LOCAL FIELDS AND p-ADIC GROUPS

MATH 519

In these notes, we follow [N, Chapter II] most, but we also use parts of [FT, L, RV, S].

1. Absolute values

Let K be a field. An *absolute value* on K is a function

$$|\cdot|_v : K \longrightarrow \mathbb{R}$$

such that

(1) For every $x \in K$, we have $|x|_v \geq 0$, and $|x|_v = 0$ if and only if $x = 0$.
(2) For all $x, y \in K$, we have $|xy|_v = |x|_v|y|_v$.
(3) For all $x, y \in K$, we have $|x + y|_v \leq |x|_v + |y|_v$.

Condition (3) is the triangle inequality. The following stronger condition is called the *ultrametric* triangle inequality.

(3*) For all $x, y \in K$, we have $|x + y|_v \leq \max(|x|_v, |y|_v)$.

If the function $|\cdot|_v$ satisfies the ulatrametric triangle inequality, then it is called a *non-archimedean* absolute value, and is otherwise called an *archimedean* absolute value.

We always have the *trivial* absolute value on any field K, defined by $|x|_v = 1$ for every nonzero $x \in K$. In these notes, we will eliminate the trivial absolute value from discussion, and an absolute value will always assumed to be nontrivial.

Example 1. Consider the field $\mathbb{Q}$ of rational numbers. There is the typical absolute value $|\cdot|$, which we will also denote by $|\cdot|_\infty$, which is an archimedean absolute value. For an example of a non-archimedean absolute value, fix a prime number p, and define an absolute value $|\cdot|_p$ on $\mathbb{Q}$ as follows. For a nonzero rational number $m/n \in \mathbb{Q}$, write m/n as $m/n = p^r(a/b)$, where r is an integer, and p does not divide a or b. Now define $|m/n|_p = p^{-r}$ (and $|0|_p = 0$). By considering divisibility of powers of p, it is apparent that $|\cdot|_p$ is a non-archimedean absolute value. It is called the *p-adic* absolute value on $\mathbb{Q}$. Note that the values of the p-adic value are bounded by 1 on $\mathbb{Z}$.

In the above example, we have a non-archimedean absolute value on $\mathbb{Q}$ which is bounded on $\mathbb{Z}$. It turns out that this is always the case.

Proposition 1.1. *Let K be a field, let $R = \{n \cdot 1 \mid n \in \mathbb{Z}\} \subset K$, and let $|\cdot|_v$ be an absolute value on K. Then $|\cdot|_v$ is non-archimedean if and only if the set of values that it takes on R is bounded.*

Proof. First assume that $|\cdot|_v$ is non-archimedean. Then by the ultrametric triangle inequality, for any $n \in \mathbb{Z}$, we have $|n \cdot 1|_v \leq |1|_v = 1$. Therefore the values of $|\cdot|_v$ on R are bounded by 1.

Coversely, suppose that $|x|_v \leq C$ for any $x \in R$. For any positive integer m, and any $x, y \in K$, then the Binomial Theorem and triangle inequality give

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

Now, we have $|x|_v^i |y|_v^{m-i} \leq (\max(|x|_v, |y|_v))^m$, and so for any positive integer m we have

$$|x+y|_v \leq (C(m+1))^{1/m} \max(|x|_v, |y|_v).$$

Since $\lim_{m\to\infty}(C(1+m))^{1/m} = 1$, it follows that the ultrametric triangle inequality must hold, and $|\cdot|_v$ is non-archimedean. □

Corollary 1.1. *Let K be a field which has an archimedean absolute value $|\cdot|_v$. Then K has characteristic 0.*

Proof. If K has characteristic $p \neq 0$, then $R = \{n \cdot 1 \mid n \in \mathbb{Z}\}$ is finite, and so $|\cdot|_v$ is bounded on R. Thus by Proposition 1.1, $|\cdot|_v$ must be non-archimedean. □

An absolute value on a field K defines a metric, and we may thus consider the metric topology on K induced by an absolute value. We remark here that any absolute value on K is a continuous function $|\cdot|_v : K \to \mathbb{R}$, which can be seen as follows. Let $\{x_n\}$ be a sequence in K which converges to $x \in K$ with respect to $|\cdot|_v$, so that $|x_n - x|_v \to 0$ as $n \to \infty$. Then $\big||x_n|_v - |x|_v\big| \leq |x_n - x|_v$ by the triangle inequality, and so $|x_n|_v \to |x|_v$ as $n \to \infty$.

In Example 1, it may be checked that the absolute values on $\mathbb{Q}$ turn it into a topological field, that is, addition, multiplication, and the additive and multiplicative inverse maps are all continuous when we give $\mathbb{Q}$ these topologies. In fact, we have the following.

Proposition 1.2. *Let K be a field, and $|\cdot|_v$ an absolute value on K. If K is given the metric topology induced by $|\cdot|_v$, then K is a topological field.*

Proof. See Problem set 2. □

Call two absolute values $|\cdot|_1$ and $|\cdot|_2$ on K *equivalent* if they induce the same topology on K. Recall that two metrics induce the same topology if and only if any open ball centered at any point in one metric contains an open ball centered at the same point of the other metric, and vice versa. Because we are dealing with a metric spaces which are also fields, it is enough to check this condition for open balls centered at 0. Note also that if two absolute values on K are equivalent, then sequences in K converge to 0 simultaneously with respect to each absolute value (Exercise). We have the following criterion for when two absolute values are equivalent.

Lemma 1.1. *Let K be a field with two absolute values $|\cdot|_1$ and $|\cdot|_2$. Then $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there is some $\lambda > 0$ such that*

$$|x|_1 = |x|_2^{\lambda} \quad \text{for all } x \in K.$$

Proof. First, if $|\cdot|_1 = |\cdot|_2^{\lambda}$ for some $\lambda > 0$, then open balls around 0 with respect to one absolute value may be contained in the other, and so the absolute values are equivalent.

