory of number fields, as is presented in Chapter II of Neukirch's *Algebraic Number Theory*. The treatment here will be at a slightly less breakneck pace, since this material is disjoint from PMATH 441. Grossly put, the local aspects of algebraic number theory introduce analytic ideas into algebraic problems. This is achieved by introducing valuations and absolute values, which can be thought of as algebraically-flavoured metrics.

3.1. **Intuition.** What we want to understand is the concept of a local field. A **local field** is a field K along with a nontrivial absolute value $|\cdot| : K \to \mathbf{R}$ such that (K, d) is a complete metric space and has a finite residue class field, where d is the metric induced by the absolute value. We will see later that these conditions are equivalent to asking for (K, d) to be a locally compact metric space.

Before going on to precisely define absolute values and develop the basic theory of local fields, let us consider why we might be interested in local fields. Intuitively speaking, local fields are algebraic objects in which we can talk about infinitesimal behaviour. An important manifestation of this is that we are able to solve polynomial equations via approximations in local fields. Moreover, by studying objects of interest locally, we are able to understand the local subtle structure of algebraic objects. As an analogy, think about studying each curve $C_n : y = x^n$ at the origin. For each n, C_n vanishes at the origin. But each are different in the sense that the C_n are "flatter" as n gets larger. This is made precise by noting that the first nonzero derivative of x^n comes later and later as n increases, which geometrically means that C_n moves away from 0 slower and slower (because $x < 1$ near 0). The differences between the C_n at the origin, then, come from differences in infinitesimal behaviour near 0.

Even more specifically, the local fields we will mostly be concerned with will be completions of fields with respect to a given absolute value. These are to be thought of as giving a power series expansion of an algebraic object, through which we can understand higher order behaviour of the object in question.

Not only do local fields carry rich local information, but when put together, they say much more. Pushing the analogy between power series and local fields a bit more, when the power series from all different points in the domain are put together, we essentially know the function in question. Analogously, when the local fields coming from all the *places*—which will come to have a precise meaning later!—are put together, information about the global field under study will emerge.

3.2. **Absolute Values.** Before we can dream of introducing analytic techniques into algebraic number theory, we need a notion that serves as the analogue of a norm in an arbitrary field K. This is the role of absolute values. An **absolute value** on K is a map $|\cdot| : K \to \mathbf{R}$ satisfying the following:

(a) $|x| > 0$ for all $x \in K^\times$;
(b) $|xy| = |x||y|$ for all $x, y \in K$;
(c) $|x + y| \leqslant |x| + |y|$.

Note that absolute values are also referred to as *(multiplicative) valuations*, but this terminology conflicts with another notion of valuation which we will need later. The use of "absolute values" here follows Bourbaki, Lang and Milne.

The first example of an absolute value is the **trivial absolute value**: for any field K, let $|\cdot| : K \to \mathbf{R}$ be defined by $|0| = 0$ and $|a| = 1$ for all $a \in K^\times$. It is obvious that this is an absolute value. Unless otherwise specified, however, whenever we talk about absolute values in these notes, we mean a nontrivial absolute value.

For a marginally more interesting class of absolute values, we consider those which arise from embeddings of number fields into the complex numbers. Let K be a number field and let $\sigma : K \hookrightarrow \mathbf{C}$ be any embedding of K into $\mathbf{C}$. Define $|\cdot|_\sigma : K \to \mathbf{R}$ by

$$|a|_\sigma := |\sigma(a)|,$$

for all $a \in K$, where the absolute value on the right is the usual one on $\mathbf{C}$: $|x + iy| = \sqrt{x^2 + y^2}$. One easily checks that $|\cdot|_\sigma$ is indeed an absolute value on K.

3.3. **Topology from Absolute Values.** One main purpose of introducing absolute values into the study of algebraic number theory is to allow us to say when algebraic objects are close to one another. Thus one very important aspect of absolute values on fields is the topology they induce. Specifically, let $|\cdot| : K \to \mathbf{R}$ be an absolute value on a field K. Define $d : K \times K \to \mathbf{R}$ by

$$d(x, y) := |x - y|.$$

The nondegeneracy and triangle inequality conditions in the definition of an absolute value make clear that d is a metric on K. Thus (K, d) is a metric space and hence a topological space once endowed with the metric topology. As in the case of norms, two absolute values $|\cdot|_1, |\cdot|_2 : K \to \mathbf{R}$ are said to be **equivalent** if they give rise to the same topology. By doing a little analysis, one can show that absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there exists $s \in \mathbf{R}_{>0}$ such that

$$|x|_1 = |x|_2^s$$

for all $x \in K$. Another characterization of when $|\cdot|_1$ and $|\cdot|_2$ are equivalent is the property that whenever $|x|_1 < 1$, $|x|_2 < 1$ as well.

3.4. **Completions of Fields.** Let K be a field with an absolute value $|\cdot|$ and view it as a metric space with the metric induced from $|\cdot|$. As mentioned in the introduction, one purpose of introducing absolute values into algebraic number theory is to allow us to solve polynomial equations via approximation techniques. This suggests that we wish to consider fields which are *complete* with respect to the equipped metric. Recall from real analysis that given a metric space, we can form its completion by taking the set of all Cauchy sequences in the metric space modulo the null sequences—those Cauchy sequences going to 0. Specializing this result to our situation, we have the following

Theorem 1. *Let $(K, |\cdot|)$ be a field equipped with an absolute value. Then there exists a complete field $(\hat{K}, |\cdot|)$ and a homomorphism $K \to \hat{K}$ preserving the absolute value which satisfies the following universal property: every absolute value preserving homomorphism $K \to L$ into a complete field $(L, |\cdot|')$ extends uniquely to a homomorphism $\hat{K} \to L$. Moreover, K can be identified with a dense subset of $\hat{K}$; in the case that $|\cdot|$ is nonarchimedean, K is actually open in $\hat{K}$.*

We will talk about nonarchimedean absolute values in the following subsection. For us, completions will be the manner in which local fields come about. Specifically, let K be a global field, $|\cdot|$ an absolute value on K and $\hat{K}$ be the completion of K with respect to the given absolute value. Then $\hat{K}$ will typically be a local field. For reasons I explain below, we wish to classify the local fields that arise in this way. We shall do this for number fields. Since number fields are finite extensions of $\mathbf{Q}$, this can be done by first classifying all the absolute values of $\mathbf{Q}$ and then examining how absolute values extend in finite field extensions. Before we go about classifying the absolute values of $\mathbf{Q}$, let us look at how the theory of absolute values on arbitrary fields consists of more than the familiar absolute values on $\mathbf{R}$ and $\mathbf{C}$.

3.5. **Nonarchimedean Absolute Values.** So far, the examples of absolute values on fields seem to echo only the familiar examples on $\mathbf{R}$ and $\mathbf{C}$. It turns out that the theory is far richer. Recall from a first course in analysis that the standard absolute values on $\mathbf{R}$ and $\mathbf{C}$ satisfy the so-called **archimedean property**:

For any $x, y \in \mathbf{R}$ (or $\mathbf{C}$), with $|x| < |y|$, there exists positive $n \in \mathbf{Z}$ such that $|y| < |nx| = n|x|$.

This rather reasonable looking property, however, does *not* hold for arbitrary absolute values. The archimedean property can be alternatively formulated as saying that the set $|\mathbf{Z}| = \{|n| : n \in \mathbf{Z}\} \subset \mathbf{R}$ is an unbounded set, where we view $\mathbf{Z}$ as a subring of $\mathbf{R}$ or $\mathbf{C}$.

An absolute value $|\cdot| : K \to \mathbf{R}$ is a **nonarchimedean absolute value** if $|n|$ remains bounded as n ranges over $\alpha(\mathbf{Z}) \subset K$, where $\alpha : \mathbf{Z} \to K$ is the unique ring homomorphism from $\mathbf{Z}$ to K. Nonarchimedean absolute values can be characterized in terms of a stronger triangle inequality condition.

Proposition 2. *Let K be a field. An absolute value $|\cdot| : K \to \mathbf{R}$ is nonarchimedean if and only if it satisfies the **strong triangle inequality** or **ultrametric inequality**: for all $x, y \in K$, $|x+y| \leqslant \max\{|x|, |y|\}$.*

Proof. If the strong inequality holds, then for $n \in \alpha(\mathbf{Z})$,

$$|n| = |1 + \cdots + 1| \leqslant 1$$

and so $|\alpha(\mathbf{Z})| \subset \mathbf{R}$ is clearly bounded. Conversely, suppose that $|\cdot|$ is nonarchimedean; then there is a positive integer N such that $|n| \leqslant N$ for all $n \in \alpha(\mathbf{Z})$. Let $a, b \in K$ with $|a| \leqslant |b|$. Then for each $n \in \mathbf{Z}_{>0}$,

$$|a+b|^n \leqslant \sum_{k=0}^{n} \left|\binom{n}{k}\right| |a|^k |b|^{n-k} \leqslant N(n+1)|b|^n.$$

Taking n^{th} roots,

$$|a+b| \leqslant N^{1/n}(n+1)^{1/n}|b|.$$

Since this holds for all $n \in \mathbf{Z}_{>0}$, taking $n \to \infty$ gives $|a+b| \leqslant |b| = \max\{|a|, |b|\}$. ∎

Either with the characterization in terms of the strong triangle inequality, or really, straight from the definition, we notice that any absolute value on any field K with positive characteristic is nonarchimedean: the set $\{\, |n| : n \in \alpha(\mathbf{Z}) \,\}$ is a set with size at most $\operatorname{char} K < \infty$.

Unfortunately for us, $\mathbf{Q}$ possesses quite a few nonarchimedean absolute values, complicating slightly the task of classifying all completions of $\mathbf{Q}$. To talk about these nonarchimedean absolute values, it will be convenient to pass from absolute values, which are multiplicative, to valuations, which are "logarithmic" in nature.

3.6. **Valuations.** Valuations should be thought of as a degree measurement on elements of a field. Even more vaguely, valuations can be thought of as a way of telling how "separated" objects are, how much objects are "folded" upon themselves, the "order of growth" of elements, etc. These vague statements will hopefully be clearer by the end of this section.

For us, valuations are primarily interesting because they give an alternate perspective on nonarchimedean absolute values. Let $|\cdot| : K \to \mathbf{R}$ be a nonarchimedean absolute value on a field K and define a function $\nu : K \to \mathbf{R} \cup \{\infty\}$ by $\nu(0) := \infty$ and for all $x \in K^\times$,

$$\nu(x) := -\log|x|.$$

The function ν satisfies the following properties, which are essentially consequences of the multiplicative properties enjoyed by absolute values, due to the application of the logarithm:

(a) $\nu(x) = \infty$ if and only if $x = 0$;
(b) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in K$;
(c) $\nu(x+y) \geqslant \min\{\nu(x), \nu(y)\}$ for all $x, y \in K$.

More generally, any function $\nu : K \to G \cup \{\infty\}$ from K into a totally ordered group G is called a **valuation** on K; if $G \cong \mathbf{Z}$, then ν is called a **discrete valuation**. Notice that we can go the other way, from a valuation back to a nonarchimedean absolute value: given a valuation $\nu : K \to \mathbf{R} \cup \{\infty\}$, define $|\cdot|_\nu : K \to \mathbf{R}_{\geqslant 0}$ by $|0|_\nu = 0$ and for all $x \in K^\times$,

$$|x|_\nu := e^{-\nu(x)}$$

for some $e > 1$. The choice of e is arbitrary, but there are some natural choices of e in the valuations we will soon encounter.

A valuation knows about the internal arithmetic of K: let ν be a valuation on K, $|\cdot|$ be the corresponding absolute value, and let

$$\begin{aligned} A &:= \{x \in K \mid \nu(x) \geqslant 0\} = \{x \in K \mid |x| \leqslant 1\}, \\ A^\times &:= \{x \in K \mid \nu(x) = 0\} = \{x \in K \mid |x| = 1\}, \\ \mathfrak{m} &:= \{x \in K \mid \nu(x) > 0\} = \{x \in K \mid |x| < 1\}. \end{aligned}$$

Then A is a ring with group of units $A^\times$ and unique maximal ideal $\mathfrak{m}$. Moreover, it is not too hard to see that K is the field of fractions of A. Any ring A that arises as a subring of a field K satisfying inequalities from a valuation defined on K is called a **valuation ring**; in the case that the valuation is discrete, A is called a **discrete valuation ring**.

Using the property (b) of valuations, we also see that for every $x \in K$, either $x \in A$ or else $x^{-1} \in A$. This property allows one to see that valuation rings are integrally closed: suppose that $x \in K - A$ satisfies the equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

where $a_i \in A$. Multiplying through by $x^{-(n-1)}$ and rearranging, it follows that

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

But the right hand side is in A since $x^{-1} \in A$, so $x \in A$, which is a contradiction.

3.7. **Discrete Valuations.** Understanding discrete valuations will help us obtain a more concrete understanding of nonarchimedean completions. There is a rather useful characterization of discrete valuation rings. The proof of this characterization can be found in most references for commutative algebra.

Theorem 3. *Let A be a commutative ring. Then A is a discrete valuation ring if and only if A is a local noetherian ring whose maximal ideal is generated by a non-nilpotent element.*

By the characterization above, if A is a discrete valuation ring and $\mathfrak{m}$ is its unique maximal ideal, then $\mathfrak{m} = (\pi)$ for some non-nilpotent $\pi \in A$. In other words, every element $x \in A$ can be written as $x = \pi^m u$ for some $u \in A^\times$, with $(u, \pi) = A$, and positive integer m; notice that since either $x \in A$ or $x^{-1} \in A$ for every $x \in K$, this shows that every $x \in K$ can be written as $x = \pi^m u$ for some $u \in A^\times$ and $m \in \mathbf{Z}$. The element π is variously called a **(local) uniformizing parameter** or **prime element** of A. The valuation defining A in its field of fractions can be recovered by defining $\nu : K^\times \to \mathbf{Z}$ by setting $\nu(x) = m$, where $x = \pi^m u$. The integer m is called the **order** of π in x.

In the context of discrete valuation rings, there is a natural choice of normalization when passing between absolute values and valuations. Let π be a local uniformizing parameter for $(K, |\cdot|)$ and let $e \in \mathbf{R}_{>1}$ be such that $-\log_e|\pi| = 1$. The valuation constructed with this choice of e is often called the **normalized discrete valuation** associated with $|\cdot|$ and is often denoted $\operatorname{ord} : K \to \mathbf{Z} \cup \{\infty\}$. Put more abstractly, any valuation ν associated with a discrete absolute value—this is an absolute value for which $|K^\times| \subseteq \mathbf{R}_{\geqslant 0}$ is a discrete set, which can be shown to be equivalent to saying that the associated valuation is discrete—has image $\nu(K^\times) = c\mathbf{Z}$ for some constant c; when $c = 1$, then ν is a normalized discrete valuation.

An example should give some geometric and algebraic intuition to the whole ordeal. Let k be a field and let $B := k[t]$ be a polynomial ring over k and let $A := B_{(t)}$ be the localization of B with respect to the principal ideal generated by t, that is,

$$B_{(t)} = \left\{ \frac{p(t)}{q(t)} \;\middle|\; p, q \in B,\ q(0) \neq 0 \right\}.$$

Then A is a noetherian local ring whose maximal ideal is generated by t and thus is a discrete valuation ring. The discrete valuation $\nu : A \to \mathbf{Z}$ is defined on $0 \neq p(t) \in A$ by factoring $p(t) = t^m q(t)$ for $q \in A$ such that $(q, t) = A$ and setting $\nu(p) = m$. More concretely, this means that m is the largest power of t dividing all the terms of p; put yet a different way, $\nu(p)$ is the order of vanishing of p at $t = 0$.