Conversely, suppose $|\cdot|_1$ and $|\cdot|_2$ are equivalent. For any $x \in K$, $i = 1, 2$, note that $|x|_i < 1$ is equivalent to the sequence $\{x^n\}_{n=1}^{\infty}$ converging to 0 with respect to $|\cdot|_i$. Since we are assuming the two absolute values are equivalent, sequences converges to 0 in each absolute value simultaneously, and so for any $x \in K$, $|x|_1 < 1$ if and only if $|x|_2 < 1$.

Now let $y \in K$ such that $|y|_1 > 1$, which we know exists since these absolute values are non-trivial. Let $x \in K$, $x \neq 0$. Then for some $\alpha \in \mathbb{R}$, we have $|x|_1 = |y|_1^\alpha$. Let $a, b \in \mathbb{Z}$ such that $a/b > \alpha$ and $b > 0$. Then we have $|x|_1 = |y|_1^\alpha < |y|_1^{a/b}$. We may then conclude the following:

$$|x^b/y^a|_1 < 1 \Rightarrow |x^b/y^a|_2 < 1 \Rightarrow |x|_2 < |y|_2^{a/b}.$$

Since $a/b > \alpha$ was arbitrary, then we have $|x|_2 \leq |y|_2^\alpha$. Now let $m, n \in \mathbb{Z}$ such that $m/n < \alpha$ with $n > 0$, so that $|x|_1 > |y|_1^{m/n}$. Then by the parallel argument as before, we conclude that $|x|_2 \geq |y|_2^\alpha$. So now $|x|_2 = |y|_2^\alpha$. Note that $|x|_1 = 1$ if and only if $\alpha = 0$, if and only if $|x|_2 = 1$, in which case $|x|_1$ is $|x|_2$ to any positive power. Now, $x \in K$, $x \neq 0$ was arbitrary while y was fixed. For $i = 1, 2$ we have $\log |x|_i = \alpha \log |y|_i$, for some α depending on x. For any $x \neq 0$, $|x|_i \neq 1$, we have

$$\frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2}.$$

Defining the constant $\lambda = (\log |y|_1)/(\log |y|_2)$, we have $\lambda > 0$ since $|y|_i > 1$ for $i = 1, 2$, and $|x|_1 = |x|_2^\lambda$ for every $x \in K$. □

It follows immediately from Lemma 1.1 that the p-adic absulute values $|\cdot|_p$ on $\mathbb{Q}$ are all inequivalent for different primes p, and they are each inequivalent to the archimedean absolute value $|\cdot|_\infty$. In fact, we now show that every absolute value on $\mathbb{Q}$ is equivalent to one of these.

Theorem 1.1 (Ostrowski)**.** *Every absolute value on $\mathbb{Q}$ is equivalent to either the archimedean absolute value $|\cdot|_\infty$, or a p-adic absolute value $|\cdot|_p$ for some prime p.*

Proof. Let $|\cdot|_v$ be an absolute value on $\mathbb{Q}$. First suppose that $|\cdot|_v$ is non-archimedean, so that $|n|_v \leq 1$ for every $n \in \mathbb{Z}$. By multiplicativity of absolute values, there must be some prime number p such that $|p|_v < 1$, otherwise $|\cdot|_v$ would be trivial. Now consider the set

$$I = \{x \in \mathbb{Z} \mid |x|_v < 1\}.$$

Then I is an ideal of $\mathbb{Z}$ such that $p\mathbb{Z} \subset I \neq \mathbb{Z}$, and so $I = p\mathbb{Z}$ since $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. Now let $a \in \mathbb{Z}$, and write $a = bp^m$ such that $p \nmid b$, so $b \notin I$. Then $|b|_v = 1$, and we have $|a|_v = |p|_v^m$. If we let $\lambda = -(\log |p|_v)/(\log p)$, then we have $|a|_v = |a|_p^\lambda$. Since $a \in \mathbb{Z}$ was arbitary, then by multiplicativity we have $|y|_v = |y|_p^\lambda$ for every $y \in \mathbb{Q}$, and so $|\cdot|_v$ is equivalent to $|\cdot|_p$ by Lemma 1.1.

Now suppose that $|\cdot|_v$ is archimedean. By the triangle inequality, we have $|a|_v \leq a$ for any positive integer a. Let $m, n > 1$ be arbitrary positive integers bigger than 1. Now, we may write $m = \sum_{i=0}^r a_i n^i$, where $0 \leq a_i \leq n - 1$ for each i and $n^r \leq m$. So, we have $r \leq (\log m)/(\log n)$, and $|a_i|_v \leq a_i \leq n$ for each i. This yields the inequalities

$$|m|_v \leq \sum_{i=0}^r |a_i|_v |n|_v^i \leq \sum_{i=0}^r |a_i|_v |n|_v^r \leq \left(1 + \frac{\log m}{\log n}\right) n \, |n|_v^{\log m / \log n}.$$

We have this inequality for any integers $m, n > 1$, and so we may replace m by m^k for any positive integer k. After this substitution, and raising each side to the $(1/k)$ power, we obtain

$$|m|_v \leq \left(n + nk \frac{\log m}{\log n}\right)^{1/k} |n|_v^{\log m / \log n}.$$

Taking the limit as $k \to \infty$, the coefficient on the right side goes to 1, and we obtain

$$|m|_v^{1/\log m} \leq |n|_v^{1/\log n}, \quad \text{and so} \quad |m|_v^{1/\log m} = |n|_v^{1/\log n},$$

since m and n may switch roles, because they were taken to be arbitrary.