3.8. **Completions of Q.** Finally, we come back to look at the absolute values of $\mathbf{Q}$ and their completions. There is one very obvious archimedean absolute value: view $\mathbf{Q}$ as a subfield of $\mathbf{R}$ and let $|\cdot|_\infty : \mathbf{Q} \to \mathbf{R}_{\geqslant 0}$ be the restriction of the standard absolute value $|\cdot| : \mathbf{R} \to \mathbf{R}_{\geqslant 0}$.

More interesting absolute values arise by considering the various discrete valuation rings contained in $\mathbf{Q}$. Fix a prime $p \in \mathbf{Z}$ and note that the noetherian local ring

$$\mathbf{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbf{Z}, p \nmid b \right\}$$

has maximal ideal generated by p. By the classification of discrete valuation rings above, we see that $\mathbf{Z}_{(p)}$ is a discrete valuation ring; let $\nu_p : \mathbf{Q} \to \mathbf{Z}$ be the corresponding discrete valuation extended to $\mathbf{Q}$. Then we obtain an absolute value $|\cdot|_p : \mathbf{Q} \to \mathbf{R}_{\geqslant 0}$ defined by

$$|x|_p := \left(\frac{1}{e}\right)^{\nu_p(x)},$$

where $e > 1$. In this case, there is a rather natural choice for e: set $e = p$. The resulting absolute value is called the **(normalized) p-adic absolute value** and the associated discrete valuation is called the **p-adic valuation**. Let $\mathbf{Q}_p$ be the completion of $\mathbf{Q}$ with respect to the p-adic absolute value and call it the **p-adic number field**. The elements of the ring of integers $\mathbf{Z}_p$ in $\mathbf{Q}_p$ are called **p-adic integers**.

It turns out that we have now seen all absolute values of $\mathbf{Q}$. Recall that equivalent absolute values define the same topology and hence have the same completion.

Theorem 4 (Ostrowski)**.** *Let $|\cdot|$ be a nontrivial absolute value on $\mathbf{Q}$.*

(1) If $|\cdot|$ is archimedean, then it is equivalent to $|\cdot|_\infty$;
(2) If $|\cdot|$ is nonarchimedean, then it is equivalent to $|\cdot|_p$ for exactly one prime $p \in \mathbf{Z}$.

As a consequence of Ostrowski's Theorem, the fields which can be obtained as completions of $\mathbf{Q}$ are $\mathbf{R}$ and the p-adic number fields $\mathbf{Q}_p$, $p \in \mathbf{Z}$ prime. The real numbers $\mathbf{R}$ is a field we (should) understand well at this point, but the p-adic number fields might be a tad more mysterious. To gain a better understanding of the $\mathbf{Q}_p$, and to lay algebraic foundations for understanding completions of other number fields, let us take a closer look at what is going on when we take a completion with respect to a nonarchimedean absolute value. We will return to classifying completions of other number fields soon.

3.9. **Nonarchimedean Completions: Analytic Perspective.** Completions of fields, as we have seen, can be described in analytic terms with the help of an absolute value and a corresponding topology. However, completions can also be constructed in a purely algebraic manner. We shall discuss how completions are treated algebraically after looking at some properties of the analytic completion procedure.

Throughout this subsection, let K be a field with nonarchimedean discrete absolute value $|\cdot|$ and denote by $\hat{K}$ the completion of K with respect to $|\cdot|$. Recall that $\hat{K}$ is constructed as the set of all Cauchy sequences of K modulo the null sequences. In other words, an element of $\hat{K}$ is represented by a Cauchy sequence $\{a_n\}$ for $a_n \in K$. Since $|K^\times| \subset \mathbf{R}$ is discrete, the absolute value of a convergent sequence must be eventually constant. In particular, this means that $|\cdot|$ extends uniquely to $\hat{K}$: set $|\{a_n\}|$ to be the value it is eventually constant at. It follows that $|K^\times| = |\hat{K}^\times|$. If $\mathrm{ord} : K^\times \to \mathbf{Z}$ is a normalized discrete valuation for $|\cdot|$, it also follows that it extends uniquely to a normalized discrete valuation $\mathrm{ord} : \hat{K}^\times \to \mathbf{Z}$.

This observation makes it clear that the ring

$$\hat{A} = \{ x \in \hat{K} \mid |x| \leqslant 1 \}$$

is the closure of the ring $A \subset K$ in $\hat{K}$. The maximal ideal

$$\hat{\mathfrak{m}} = \{ x \in \hat{K} \mid |x| < 1 \}$$

is the closure of $\mathfrak{m} \lhd A$ in $\hat{A}$. If $\pi \in K$ is such that $\mathrm{ord}(\pi) = 1$, then π generates $\mathfrak{m}$ in A and by the same reasons, generates $\hat{\mathfrak{m}}$ in $\hat{A}$. In similar spirit, the powers $\hat{\mathfrak{m}}^n$, $n \in \mathbf{Z}_{>0}$, of $\hat{\mathfrak{m}}$ are the closures of $\mathfrak{m}^n$ in $\hat{A}$ and $\hat{\mathfrak{m}}^n$ is generated in $\hat{A}$ by π^n.

Notice that since $\mathfrak{m}^n \subseteq \hat{\mathfrak{m}}^n$ and $A \subseteq \hat{A}$, via the identification of A with the equivalence class of Cauchy sequences in $\hat{A}$ represented by constant sequences, we have an induced map

$$A/\mathfrak{m}^n \to \hat{A}/\hat{\mathfrak{m}}^n$$

for each $n \in \mathbf{Z}_{>0}$.

Lemma 5. *The map $A/\mathfrak{m}^n \to \hat{A}/\hat{\mathfrak{m}}^n$ is an isomorphism for each positive integer n.*

Proof. The maximal ideals can be described via inequalities which show it to be both open and closed:

$$\mathfrak{m}^n = \{\, x \in A \mid |x| \leqslant |\pi|^n \,\} = \{\, x \in A \mid |x| < |\pi|^{n-1} \,\},$$

where the second equality is due to the discreteness of $|\cdot|$. Now suppose $a \in A$ is in the kernel of the above map. By definition, this means that the constant sequence consisting of all a converges to an element of $\hat{\mathfrak{m}}^n$. Since each element of the sequence is found in A the closedness of $\mathfrak{m}^n$ in A implies $a \in \mathfrak{m}^n$, i.e. $a = 0$ in $A/\mathfrak{m}^n$. Now, the map is surjective since $A \hookrightarrow \hat{A}$ has a dense image and $\hat{\mathfrak{m}}$ is open. ∎

This lemma allows us to forget trying to work with Cauchy sequences for the most part and just use regular elements of A when working with the quotient rings. To describe all the new elements added in the completion, we can use power series.

Lemma 6. *Let S be a system of representatives for $A/\mathfrak{m}$. Then for any positive integer n, the series*

$$a_{-n}\pi^{-n} + \cdots + a_0 + a_1\pi + \cdots, \qquad a_i \in S$$

is a Cauchy series in $\hat{K}$, and every Cauchy series in $\hat{K}$ is equivalent to exactly one series of this form. In particular, every element of $\hat{K}$ has a unique representative of this form.

Proof. Let $s_M := \sum_{i=-n}^{M} a_i\pi^i$ denote the M^{th} partial sum and note that since $|\cdot|$ is nonarchimedean, we have

$$|s_M - s_N| \leqslant |\pi^{M+1}|, \qquad M < N,$$

which shows that the series is Cauchy.