Now let $c = |n|_v^{1/\log n}$, which is a constant for any integer $n > 1$. Letting $\lambda = \log c$, we have $\lambda = (\log |n|_v)/(\log n)$ for any integer $n > 1$, and so $|n|_v = e^{\lambda \log n} = |n|_\infty^\lambda$ for any positive integer n. It follows from multiplicativity that $|y|_v = |y|_\infty^\lambda$ for any $y \in \mathbb{Q}$, and so $|\cdot|_v$ is equivalent to $|\cdot|_\infty$ by Lemma 1.1. □

2. Completions

A field F with an absolute value $|\cdot|_v$ is called *complete* if every Cauchy sequence in F with respect to $|\cdot|_v$ converges to an element in F. If a field F is not complete with respect to $|\cdot|_v$, one may construct the *completion* of F, which we describe now. This notion is familiar from analysis, and in fact the construction exactly parallels the classical construction of $\mathbb{R}$ from $\mathbb{Q}$ with respect to the archimedean absolute value $|\cdot|_\infty$, and so we just outline the construction.

First, the set of all Cauchy sequences in F form a ring R under pointwise addition and multiplication, the multiplicative identity in which is the sequence consisting of all 1's. The sequences in R which converge to 0 form an ideal in R, call it $\mathfrak{m}$. Given any Cauchy sequence $\{a_n\}$ in R which is not in $\mathfrak{m}$, one may find another Cauchy sequence $\{b_n\}$ in R such that the product of these sequences, $\{a_n b_n\}$, differs from the sequence of all 1's by an element in $\mathfrak{m}$. In other words, $\mathfrak{m}$ is a maximal ideal in R, and so $\hat{F} = R/\mathfrak{m}$ is a field. We may view F as embedded in $\hat{F}$ by mapping $a \in F$ to the coset of $\mathfrak{m}$ in $\hat{F}$ represented by the sequence consisting of all a's. The field $\hat{F}$ is the *completion* of F with respect to $|\cdot|_v$. If $\overline{\{a_n\}} = \{a_n\} + \mathfrak{m}$ is an element of $\hat{F}$, we may define its absolute value by

$$|\overline{\{a_n\}}|_v' = \lim_{n\to\infty} |a_n|_v,$$

which is well-defined since $\big||a_n|_v - |a_m|_v\big| \leq |a_n - a_m|_v$. In fact, $|\cdot|_v'$ defines an absolute value on $\hat{F}$ which extends the absolute value $|\cdot|_v$ when viewing F as embedded in $\hat{F}$. We summarize the properties of the completion of F below, a detailed proof of which may be found in [FT, Section II.3].

Theorem 2.1. *Let F be a field with absolute value $|\cdot|_v$, and let $\hat{F}$ and $|\cdot|_v'$ be as described above, in which F is embedded. Then $|\cdot|_v'$ is an absolute value on $\hat{F}$ which extends $|\cdot|_v$, and $\hat{F}$ is a complete field with respect to $|\cdot|_v'$ in which F is dense. If K with $|\cdot|_w$ is any other complete field which contains F as a dense subfield, and such that $|\cdot|_w$ extends $|\cdot|_v$, then $\hat{F}$ and K are isomorphic as topological fields.*

Example 2. We have already mentioned the example of $\mathbb{R}$ being the completion of $\mathbb{Q}$ with respect to the absolute value $|\cdot|_\infty$. Similarly, consider the field $\mathbb{Q}(i)$ with the absolute value $|z|_\infty = \sqrt{z\bar{z}}$, where $\bar{z}$ is complex conjugation. Then the completion of $\mathbb{Q}(i)$ with respect to this absolute value is the complex field $\mathbb{C}$, with the usual absolute value. Note that the usual absolute value on $\mathbb{C}$ extends that of $\mathbb{R}$, and in fact, it is the only absolute value on $\mathbb{C}$ which does so (Exercise). As we see below, these are essentially the only archimedean examples of complete fields.

Theorem 2.2 (Ostrowski)**.** *Let F be a field which is complete with respect to an archimedean absolute value $|\cdot|_v$. Then F is isomorphic as a topological field to either $\mathbb{R}$ or $\mathbb{C}$, with their usual archimedean absolute values.*

Proof. From Corollary 1.1, we know that F has characteristic zero, and so we may assume that $\mathbb{Q} \subset F$. When restricting to $|\cdot|_v$ to $\mathbb{Q}$, we must have a non-trivial absolute value, otherwise $|\cdot|_v$ would be bounded on $\mathbb{Z}$, and by Proposition 1.1 would be non-archimedean. By Theorem 1.1, we must have that $|\cdot|_v$ on $\mathbb{Q}$ is equivalent to the archimedean absolute value $|\cdot|_\infty$. We may then replace $|\cdot|_v$ by an equivalent absolute value, without loss of generality, so that $|\cdot|_v$ retricts to $|\cdot|_\infty$ on $\mathbb{Q}$. Since F is complete, we may assume that $\mathbb{R} \subset F$. If we show that any element of F satisfies a quadratic equation over $\mathbb{R}$, then we would have $F = \mathbb{R}$ or $\mathbb{C}$ as a field, and since the only way to extend the archimedean absolute value on $\mathbb{R}$ to $\mathbb{C}$ is with the usual archimedean absolute value on $\mathbb{C}$ (as in Example 2), the result would follow.

Let $\alpha \in K$. Consider the function $f : \mathbb{C} \to \mathbb{R}$ defined by

$$f(z) = |\alpha^2 - (z + \bar{z})\alpha + z\bar{z}|_v.$$

Now, f is continuous, and $f(z) \to \infty$ as $|z|_\infty \to \infty$, and so $f(z)$ takes some absolute minimum m. The goal is to show that $m = 0$, in which case α is the zero of a quadratic over $\mathbb{R}$. Letting $S = \{z \in \mathbb{C} \,|\, f(z) = m\}$, we see that S is closed since f is continuous, and is bounded since $f(z) \to \infty$ as $|z|_\infty \to \infty$. Since S is then compact, it follows from the continuity of $|\cdot|_\infty$ on $\mathbb{C}$ that there is an element $z_0 \in S$ such that $|z_0|_\infty \geq |z|_\infty$ for any $z \in S$.

Suppose that $m > 0$. Choose ε such that $0 < \varepsilon < m$, and consider the quadratic polynomial over $\mathbb{R}$ defined as

$$g(x) = x^2 - (z_0 + \bar{z}_0)x + z_0\bar{z}_0 + \varepsilon,$$

and suppose that $z_1, \bar{z}_1 \in \mathbb{C}$ are the roots of $g(x)$. Then $z_1\bar{z}_1 = z_0\bar{z}_0 + \varepsilon$, and so $|z_1|_\infty > |z_0|_\infty$. By choice of z_0, we must have $f(z_1) > m$.

For any positive integer n, consider the polynomial

$$G_n(x) = (g(x) - \varepsilon)^n - (-\varepsilon)^n,$$

so that $G_n(z_1) = 0$ since $g(x)$ is a factor of $G_n(x)$. Let $z_1 = w_1, w_2, \ldots, w_{2n}$ be the zeros of $G_n(x)$ in $\mathbb{C}$. Since this set of zeros is the same as the set of its conjugates, we have

$$G_n(x) = \prod_{i=1}^{2n}(x - w_i) = \prod_{i=1}^{2n}(x - \bar{w}_i), \quad \text{and} \quad G_n(x)^2 = \prod_{i=1}^{2n}(x^2 - (w_i + \bar{w}_i)x + w_i\bar{w}_i).$$

Substituting α into the polynomial $G(x)_n^2$ and applying the absolute value $|\cdot|_v$, we obtain

$$|G_n(\alpha)|_v^2 = \prod_{i=1}^{2n} f(w_i) \geq f(z_1)m^{2n-1}.$$

But we also have, from the definition of $G_n(x)$ and the triangle inequality,

$$|G_n(\alpha)|_v^2 \leq (f(z_0)^n + \varepsilon^n)^2 = (m^n + \varepsilon^n)^2,$$

since $|g(\alpha) - \varepsilon|_\infty = f(z_0)$. So, $f(z_1)m^{2n-1} \leq (m^n + \varepsilon^n)^2$, which gives

$$\frac{f(z_1)}{m} \leq \left(1 + \left(\frac{\varepsilon}{m}\right)^n\right)^2.$$

Since $\varepsilon < m$, and n was an arbitrary positive integer, letting $n \to \infty$ gives $f(z_1) \leq m$, contradicting $f(z_1) > m$. Thus $m = 0$. □

Example 3. Since Theorem 2.1 takes care of all fields which are complete with respect to an archimedean absolute value, the next case is to consider a non-archimedean absolute value. Since $\mathbb{Q}$ has the p-adic absolute values, we may complete $\mathbb{Q}$ with respect to one of them. The resulting field is denoted $\mathbb{Q}_p$, and is called the field of *p-adic rationals*. We will study these types of fields in detail in the next section.

3. Non-archimedean local fields

Let F be a field with absolute value $|\cdot|_v$. Since $|\cdot|_v$ is not trivial, there is some $x \in F$ such that $|x|_v > 1$. By multiplicativity, $|x^n|_v$ is unbounded as $n \to \infty$. So, the image of F under $|\cdot|_v$ is not bounded above in $\mathbb{R}$, and so cannot be compact in $\mathbb{R}$. Since $|\cdot|_v$ is continuous, then F cannot be compact with this topology.

So, when studying the topology of fields with an absolute value, the most we can hope for is local compactness, such as is the case of $\mathbb{R}$ with the archimedean absolute value. We have the following basic properties of a field which is locally compact with respect to an absolute value.

Lemma 3.1. *Let F be a field with an absolute value $|\cdot|_v$. Suppose that F is locally compact with the topology given by $|\cdot|_v$. Then:*

1. *For any $r > 0$, the set $D_r = \{x \in F \mid |x|_v \leq r\}$ is compact.*
2. *The image of $F^\times$ under $|\cdot|_v$ is a closed subgroup Γ of $\mathbb{R}^\times$.*
3. *The map $|\cdot|_v$ is an open map onto Γ.*

Proof. (1): It is enough to prove the statement for $r \geq 1$, since for any positive $s < 1$, D_s is closed and $D_s \subset D_1$, making D_s compact. If $r \geq 1$, let V be a compact neighborhood of 0 such that $V \subset D_r$, which exists since F is a locally compact Hausdorff space. Since V is a neighborhood of 0, then there is an $\varepsilon > 0$ such that $D_\varepsilon \subset V$, and then D_ε is compact since it is closed and V is compact. Now let $y \in D_\varepsilon$ such that $|y|_v < \varepsilon/r$ and $y \neq 0$. Then the set $y^{-1}D_\varepsilon$ is a compact set containing 0, by continuity of multiplication. Also, if $x \in D_r$, then $x = y^{-1}(yx)$, and $|yx|_v = |y|_v|x|_v < (\varepsilon/r)(r) = \varepsilon$, and so $D_r \subset y^{-1}D_\varepsilon$. Now D_r is a closed subset of a compact set, and so D_r is compact.