For the second statement, begin with $\alpha \in \hat{K}$ and write $\alpha = \pi^n\alpha_0$ for some $n \in \mathbf{Z}$ and $\alpha_0 \in \hat{A}^\times$. Since $A/\mathfrak{m} \cong \hat{A}/\hat{\mathfrak{m}}$, the definition of S shows that there exists $a_0 \in S$ such that $\alpha_0 - a_0 \in \hat{\mathfrak{m}}$. Let $\alpha_1 := \frac{\alpha_0 - a_0}{\pi}$, then $\alpha_1 \in \hat{A}$—and may already be in $\hat{\mathfrak{m}}$—so we may yet again find $a_1 \in S$ such that $\alpha_1 - a_1 \in \hat{\mathfrak{m}}$. Let $\alpha_2 := \frac{\alpha_1 - a_1}{\pi} \in A$ and let $a_2 \in S$ be such that $\alpha_2 - a_2 \in \hat{\mathfrak{m}}$. Continuing in this fashion, we have

$$\alpha_0 = a_0 + a_1\pi + a_2\pi^2 + \cdots, \qquad \alpha = \pi^n\alpha_0.$$

This shows existence of the power series representation. For uniqueness, it suffices to show that there is a unique representative for 0. Since the absolute value is nonarchimedean

$$\left|\sum_i a_i\pi^i\right| = |\pi^m|$$

where a_m is the first nonzero coefficient in the series. From this, it easily follows that the series represents 0 if and only if every coefficient is 0. ∎

3.10. **Interlude on Inverse Limits.** To discuss algebraic completions, we need a purely algebraic way of constructing limits. This construction is useful for completing fields, but also for understanding the Galois theory of infinite extensions. We shall therefore take some time and develop the algebra behind inverse limits and look at a few important instances of this construction.

An *inverse limit* (or sometimes *projective limit* or simply *limit*) is to be thought of as the result of zooming closer and closer to an object: we start with a sequence of "magnifications" of this algebraic entity and then we take this sequence to the limit.

The "sequence of magnifications" idea is made precise by the notion of an inverse system. Let $\mathcal{I}$ be a nonempty poset and let $(A_i)_{i\in\mathcal{I}}$ be a collection of objects of a category $\mathcal{C}$ indexed by $\mathcal{I}$, i.e. view $\mathcal{I}$ as a diagram in $\mathcal{C}$. Assume that for each $i \leqslant j \in \mathcal{I}$ there is a morphism $\varphi_{ij} : A_j \to A_i$. The collection $(A_i, \varphi_{ij} : A_j \to A_i)$ is then called an **inverse system** if

(1) $\varphi_{ii} = \mathrm{id}_{A_i}$ for all $i \in \mathcal{I}$; and
(2) $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ for all $i \leqslant j \leqslant k \in \mathcal{I}$.

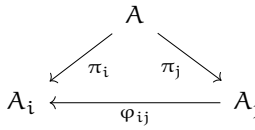
Note for the cognoscente: An inverse system can be defined more generally as a functor from a cofiltered category, but for our purposes, the notion of an inverse directed set is more than sufficient.

Most often, $\mathcal{I}$ will be a linearly ordered set, so the diagram given by $\mathcal{I}$ in $\mathcal{C}$ will have the shape

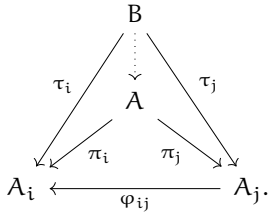
$$\cdots \longleftarrow A_\alpha \longleftarrow A_\beta \longleftarrow A_\gamma \longleftarrow \cdots$$

and the inverse system axioms merely say that the composite morphisms above behave as expected. Intuitively, this diagram describes the situation where you are able to obtain information at arbitrarily fine resolutions, but you do not have the ability to zoom in to improve coarse information to a finer resolution; the morphisms present only allow you to "zoom out" (think, for example, of truncating terms of a power series).

The **inverse limit** of the inverse system (A_i, φ_{ij}) is then the limit over the diagram $\mathcal{I}$. More concretely, this consists of an object A in $\mathcal{C}$ and morphisms $\pi_i : A \to A_i$ for each $i \in \mathcal{I}$ such that $\varphi_{ij} \circ \pi_j = \pi_i$ for each $i \leqslant j \in \mathcal{I}$, i.e. each of the following triangles commute:



and such that A is "final" with this property: for any object B in $\mathcal{C}$ with morphisms $\tau_i : B \to A_i$ satisfying $\varphi_{ij} \circ \tau_j = \tau_i$, each instance ($i \leqslant j$) of the diagram below commutes:



Back to the magnification metaphor, the inverse limit is an object that holds the finest image possible; the resolution of the limit is so high that any other picture B which can zoom out to the constituent pictures A_i must be contained in A.

The description of the inverse limit immediately tells us that A is obtained as a subobject of the product of the A_i. This is because the product is final for a more general class of "cones" than is the inverse limit (namely, one omits the "satisfying $\varphi_{ij} \circ \tau_j = \tau_i$" coherence condition). Indeed, if $\mathcal{C}$ is a concrete category in which the product of the A_i exists, A can be taken as

$$\varprojlim_i A_i := A = \left\{ (a_i)_i \in \prod_{i \in \mathcal{I}} A_i \;\middle|\; \varphi_{ij}(a_j) = a_i \;\forall\, i \leqslant j \in \mathcal{I} \right\}.$$

An important instance of inverse limits which we will encounter soon enough is that of profinite groups. A **profinite group** is a topological group which is isomorphic to the inverse limit of an inverse system of discrete finite groups. Profinite groups are important for us for two reasons. First, the Galois groups of infinite Galois extensions are profinite groups obtained as inverse limits indexed by the finite subextensions of the big extension. Second, the p-adic integers $\mathbf{Z}_p$, $p \in \mathbf{Z}$ prime, are profinite groups. We will explore the p-adic numbers soon enough and we will also discuss infinite Galois theory at some point in the future.

3.11. **Nonarchimedean Completions: Algebraic Perspective.** Back to talking about completions. The inverse limit operation is the algebraic formalism required to construct completions of rings in a purely algebraic manner. First let us describe how inverse limits are usually used in this context. Let A be a ring

and let $\mathfrak{m}$ be an ideal (not necessarily maximal) of A. Then we have an inverse system obtained by setting $A_0 := A$, and for $i \geqslant 1$, $A_i := A/\mathfrak{m}^i$ and the maps $A_j \to A_i$, where $i \leqslant j$, are the natural quotient maps:

$$A/\mathfrak{m} \leftarrow A/\mathfrak{m}^2 \leftarrow A/\mathfrak{m}^3 \leftarrow \cdots .$$

The descending sequence $A := \mathfrak{m}^0 \supseteq \mathfrak{m}^1 \supseteq \mathfrak{m}^2 \supseteq \cdots$ is called the **$\mathfrak{m}$-adic filtration** of A and the inverse limit of the corresponding sequence of quotient rings, as above, is called the **completion of A with respect to $\mathfrak{m}$**, and will be denoted $\hat{A}_\mathfrak{m}$ or simply $\hat{A}$ when $\mathfrak{m}$ is understood.

We can describe the completion $\hat{A}$ explicitly as follows:

$$\hat{A} = \left\{ (a_1, a_2, \ldots) \in \prod A/\mathfrak{m}^i \;\middle|\; a_j \equiv a_i \pmod{\mathfrak{m}^i} \right\}.$$

First notice that this completion is isomorphic to the analytic one: this follows from the lemma that $A/\mathfrak{m}^n \to \hat{A}/\hat{\mathfrak{m}}^n$ is an isomorphism for all n and the universal property of $\hat{A}$.

3.12. **p-adic Numbers.** Having looked at the general theory of completions, let us consider the example of the p-adic numbers $\mathbf{Q}_p$, $p \in \mathbf{Z}$ prime. Recall first that $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to the absolute value associated to the prime ideal $p\mathbf{Z}$ of $\mathbf{Z}$. Alternatively, $\mathbf{Q}_p$ can be constructed as the field of fractions of the completion $\mathbf{Z}_p$ of $\mathbf{Z}$ with respect to the $p\mathbf{Z}$-adic filtration. The analytic perspective suggests that elements of $\mathbf{Q}_p$ are equivalence classes of Cauchy sequences of $\mathbf{Q}$ with respect to $|\cdot|_p$. But we also have shown that we can represent each equivalence class uniquely in the form of a Laurent series in p,

$$\sum_{i \geqslant n} a_i p^i$$

for some $n \in \mathbf{Z}$ and with each $a_i \in \{0, \ldots, p-1\}$. It's not too difficult to see that elements of $\mathbf{Z}_p$ can be represented as power series in p, i.e. the index of the first nonzero coefficient is nonnegative.