(2): Let Γ be the image of $F^\times$ in $\mathbb{R}^\times$ under $|\cdot|_v$, which is a subgroup since $|\cdot|_v$ is a multiplicative homomorphism. Let $\{a_n\}$ be a sequence in Γ which converges to some point $a \in \mathbb{R}^\times$, and let $a_n = |x_n|_v$, for $x_n \in F^\times$. Now, since

$$\big||x_n|_v - a\big| \to 0 \quad \text{as} \quad n \to \infty,$$

then the values $|x_n|_v$ are bounded, and so for some $r > 0$ and some integer $N > 0$, $x_n \in D_r$ for every $n \geq N$. Since D_r is compact in F by (1), then $D_r \setminus \{0\}$ is compact in $F^\times$, and its image C under $|\cdot|_v$ is compact in $\mathbb{R}^\times$, and so closed in $\mathbb{R}^\times$. Now a is a limit point of C, while C is closed, and so $a \in C \subset \Gamma$. Thus Γ is closed.

(3): Let $U \subset F^\times$ be open, and let $V \subset \Gamma$ be the image of U in $\mathbb{R}^\times$ under $|\cdot|_v$. To show that V is open, it is enough to show that given any $a \in V$, and any sequence $\{a_n\}$ in Γ which converges to a, there is a subsequence of $\{a_n\}$ which eventually is contained in V (otherwise there is a point in V all of whose neighborhoods are not contained in V). Taking such a point $a \in V$ and sequence $\{a_n\}$ in Γ, we know that $a \in \Gamma$ since Γ is closed by (2), so let $a = |x|_v$ for some $x \in U$. Now, there is a sequence $\{x_n\}$ in $F^\times$ such that

$|x_n|_v = a_n$ for each n, and since $|x_n|_v$ converges, then as in the proof of (2), there is some $r > 0$ and some integer $N > 0$ such that $x_n \in D_r$ for every $n \geq N$. Since D_r is compact, then there is some subsequence $\{x_{n_j}\}$ of $\{x_n\}$ which converges to some $z \in F^\times$. Since $|\cdot|_v$ is continuous, then we must have $|z|_v = a$. Now let $S^1 = \{y \in F^\times \mid |y|_v = 1\}$, which is the kernel of the multiplicative homomorphism $|\cdot|_v$. Since $|x|_v = |z|_v$, then we have $z \in xS^1 \subset US^1$. Since U is open, then US^1 is open, and since $z \in US^1$ and $\{x_{n_j}\}$ is a sequence in $F^\times$ converges to z, then eventually all of the terms of the sequence $\{x_{n_j}\}$ are in US^1. The image of U is the same as the image of US^1 under $|\cdot|_v$, and so the terms of the subsequence $\{a_{n_j}\}$ of $\{a_n\}$, where $a_{n_j} = |x_{n_j}|_v$, eventually are all in V. □

From Theorem 2.1, we see that any field with an archimedean absolute value may be embedded topologically as a subfield of $\mathbb{C}$ with the usual absolute value, so we now concentrate on fields with non-archimedean absolute values, dropping the assumption that the field is locally compact for the moment. If F is a field with non-archimedean absolute value $|\cdot|_v$, let

$$\mathcal{O} = \{x \in F \mid |x|_v \leq 1\}, \quad \text{and} \quad \mathfrak{p} = \{x \in F \mid |x|_v < 1\}.$$

We have the following.

Proposition 3.1. *Let F be a field with a non-archimedean absolute value, and let $\mathcal{O}$ and $\mathfrak{p}$ be as above. The set $\mathcal{O} \subset F$ is a ring, with group of units*

$$\mathcal{O}^\times = \{x \in F \mid |x|_v = 1\},$$

and $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}$.

Proof. It follows immediately from the ultrametric triangle inequality and multiplicativity of absolute values that $\mathcal{O}$ is a ring and $\mathfrak{p}$ is an ideal of $\mathcal{O}$. The statement that the units of $\mathcal{O}$ are exactly those elements with absolute value 1 follows from the fact that $|x^{-1}|_v = |x|_v^{-1}$, and since the elements of $\mathfrak{p}$ are exactly the non-units of $\mathcal{O}$, then it is the unique maximal ideal of $\mathcal{O}$. □

Call $\mathcal{O}$ the *ring of integers* of F. Since $\mathcal{O}$ is a ring and $\mathfrak{p}$ is a maximal ideal, then $\mathcal{O}/\mathfrak{p}$ is a field, called the *residue field* of F. An absolute value $|\cdot|_v$ on F is called *discrete* if the image of $F^\times$ under $|\cdot|_v$ is discrete in $\mathbb{R}^\times$. If we assume that a field with a non-archimedean absolute value is locally compact, then the absolute value is automatically discrete, as we see now.

Proposition 3.2. *Let F be a field which is locally compact with respect to a non-archimedean absolute value $|\cdot|_v$. Then the image Γ of $F^\times$ under $|\cdot|_v$ is discrete in $\mathbb{R}^\times$.*

Proof. First, $1 + \mathfrak{p}$ is an open set in $F^\times$ containing 1, and for every $y \in 1 + \mathfrak{p}$, $|y|_v \leq 1$ since $|\cdot|_v$ is non-archimedean. If Γ is the image of $F^\times$ in $\mathbb{R}^\times$ under $|\cdot|_v$, then by part (3) of Lemma 3.1, $|\cdot|_v$ maps $1 + \mathfrak{p}$ onto an open subset V of Γ, which must satisfy $V \subset [0, 1]$. So, V is the intersection of an open subset of $\mathbb{R}$ with Γ, and so there is an open interval containing 1 in $\mathbb{R}$ whose intersection with Γ is contained in $[0, 1]$. If the intersection of such an open interval with Γ is the singleton $\{1\}$, then Γ is discrete by homogeneity. If this is not the case, there is a sequence $\{a_n\}$ in $F^\times$ such that $|a_n|_v$ gets arbitrarily close to 1, while less than 1, since the intersection of the open interval with Γ is contained in $[0, 1]$. However, this would mean $|a_n^{-1}|_v$ would get arbitrarily close to 1, while greater than 1, meaning the intersection of the open interval with Γ would have to have elements greater than 1, a contradiction. Thus Γ is discrete. □

We now assume that F is a field with a discrete non-archimedean absolute value $|\cdot|_v$, so by Proposition 3.2, this is the situation if F is locally compact with respect to $|\cdot|_v$. In particular, this means that $|\cdot|_v$ takes some largest positive value less than 1, say β. Then the values in the image of $F^\times$ under $|\cdot|_v$ must be exactly $\{\beta^m \mid m \in \mathbb{Z}\}$, otherwise we could get a value larger than β and smaller than 1 (Exercise). In this case, if $\pi \in F$ is an element such that $|\pi|_v = \beta$, then π is called a *uniformizer* (or a *uniformizing parameter*). Note that we then have

$$\mathfrak{p} = \{x \in F \mid |x|_v < 1\} = \{x \in F \mid |x|_v \leq \beta\}.$$

Proposition 3.3. *Let F be a field with a discrete non-archimedean absolute value $|\cdot|_v$, with π a uniformizer and $|\pi|_v = \beta$. Then:*

(1) *Every element $x \in F^\times$ can be written uniquely as $x = u\pi^m$, for $u \in \mathcal{O}^\times$ and $m \in \mathbb{Z}$.*
(2) *The ring $\mathcal{O}$ is a principal ideal domain, and the nonzero ideals of $\mathcal{O}$ are exactly*
$$\mathfrak{p}^n = \pi^n\mathcal{O} = \{x \in F \mid |x|_v \leq \beta^n\}, \quad n \geq 0.$$
(3) *For each $n \geq 0$, we have $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$.*

Proof. (1): Let $x \in F^\times$, then $|x|_v = \beta^m$ for some $m \in \mathbb{Z}$. Then we have $|x\pi^{-m}|_v = 1$, so $x\pi^{-m} = u \in \mathcal{O}^\times$, and $x = u\pi^m$. Uniqueness is immediate.

(2): Let I be a nonzero ideal of $\mathcal{O}$, and let $x \in I$ with $|x|_v = \beta^n$ such that n is minimal. Then $x = u\pi^n$ with $u \in \mathcal{O}^\times$, and $\pi^n\mathcal{O} \subset I$. If $y \in I$ is any other nonzero element of I, with $y = v\pi^m$, $v \in \mathcal{O}^\times$, then $m \geq n$ by choice of n. Then $y = (v\pi^{m-n})\pi^n \in \pi^n\mathcal{O}$. So, $I = \pi^n\mathcal{O}$, and $\mathcal{O}$ is a principal ideal domain with exactly $\mathfrak{p}^n$, $n \geq 0$, as its ideals.

(3): Let $a\pi^n \in \mathfrak{p}^n$, where $a \in \mathcal{O}$. Define the map $f : \mathfrak{p}^n \to \mathcal{O}/\mathfrak{p}$ by $f(a\pi^n) = a + \mathfrak{p}$. Then f is a surjective homomorphism of rings, and $a\pi^n$ is in the kernel of f exactly when $a \in \mathfrak{p}$, or when $a\pi^n \in \mathfrak{p}^{n+1}$. □

Now suppose that F is locally compact with non-archimedean absolute value $|\cdot|_v$, which is discrete by Proposition 3.2. Then by part (1) of Lemma 3.1, each $\mathfrak{p}^n = D_{\beta^n}$ is compact. For each $n \geq 1$, we see that

$$\mathfrak{p}^n = \{x \in F \mid |x|_v \leq \beta^n\} = \{x \in F \mid |x|_v < \beta^{n-1}\},$$

so that $\mathfrak{p}^n$ is also open. Viewing F as an additive group, we have that any neighborhood of 0 contains some $\mathfrak{p}^n$, which is a compact open additive subgroup. In particular, F is locally compact and totally disconnected.

Remark. Let F be a field with a non-archimedean absolute value $|\cdot|_v$. Suppose that $x, y \in F$ are such that $|x|_v \neq |y|_v$, and say $|x|_v > |y|_v$. Then $|x+y|_v \leq \max(|x|_v, |y|_v) = |x|_v$. But also, $|x|_v = |x+y+(-y)|_v \leq \max(|x+y|_v, |y|_v)$. But since we have assumed $|x|_v > |y|_v$, then we must have $|x+y|_v = |x|_v$. That is, for any $x, y \in F$, if $|x|_v \neq |y|_v$, then $|x+y|_v = \max(|x|_v, |y|_v)$.

Suppose again that F is locally compact with non-archimedean absolute value $|\cdot|_v$. Then we have $1+\mathfrak{p}^n$ is a compact open neighborhood of 1 for each $n \geq 1$. Also $1+\mathfrak{p}^n \subset \mathcal{O}^\times$, since by the above remark, if $x = 1 + y \in 1 + \mathfrak{p}^n$, then $|x|_v = \max(1, |y|_v) = 1$. We also have that if $x \in 1 + \mathfrak{p}^n$, then

$$|x^{-1} - 1|_v = |x^{-1}|_v|1 - x|_v = |1 - x|_v \leq \beta^n,$$

and so $x^{-1} \in 1 + \mathfrak{p}^n$. Since $1 + \mathfrak{p}^n$ is also closed under multiplication, then each $1 + \mathfrak{p}^n$ is a subgroup of $\mathcal{O}^\times$, and so of $F^\times$. Each neighborhood of 1 in $F^\times$ (or in $\mathcal{O}^\times$) contains some $1 + \mathfrak{p}^n$ as a compact open subgroup.

We now turn to the case of the completion of a field with some non-archimedean absolute value. What we are most interested in is such a field which is also locally compact. A *local field* is a field which is locally compact and complete with respect to some absolute value. If the absolute value is archimedean, the field is called an *archimedean local field*, which we know by Theorem 2.2 is always isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, and if the absolute value is non-archimedean, the field is called a *non-archimedean local field*.