From the algebraic perspective, elements of $\mathbf{Z}_p$ are tuples $(A_1, A_2, \ldots)$ in $\prod_i \mathbf{Z}/p^i\mathbf{Z}$ for which $A_j \equiv A_i \pmod{p^i}$ for all $i \leqslant j$. A moment's thought should allow one to see that the A_i are the partial sums of the power series representation. A similar representation for $\mathbf{Q}_p$ can be described, where the tuple now is doubly infinite with support bounded below.

Let's work out an example. Let p be any prime and consider the sum

$$1 + p + p^2 + \cdots + p^n + \cdots \in \mathbf{Q}_p.$$

The n^{th} partial sum of this series is

$$1 + p + \cdots + p^{n-1} = \frac{p^n - 1}{p - 1}.$$

Taking $n \to \infty$, we have that

$$\sum_{k \geqslant 0} p^k = \frac{1}{1-p}.$$

Especially cute are when $p = 2$ and $p = 3$, where one obtains -1 and $-1/2$, respectively.

3.13. **Polynomials in Complete Fields.** One more piece of algebra before we get back to looking at number fields. Our objects of study are field extensions, where the fields are eventually assumed to be complete. Completeness, as we mentioned in the beginning, allows us to find roots of polynomials via approximation techniques. That is what we will look at presently. Note that these results can be cast in a more general setting; consult just about any algebra book. There are several ways to state the following result; we shall phrase it in terms of factoring polynomials since splitting of primes is what we are primarily interested in.

For this section, let A be a complete discrete valuation ring, let π be a generator for the maximal ideal $\mathfrak{m}$ of A and let k be the residue field of A. For $f(x) \in A[x]$, write $\bar{f}(x)$ for the image of $f(x)$ in $k[x]$ under the quotient map (that is, reduce the coefficients modulo $\mathfrak{m}$). We use these notations unless otherwise stated.

Theorem 7 (Hensel's Lemma)**.** *Let $f(x) \in A[x]$ be a monic polynomial. If $\bar{f}(x)$ factors as $\bar{f} = g_0 h_0$ with g_0 and h_0 monic and relatively prime, then f itself factors as $f = gh$ with g and h monic and such that $\bar{g} = g_0$ and $\bar{h} = h_0$. Moreover, g and h are uniquely determined, and $(g, h) = A[x]$.*

The existence proof will make clear why this result should be thought of solving the polynomial f via approximations.

Proof of Hensel's Lemma. Notice that the hypotheses of the theorem are equivalent to saying that

$$f - g_0 h_0 \in \pi \cdot A[x].$$

Completeness of A along with this view of the hypotheses suggests that we should look for g and h by looking for power series in π. The power series will be constructed inductively. Suppose that g_n and h_n are found such that

$$f \equiv g_n h_n \mod \pi^{n+1} \cdot A[x]$$

and such that $g_n \equiv g_0$ and $h_n \equiv h_0$ in $\pi A[x]$. The next approximation will be obtained by adding a π^{n+1} term, which means that we want to find $u, v \in A[x]$ such that

$$f - (g_n + \pi^{n+1}u)(h_n + \pi^{n+1}v) \equiv 0 \mod \pi^{n+2}A[x].$$

We want the approximate factors to reduce to g_0 and h_0 so we should have the degree of u and v less than g_0 and h_0, respectively; however, since we can add terms with coefficient divisible by π, which will disappear during the reduction, we need to impose this condition explicitly in order for g_{n+1} and h_{n+1} to be uniquely specified. Rearranging the above equation, we are looking for $u, v \in A[x]$ with $\deg u < \deg g_0$ and $\deg v < \deg h_0$ and

$$uh_n + vg_n \equiv \frac{f - g_n h_n}{\pi^{n+1}} \mod \pi A[x].$$

Since g_0 and h_0 are relatively prime, the following lemma will show that u and v exists. ∎

Lemma 8. *If $g, h \in A[x]$ are such that $\bar{g}$ and $\bar{h}$ are relatively prime, and g is monic, then there exists $u, v \in A[x]$ with $\deg u < \deg g$ and $\deg v < \deg h$ such that $uh + vg = 1$.*

Proof. Let $M := A[x]/(g, h)$. Since g is monic, M is a finitely generated A-module. Since $(\bar{g}, \bar{h}) = k[x]$, we have $(g, h) + \mathfrak{m}A[x] = A[x]$, from which dividing out by (g, h) shows that $\mathfrak{m}M = M$. Nakayama's Lemma then implies $M = 0$.

Let $u, v \in A[x]$ be such that $uh + vg = 1$ and suppose that $\deg v \geqslant \deg h$. Write $v = hq + r$ for $\deg r < \deg h$, then

$$(u + gq)h + rg = 1$$

and note that the equality above immediately implies $\deg(u + gq) < \deg g$. ∎

3.14. **Extending Absolute Values from Complete Base Fields.** Back to absolute values. Recall that our purpose was to classify the absolute values of number fields and we intended to do this by figuring out how absolute values of $\mathbf{Q}$ extend up. Well, let us worry about the nonarchimedean absolute values first. Let K be a finite extension of $\mathbf{Q}$ and let $|\cdot|$ be a nonarchimedean absolute value on $\mathbf{Q}$. From our discussions before, we know that each nonarchimedean absolute value on $\mathbf{Q}$ arises from the valuation associated to some prime number $p \in \mathbf{Z}$. Let A be the integral closure of $\mathbf{Z}$ in K; then A is a Dedekind domain and the ideal $pA \subseteq A$ factors uniquely into a product of prime ideals

$$pA = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Each of the primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ give rise to a valuation on K and hence an absolute value. How might these be related to the absolute value we started with? This question can be answered in a rather nice way in the case the underlying field is complete with respect to the absolute value we started with.

Theorem 9. *Let K be a field complete with respect to an absolute value $|\cdot|_K$ and let L be an algebraic extension of K of degree n. Then $|\cdot|_K$ extends uniquely to an absolute value $|\cdot|_L$ on L and L is complete with respect to this absolute value. Moreover, when $[L : K] = n < \infty$, this extension is given by, for all $\beta \in L$,*

$$|\beta|_L = |N_{L|K}\, \beta|_K^{1/n}$$

Proof. Note that since algebraic extensions are given by the union of all finite subextensions, it suffices to prove the uniqueness for finite extensions L of K. For complete proofs, see Milne ANT Theorem 7.38 and Neukirch Chapter 2 Theorem 4.8. ∎

There is an important technical consequence of this theorem. The uniqueness of the extension implies that there is a unique valuation which extends the valuation associated to $\mathfrak{p}$. But each unique prime in $\mathcal{O}_L$ over $\mathfrak{p}$ would give a distinct valuation extending $\mathfrak{p}$. So in fact, the uniqueness tells us that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e$ for a unique prime $\mathfrak{P}$ of $\mathcal{O}_L$ and for some positive integer e. Recall that e is called the *ramification degree* of $\mathfrak{P}$ over $\mathfrak{p}$; there is also an integer $f := [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ called the *inertia degree* (or *residue class degree*) of $\mathfrak{P}$ over $\mathfrak{p}$. Since in general, $[L : K] = \sum e_i f_i$ where the sum is taken over all primes lying over $\mathfrak{p}$, we have the following

Corollary 10. *Let K and L be as above. Then $n = ef$, where $n = [L : K]$, e is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, and f is the degree of the residue field extension.*