Now let F be a field with a non-archimedean absolute value $|\cdot|_v$, and let $\hat{F}$ be the completion of F with absolute value $|\cdot|'_v$ extending $|\cdot|_v$. It is immediate that $|\cdot|'_v$ is also a non-archimedean. If $a \in \hat{F}^\times$, and $\{a_n\}$ is a Cauchy sequence of elements of F which represents a, then by definition $|a|'_v = \lim_{n\to\infty} |a_n|_v$, and $a = \lim_{n\to\infty} a_n$ when embedding F in $\hat{F}$, and so for large enough n we have $|a - a_n|'_v < |a|'_v$. For large enough n, then, we have

$$|a_n|_v = |a_n - a + a|'_v = \max(|a_n - a|'_v, |a|'_v) = |a|'_v.$$

In other words, the absolute values of elements in such a Cauchy sequence eventually stabilize, and it follows that the image of $|\cdot|'_v$ in $\mathbb{R}$ must be the same as the image of $|\cdot|_v$. In particular, if $|\cdot|_v$ is discrete, then so is $|\cdot|'_v$, and if π is a uniformizer for F, then it is for $\hat{F}$ also.

Proposition 3.4. *Let F be a field with a non-archimedean value $|\cdot|_v$, with ring of integers $\mathcal{O}$, and $\mathfrak{p}$ the maximal ideal of $\mathcal{O}$. Let $\hat{F}$ be the completion of F with ring of integers $\hat{\mathcal{O}}$, and $\hat{\mathfrak{p}}$ the maximal ideal of $\hat{\mathcal{O}}$. Then*

$$\mathcal{O}/\mathfrak{p} \cong \hat{\mathcal{O}}/\hat{\mathfrak{p}} \quad \text{as fields.}$$

If $|\cdot|_v$ is discrete, then for every $n \geq 1$,

$$\mathcal{O}/\mathfrak{p}^n \cong \hat{\mathcal{O}}/\hat{\mathfrak{p}}^n \quad \text{as rings.}$$

Proof. Define the map $f : \mathcal{O} \to \hat{\mathcal{O}}/\hat{\mathfrak{p}}$ by $f(a) = a + \hat{\mathfrak{p}}$. Then f is a ring homomorphism with $\ker(f) = \mathfrak{p}$, and we must show f is surjective. If $\alpha \in \hat{\mathcal{O}}$, we need to show that there is an $a \in \mathcal{O}$ such that $a - \alpha \in \hat{\mathfrak{p}}$, or $|a - \alpha|'_v < 1$. We can assume $\alpha \neq 0$ since $f(0) = \hat{\mathfrak{p}}$. We may choose a Cauchy sequence $\{a_k\}$ in F, viewed as embedded in $\hat{F}$, such that $a_k \to \alpha$ in $\hat{F}$. As in the discussion above, the absolute values of the a_k eventually stabilize, so we may choose n_0 such that $|a_{n_0}|_v = |\alpha|'_v \leq 1$, so $a_{n_0} \in \mathcal{O}$. Also, $|a_k - \alpha|'_v \to 0$, and so we may choose $m \geq n_0$ large enough so that $|a_m - \alpha|'_v < 1$. Then $a_m \in \mathcal{O}$, and $f(a_m) = \alpha + \hat{\mathfrak{p}}$.

If $|\cdot|_v$ is discrete and $n \geq 1$, we define $h : \mathcal{O} \to \hat{\mathcal{O}}/\hat{\mathfrak{p}}^n$ by $h(a) = a + \hat{\mathfrak{p}}^n$. Then h is a ring homomorphism and $\ker(h) = \mathfrak{p}^n$, and so we must show h is surjective. Let $\alpha \in \hat{\mathcal{O}}$, with $\alpha \neq 0$ say, and let π be a uniformizer for F (and so for $\hat{F}$), with $|\pi|'_v = \beta$. As before, we choose $\{a_k\}$ a Cauchy sequence in F which converges to α in $\hat{F}$, and now we may choose m large enough so that $|a_m|'_v \leq 1$ and $|a_m - \alpha|'_v \leq \beta^n$, so $a_m - \alpha \in \hat{\mathfrak{p}}^n$. Then $h(a_m) = \alpha + \hat{\mathfrak{p}}^n$, and h is surjective. □

Let $\{a_n\}$ be some sequence in a field F with non-archimedean absolute value $|\cdot|_v$. For any distinct positive integers m and n with $m > n$, we have

$$|a_m - a_n|_v \leq \max(|a_m - a_{m-1}|_v, |a_{m-1} - a_{m-2}|_v, \ldots, |a_{n+1} - a_n|_v).$$

So, if $|a_{n+1}-a_n|_v \to 0$ as $n \to \infty$, then the sequence $\{a_n\}$ is Cauchy. If we further assume that F is complete, then this means an infinite series $\sum_{i=0}^{\infty} c_i$ converges if and only if $|c_i|_v \to 0$ as $i \to \infty$.