I should say a word about what normalizations are typically chosen for the absolute values associated to primes $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of a number field K. As before, localize $\mathcal{O}_K$ with respect to $\mathfrak{p}$ and let $\nu_\mathfrak{p}$ be the discrete valuation defined on $(\mathcal{O}_K)_\mathfrak{p}$ which sends a local uniformizing parameter of $(\mathcal{O}_K)_\mathfrak{p}$ to 1. Let $\mathbf{N}\mathfrak{p}$ denote the cardinality of the residue field of $(\mathcal{O}_K)_\mathfrak{p}$—recall that this is finite since the residue field is a finite extension of $\mathbf{Z}/p\mathbf{Z}$, where $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$, and the degree of the field extension is bounded by $[K : \mathbf{Q}]$. Then set, for $x \in K$,

$$|x|_\mathfrak{p} := \left(\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{\nu_\mathfrak{p}(x)}.$$

3.15. **Extending Absolute Values in General.** With an understanding of how absolute values extend when the base field is complete, we can look at what happens when the base field is not necessarily complete. Let K be a field with absolute value $|\cdot|$ and let L be a finite separable extension of K. By the Theorem of Primitive Elements, we can write $L = K[\alpha]$ for some $\alpha \in L$. Let $f(x) \in K[x]$ be the minimal polynomial of α. Let $|\cdot|'$ be any extension of $|\cdot|$ to L. Forming the completion $\hat{L}$ of L with respect to $|\cdot|'$ gives the diagram:

$$\begin{array}{ccc} L & \hookrightarrow & \hat{L} \\ \uparrow & & \uparrow \\ K & \hookrightarrow & \hat{K} \end{array}$$

where the absolute values on each of the fields are extensions of one another. Notice that $\hat{K}[\alpha]$ is a finite extension of $\hat{K}$ and $\hat{K}$ is complete with respect to the absolute value $|\cdot|$ inherited from K. By the theorem, $\hat{K}[\alpha]$ itself is complete. But notice that $L = K[\alpha] \subseteq \hat{K}[\alpha]$. The facts that L is contained in $\hat{K}[\alpha]$ and that $\hat{K}[\alpha]$ is complete implies that $\hat{L} \subseteq \hat{K}[\alpha]$; the other inclusion is easily obtained by viewing $\hat{L}$ as the completion of the ring $K[\alpha] = L$.

Now let $g(x) \in \hat{K}[x]$ be the minimal polynomial of α over $\hat{K}$. We can view $f(x)$ as a polynomial in $\hat{K}[x]$ and note that since $f(\alpha) = 0$, g must divide f. In this way, we can associate an irreducible factor g of f in $\hat{K}[x]$ to the extension $|\cdot|'$.

Conversely, let $g(x) \in \hat{K}[x]$ be a monic irreducible factor of $f(x)$ in $\hat{K}[x]$ and let $\hat{K}[\alpha] := \hat{K}[x]/(g)$. This gives us a diagram

$$\begin{array}{ccc} L & \hookrightarrow & \hat{K}[\alpha] \\ \uparrow & & \uparrow \\ K & \hookrightarrow & \hat{K}. \end{array}$$

But note that $\hat{K}$ is complete, so by the previous theorem, the absolute value on $\hat{K}$ extends to a unique absolute value on $\hat{K}[\alpha]$. This, in turn, restricts to an absolute value on L which extends $|\cdot|$. Observe that these operations are inverse to one another, hence we have shown the following.

Proposition 11. *Let $L = K[\alpha]$ be a finite separable extension of a field K, and let $f(x) \in K[x]$ be the minimal polynomial of α. Then there is a natural one-to-one correspondence between the extensions of $|\cdot|$ to L and the irreducible factors of $f(x)$ in $\hat{K}[x]$.*

What does this really mean in our context of interest? Well let K be a number field, L a finite extension of K. Write $\mathcal{O}_K$ for the ring of integers of K and let $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in L$ and let $f(x) \in K[x]$ be the

minimal polynomial. Suppose that our absolute value $|\cdot|$ on K comes from the valuation associated to a prime $\mathfrak{p}$ of $\mathcal{O}_K$. Now let

$$f(x) = f_1(x) \cdots f_g(x).$$

for $f_1, \ldots, f_g \in \hat{K}[x]$ irreducible. Since the f_i are irreducible in $\hat{K}[x]$ and $\hat{K}$ is complete, Hensel's Lemma implies that the f_i, modulo $\hat{\mathfrak{p}}$, are powers of irreducible polynomials $h_i(x)$,

$$\bar{f}_i(x) = h_i(x)^{e_i} \mod \hat{\mathfrak{p}}.$$

Then reducing f by $\hat{\mathfrak{p}}$, we have the factorization

$$\bar{f}(x) = h_1(x)^{e_1} \cdots h_g(x)^{e_g} \mod \hat{\mathfrak{p}}.$$

This is useful in view of the following result about factorization of ideals in extensions of Dedekind domains.

Theorem 12. *Let A be a Dedekind domain with field of fractions K. Let L be a finite separable extension of K and let B be the integral closure of A in L. Suppose $B = A[\alpha]$ and let $f(x) \in A[x]$ be the minimal polynomial of α. Let $\mathfrak{p}$ be a prime ideal of A. Suppose*

$$f(x) \equiv \prod h_i(x)^{e_i} \mod \mathfrak{p}$$

for some distinct irreducible polynomials $h_i \in A[x]/\mathfrak{p}$ and positive integers e_i. Then

$$\mathfrak{p}B = \prod (\mathfrak{p}, h_i(\alpha))^{e_i}$$

is the factorization of the ideal generated by $\mathfrak{p}$ in B into product of powers of distinct prime ideals.

Proof. See Milne ANT Theorem 3.41. ∎

Applying this theorem in our situation, we find that

$$\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}, \quad \mathfrak{P}_i = (\mathfrak{p}, g_i(\alpha))$$

From here, we see that the absolute values extending $|\cdot|_\mathfrak{p}$—that is, which are equivalent to $|\cdot|_\mathfrak{p}$ when restricted from L to K—are precisely those that correspond to the $\mathfrak{P}_i$. The content of the previous proposition says that these are all.

3.16. **Aside: Local-to-Global Principle.** Let me take a moment to point out an important idea lurking in the previous section. We wanted to understand how the field extension $L \mid K$ behaves, where the fields K and L are number fields of sorts. To do this, we passed to completions of either field with respect to some valuation (or absolute value). In a sense, what we have done to understand $L \mid K$ is to pass from the global objects K and L to the local objects manifested by their completions.

To enlighten the terminology a bit more, suppose instead that K and L are function fields: for instance, take K to be $\mathbf{C}(t)$ and L a finite extension of K. Then K could be thought of the regular functions on a Riemann surface and L is some field of algebraic functions, both of which are objects of global nature—they are defined on the whole Riemann surface. Now, passing to the completion corresponds to passing to the fields of power series expansions. Geometrically, this corresponds to focussing our attention on some local part of the Riemann surface. From this local study, we are somehow able to obtain information about the original global objects.

But why do we bother to pass to the local objects in both cases? Well, this is because the local objects are usually easier to handle in some way. In both cases, this at least partially manifests in how it is easier to solve equations with local objects than global objects: as we saw with Hensel's Lemma, equations can be solved via approximation methods. In the context of number theory, we pass to completions with respect to valuations because the arithmetic of complete fields, meaning the ideal structure of the ring of integers, is significantly simpler than that of arbitrary number fields.

3.17. **Classifying Completions of Global Fields.** Finally, the extension theorem above allows us to classify all the completions of number fields. Let K be a number field and let $|\cdot|$ be a nonarchimedean absolute value on K. Restricting this to $\mathbf{Q}$, we clearly obtain a nonarchimedean absolute value on $\mathbf{Q}$. By Ostrowski's Theorem, we know that this comes from a prime $p \in \mathbf{Z}$. If $\mathcal{O}_K$ is the ring of integers of K and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, then the results of the previous section imply that $|\cdot|$ must be equivalent to the absolute value induced by one of the $\mathfrak{p}_i$. This shows that all nonarchimedean absolute values of number fields correspond to a unique prime ideal in the ring of integers.

What about the archimedean absolute values on K? Let $|\cdot|$ be one such absolute value. Restricting to $\mathbf{Q}$, we obtain an archimedean absolute value, from which Ostrowski's Theorem implies it is equivalent to embedding $\mathbf{Q}$ into $\mathbf{C}$ and taking the usual absolute value there. Going back to the extension arguments of the previous section, we see that $\hat{K}$ must be a finite extension of $\mathbf{C}$ (there is an error here; what if $K = \mathbf{Q}$?). Since $\mathbf{C}$ is algebraically closed, $\hat{K} = \mathbf{C}$. This tells us that $|\cdot|$ coincides with the absolute value obtained from an embedding $\sigma : K \hookrightarrow \mathbf{C}$. There are now two cases to consider, depending on whether or not the complex conjugate $\bar{\sigma}$ coincides with σ. If $\bar{\sigma} = \sigma$, then $\sigma(K) \subseteq \mathbf{R}$, in which case we have an absolute value that is distinct from that obtained from other embeddings; if $\bar{\sigma} \neq \sigma$, on the other hand, $\sigma(K)$ is not contained in $\mathbf{R}$ and also the absolute values $|\cdot|_\sigma$ and $|\cdot|_{\bar{\sigma}}$ are easily seen to be equivalent. The theorem of the previous section shows that these are all the archimedean absolute values.

These results will be summarized with the help of some terminology. Let K be a number field. An equivalence class of absolute values on K is called a **prime** or **place** of K.

Theorem 13. *Let K be a number field. Then there exists exactly one prime of K*

(1) for each prime ideal $\mathfrak{p} \subset \mathcal{O}_K$;
(2) for each real embedding $\sigma : K \hookrightarrow \mathbf{R} \subset \mathbf{C}$;
(3) for each conjugate pair of complex embeddings $\bar{\sigma}, \sigma : K \hookrightarrow \mathbf{C}$.

Because primes of K refer to equivalence classes of absolute values, there will be a choice of normalization for each class of primes above. Typical normalizations that we will follow for each class of primes are as follows:

(1) For $|\cdot|_\mathfrak{p}$, $\mathfrak{p}$ an ideal of $\mathcal{O}_K$, set $|x|_\mathfrak{p} := (\mathbf{N}\mathfrak{p})^{-\operatorname{ord}_\mathfrak{p} x}$;
(2) For $|\cdot|_\sigma$, $\sigma : K \hookrightarrow \mathbf{R}$, set $|x|_\sigma := |\sigma(x)|$;
(3) For $|\cdot|_{\bar{\sigma}}$, $\bar{\sigma} \neq \sigma : K \hookrightarrow \mathbf{C}$, set $|x|_{\bar{\sigma}} := |\sigma(x)||\bar{\sigma}(x)| = |\sigma(x)|^2$.

Note that the complex case is not technically an absolute value—if you try proving the triangle inequality, you will fail miserably—but this form is convenient for statements of theorems.

3.18. **Local Fields.** Remember that our whole purpose in all the preceding algebra was to understand a bit more about so-called local fields. Recall that we said a field $(K, |\cdot|)$ is a **local field** if K is complete with respect to the absolute value and has a finite residue field. In case the absolute value is nonarchimedean, this can be characterized by compactness of the ring of integers.

Proposition 14. *Let K be complete with respect to a nonarchimedean absolute value $|\cdot|$ and let A be the ring of integers of K with maximal ideal $\mathfrak{m}$. Then the residue field $k = A/\mathfrak{m}$ is finite if and only if A is compact.*

Proof. Let S be a system of representatives for $A/\mathfrak{m}$, then our goal is to show that S is finite if and only if A is compact. First suppose that A is compact. Since

$$\mathfrak{m} = \{ x \in A \mid |x| < 1 \},$$

we see that $\mathfrak{m}$ is open. Then the sets $s + \mathfrak{m}$ as s ranges over the elements of S form a disjoint open covering of A. Since A is compact, there can only be finitely many sets in this covering, meaning that S is finite.

Conversely, assume that S is finite. Then every element of A can be written as a power series $s_0 + s_1\pi + s_2\pi^2 + \cdots$, where π is a generator for $\mathfrak{m}$ and $s_i \in S$ for all i. Now, for each positive integer n, there are only finitely many distinct elements of the form

$$s_0 + s_1\pi + \cdots + s_n\pi^n.$$

Since $|\cdot|$ is nonarchimedean, every element of A is within $|\pi^{n+1}|$ of this element—i.e. the collection of open balls

$$\{ B(|\pi^{n+1}|, s_0 + s_1\pi + \cdots + s_n\pi^n) \mid s_i \in S \}$$

will be a finite cover of A. Recall from real analysis that this means that A is a totally bounded metric space. Since it is complete with respect to the absolute value, A is also compact. ■

Recall that a closed subspace of a compact space is itself compact. A nice consequence of this elementary topological fact along with the above characterization is that we obtain some very useful compact subspaces of local fields.

Corollary 15. *Let K be a nonarchimedean local field. Then $\mathfrak{p}^n$, $1+\mathfrak{p}^n$ and $A^\times$ are all compact.*

Let me remind you that $\mathfrak{p}$ here refers to the prime which the nonarchimedean absolute value on K corresponds to, viewed as the maximal ideal of the corresponding discrete valuation ring. Since a discrete valuation ring is local, $\mathfrak{p}$ is also the Jacobson radical of the ring. Thus $1+\mathfrak{p}^n \subseteq 1+\mathfrak{p}$ consists of units for all positive integers n.

Recall from our discussion of nonarchimedean absolute values that every element of K can be written in the form $a\pi^n$ for some $a \in A^\times$ and $n \in \mathbf{Z}$. It is then easy to see that every element of K admits a compact neighbourhood: just take a translation of $A^\times$. This means that nonarchimedean local fields can also be characterized as locally compact fields.

Some authors define local fields as fields which are locally compact. The advantage of this is that completions of number fields with respect to archimedean absolute values are also considered local fields. By Ostrowski's Theorem, this is saying that we might want to consider $\mathbf{R}$ and $\mathbf{C}$ as local fields. Besides $\mathbf{R}$ and $\mathbf{C}$, local fields are either finite extensions of the p-adic numbers $\mathbf{Q}_p$ for some prime p or else finite extensions of the field of Laurent series $k((t))$ for some finite field k. The former will be of interest for our study of number theory, whereas the latter will come up when we begin looking at some geometry.

3.19. **Unramified Extensions.** In the study of field extensions, a particularly nice class of extensions are unramified extensions. Roughly speaking, these are field extensions in which the ring of integers of the extension field does not "fold over" anywhere. The point of studying unramified field extensions is that their arithmetic is simpler than general field extensions: somehow, these extensions behave a lot like extensions of finite fields, which are well understood. For reasons such as these, our study of class field theory will begin with unramified field extensions.

For this subsection, let K be a complete field with respect to a discrete absolute value $|\cdot|$. Write k for the residue field of K and let A be the corresponding discrete valuation ring. For an extension field L of K, write l for the residue field and B the corresponding discrete valuation ring.

A finite extension $L \mid K$ is called **unramified** if the extension $l \mid k$ of the residue fields is separable and $[L : K] = [l : k]$. An arbitrary extension is called **unramified** if it is the union of finite unramified subextensions. Note that when L is a possibly infinite extension of K, we define

$$B := \{ x \in L \mid |x| \leqslant 1 \}, \quad \mathfrak{P} := \{ x \in B \mid |x| < 1 \}$$

and define the quotient $B/\mathfrak{P}$ to be the residue field of L. This definition will coincide with taking B as the integral closure of A in L when the extension is finite.

The following result makes precise some of the statements made in the first paragraph.

Proposition 16. *Let L be an algebraic extension of K. The map $K' \mapsto k'$ sending an unramified extension $L \mid K' \mid K$ to its residue field k' is a one-to-one correspondence between the sets*

$$\{ K' \subseteq L, \textit{finite and unramified over } K \} \leftrightarrow \{ k' \subseteq l, \textit{finite over } k \}.$$

Moreover, if $K' \leftrightarrow k'$ and $K'' \leftrightarrow k''$, then:

(1) $K' \subseteq K''$ if and only if $k' \subseteq k''$;

(2) K' is Galois over K if and only if k' is Galois over k, in which case there is a canonical isomorphism $\mathrm{Gal}(K' \mid K) \to \mathrm{Gal}(k' \mid k)$.

Proof. See Milne ANT Proposition 7.50. ■

An important step in the proof of this proposition is to show that the compositum of two unramified extensions is itself unramified.

Lemma 17. *Suppose* $K' \mid K$ *and* $K'' \mid K$ *are two unramified extensions of* K *contained in* L*. Then the compositum* $K'K'' \mid K$ *is an unramified extension of* K *in* L*.*

Proof. From global theory, we know that a prime ramifies in an extension if and only if the prime divides the discriminant of the extension (cf. Milne ANT Theorem 3.20). Since $K' \mid K$ and $K'' \mid K$, the prime $\mathfrak{p}$ of K does not divide the discriminants $\Delta_{K'}$ and $\Delta_{K''}$. But we also have

$$\Delta_{K'K''} = \Delta_{K'}^{[K':K]} \Delta_{K''}^{[K'':K]},$$

(cf. Milne ANT Remark 6.6c). Since $\mathfrak{p}$ does not divide the right hand side, $\mathfrak{p}$ cannot divide $\Delta_{K'K''}$, implying that $K'K''$ is an unramified extension of K. Since the elements of $K'K''$ are linear combinations of all products of elements in K' and K'', it is clear that $K'K'' \subseteq L$. ■

This lemma allows us to apply Zorn's Lemma to find that there is always a **largest unramified extension** K_0 of K contained in L, which contains all other unramified extensions of K. In fact, more can be said when k is finite. All finite extensions of a finite field can be obtained by adjoining roots of unity prime with degree prime to the characteristic of k. Thus, in case that k is finite, K_0 is obtained by adjoining all such roots of unity contained in l.

Not surprisingly, the most important choice for L is the algebraic closure K^{al} of K.

Corollary 18. *Assume both* K *and* k *are perfect. The residue field of* K^{al} *is* k^{al}*; there is a subfield* K^{un} *of* K^{al} *such that a subfield* L *of* K^{al}*, finite over* K*, is unramified if and only if* $L \subseteq K^{un}$*.*

Proof. Let $f_0(x) \in k[x]$ be any polynomial and let $f(x) \in A[x]$ be any lift of $f_0(x)$. Then K^{al} contains all the roots of f and hence the residue field k' of K^{al} contains all the roots of $f_0(x)$. Thus k' is algebraic over k and every polynomial over k splits in k', so $k' = k^{al}$. The field K^{un} is the largest unramified extension of K contained in K^{al}. ■

Since all finite extensions of K will be contained in the algebraic closure of K, the above result gives a sort of absolute property to the correspondence between finite, unramified extensions of K and finite extensions of k. More precisely, we have:

Corollary 19. *Assume* K *and* k *are perfect fields. Then there is an equivalence of categories between the category of finite, unramified extensions of* K *and the finite extensions of* k*.*

As mentioned in the opening of this section, this equivalence of categories will be important for us because it relates the extensions of our local fields with extensions of finite fields. One particularly useful property is that this gives the existence of an element analogous to the Frobenius element in the Galois group of finite extensions of local fields.

More precisely, let K be a local field and let q be the order of the residue field k of K. For each positive integer n, there is a unique, up to k-isomorphism, field extension $k_n \mid k$ of degree n. Recall that the Galois group $\mathrm{Gal}(k_n \mid k)$ is cyclic of order n and has a canonical generator $x \mapsto x^q$ called the **Frobenius element**. By the above equivalence of categories and the relation between the Galois groups, we see that for each positive integer n, there is an unramified extension $K_n \mid K$ of degree n which unique up to K-isomorphism. Moreover, the Galois group $\mathrm{Gal}(K_n \mid K)$ is cyclic of order n and has a canonical generator, which is also known as the **Frobenius element**, characterized by the property

$$\sigma(\beta) = \beta^q \pmod{\mathfrak{p}}$$

for all $\beta \in B$, where B is the discrete valuation ring of K_n and $\mathfrak{p}$ is the prime of K.

3.20. **Two More Local Results.** There are two more theorems that are typically covered in the local theory. Unfortunately, these results seem very unmotivated at first. This is because the power of these theorems only comes about when trying to go from the local objects to the global objects. Specifically, the forthcoming theorems become important when we discuss idèles.

The first of these results is the so-called *Weak Approximation Theorem*. Roughly it says that different absolute values are essentially independent. When looking at the statement, keep the Chinese Remainder Theorem in mind: think of absolute values in terms of their valuations and thus in connection with primes and think of the approximations as finding an element in some power of the ideal.

Theorem 20 (Weak Approximation Theorem)**.** *Let $|\cdot|_1, \dots, |\cdot|_n$ be nontrivial inequivalent absolute values on a field K, and let $a_1, \dots, a_n \in K$. For every $\epsilon > 0$, there is an element $a \in K$ such that $|a - a_i|_i < \epsilon$ for each $i = 1, \dots, n$.*

Proof. See Milne ANT Theorem 7.20 and Neukirch Chapter II Theorem 3.4. ■

The Weak Approximation Theorem will help us show that a certain map defined from the idèle class group is surjective.

If we think of the Weak Approximation Theorem as stating some independence condition on any finite set of inequivalent absolute values, the *Product Formula* can be thought of as saying there is a nontrivial relation when all the absolute values are considered together. We shall state this in two parts: first we state it for $\mathbf{Q}$ and then for an arbitrary number field.

Theorem 21 (Product Formula)**.** *For $p = 2, 3, 5, 7, 11, 13, \dots, \infty$ let $|\cdot|_p$ denote the corresponding normalized absolute value on $\mathbf{Q}$. Then for any $0 \neq x \in \mathbf{Q}$,*

$$\prod_p |x|_p = 1.$$

Proof. Let $x = \frac{a}{b}$ for $a, b \in \mathbf{Q}$. Now recall the definition of $|\alpha|_p$: this will be p^{-n}, where n is the order α_p to which p divides a minus the order β_p to which p divides b. Thus $|x|_p = 1$ unless $p \mid a$ or $p \mid b$. Note this shows that the product is finite and thus makes sense. Now we compute:

$$\prod_p |x| = \left(\prod_{p \mid a} \frac{1}{p^{\alpha_p}} \right) \left(\prod_{q \mid b} q^{\beta_p} \right) \left| \frac{a}{b} \right|_\infty = \frac{1}{a} \cdot b \cdot \frac{a}{b} = 1.$$ ■

An analogous result holds for general number fields. The proof of the general case is done by using the formula for extensions of absolute values and the product formula for $\mathbf{Q}$.

Theorem 22 (Product Formula)**.** *For each prime ν, let $|\cdot|_\nu$ be the normalized absolute value corresponding to ν. Then for every $0 \neq x \in K$,*

$$\prod_\nu |x|_\nu = 1.$$

Before leaving off, let me mention that the product formula may be used as an axiom for global fields. This axiomatization was achieved by Artin and Whaples in 1945. Let K be a field with a set of primes $\mathfrak{V}$ satisfying the following two axioms:

(1) There is a set of representatives $|\cdot|_\nu$ for the primes such that, for any nonzero $x \in K$, $|x|_\nu \neq 1$ for only finitely many $\nu \in \mathfrak{V}$ and
$$\prod_{\nu \in \mathfrak{V}} |x|_\nu = 1.$$
(2) There exists at least one prime $\nu \in \mathfrak{V}$ for which K_ν is a local field.

Then K is a global field and $\mathfrak{V}$ consists of all primes of K.