Lemma 3.2. *Let F be a field with discrete non-archimedean absolute value $|\cdot|_v$, with ring of integers $\mathcal{O}$, uniformizer π, and $\mathfrak{p} = \pi\mathcal{O}$. Let $S \subset \mathcal{O}$ be a set of representatives for $\mathcal{O}/\mathfrak{p}$ such that $0 \in S$, and let $\hat{F}$ be the completion of F with $|\cdot|_v$, with ring of integers $\hat{\mathcal{O}}$, and $\hat{\mathfrak{p}} = \pi\hat{\mathcal{O}}$. Then every nonzero $x \in \hat{F}$ may be written uniquely as a convergent series*

$$x = \pi^m \sum_{i=0}^{\infty} a_i \pi^i, \quad a_i \in S, a_0 \neq 0, m \in \mathbb{Z}.$$

Proof. Let $x \in \hat{F}^\times$, and write $x = \pi^m u$, with $u \in \hat{\mathcal{O}}^\times$ and $m \in \mathbb{Z}$, which can be done uniquely by Proposition 3.3(2). We prove by induction that for any $n \geq 0$, we can write u as

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n + \pi^{n+1}b_{n+1},$$

for some $b_{n+1} \in \hat{\mathcal{O}}$, and for unique $a_i \in S$ with $a_0 \neq 0$. First, from the proof of Proposition 3.4, there is a unique $a_0 \in S$ such that $u - a_0 \in \hat{\mathfrak{p}}$, so we have $u = a_0 + \pi b_1$ for some $b_1 \in \hat{\mathcal{O}}$, and $a_0 \neq 0$. Now assume that there are unique $a_0, \ldots, a_{n-1} \in S$, and some $b_n \in \hat{\mathcal{O}}$, such that

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \pi^n b_n.$$

Again, from the proof of Proposition 3.4, there is a unique $a_n \in S$ such that $b_n - a_n \in \hat{\mathfrak{p}}$, so then $\pi^n b_n = \pi^n(a_n + \pi b_{n+1}) = a_n\pi^n + b_{n+1}\pi^{n+1}$ for some $b_{n+1} \in \hat{\mathcal{O}}$, and the claim in proven. So now, $\sum_{i=0}^{\infty} a_i\pi^i$ converges to u in $\hat{F}$ since the terms go to 0. □

Suppose that F is complete with respect to a discrete non-archimedean absolute value, with ring of integers $\mathcal{O}$, and uniformizer π, with $\mathfrak{p} = \pi\mathcal{O}$. Since each $\mathfrak{p}^n$ is open in $\mathcal{O}$, the quotient topological rings $\mathcal{O}/\mathfrak{p}^n$ have the discrete topology. The natural projection maps $\rho_n^m : \mathcal{O}/\mathfrak{p}^m \to \mathcal{O}/\mathfrak{p}^n$, with $m \geq n$, form an inverse system of homomorphisms, and we may consider the inverse limit

$$\varprojlim_n \mathcal{O}/\mathfrak{p}^n,$$

giving a topological ring. We also have the projections $\rho_n : \mathcal{O} \to \mathcal{O}/\mathfrak{p}^n$, which are compatible with the maps ρ_n^m, giving a map

$$\rho : \mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n.$$

In fact, this gives an isomorphism of topological rings.

Theorem 3.1. *Let F be a field which is complete with respect to a non-archimedean discrete absolute value $|\cdot|_v$, with $\mathcal{O}$ the ring of integers with maximal ideal $\mathfrak{p}$. Then*

$$\mathcal{O} \cong \varprojlim_n \mathcal{O}/\mathfrak{p}^n \quad \textit{as topological rings.}$$

Proof. We show that the map ρ defined above is both an isomorphism of rings, and a homeomorphism. First, $\ker(\rho) = \cap_{n\geq 1}\mathfrak{p}^n = 0$, and so ρ is injective.

Let π be a uniformizer for F, and let S be a set of representatives for $\mathcal{O}/\mathfrak{p}$ with $0 \in S$. It follows from Lemma 3.2 that for any $n \geq 1$, any element of $\mathcal{O}/\mathfrak{p}^n$ may be written uniquely as

$$(a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}) + \mathfrak{p}^n,$$

where $a_0, a_1, \ldots, a_{n-1} \in S$. From this and by the definition of the inverse limit, any element

$$x \in \varprojlim_n \mathcal{O}/\mathfrak{p}^n$$

may be written uniquely as a sequence

$$x = (a_0 + \mathfrak{p}, a_0 + a_1\pi + \mathfrak{p}^2, \ldots, a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \mathfrak{p}^n, \ldots), \quad a_i \in S, i \geq 0.$$

Also from Lemma 3.2, the element $y = \sum_{i=0}^{\infty} a_i\pi^i$ is an element of $\mathcal{O}$, and now we have $\rho(y) = x$, and ρ is surjective.

We now show that ρ is a homeomorphism. Since ρ is a ring isomorphism, if we show that ρ^{-1} of a basis neighborhood of the additive identity in the image is a basis neighborhood of 0 in $\mathcal{O}$, then ρ is continuous. Then, since $\mathcal{O}$ is compact and the image is Hausdorff (since each $\mathcal{O}/\mathfrak{p}^n$ is discrete), then ρ will be a homeomorphism (by Exercise 2 of the *Direct Limits, Inverse Limits, and Profinite Groups* notes). Now, in the space $\prod_{i=1}^{\infty} \mathcal{O}/\mathfrak{p}^i$, the sets

$$B_m = \prod_{i=1}^{m} \{\mathfrak{p}^i\} \times \prod_{j=m+1}^{\infty} \mathcal{O}/\mathfrak{p}^j,$$

where $\mathfrak{p}^i$ is the additive identity in $\mathcal{O}/\mathfrak{p}^i$, form a basis for neighborhoods at the additive identity $\prod_{i=1}^{\infty} \mathfrak{p}^i$. Then we have the sets

$$B'_m = B_m \cap \varprojlim_n \mathcal{O}/\mathfrak{p}^n$$

form a basis for the additive identity in the inverse limit, and we claim that $\rho^{-1}(B'_m) = \mathfrak{p}^m$, where the sets $\mathfrak{p}^m$, $m \geq 1$, form a basis of neighborhoods of 0 in $\mathcal{O}$. If $\rho(y) \in B'_m$, then we must have $y \in \mathfrak{p}^m$, and to see that $\mathfrak{p}^m$ surjects onto B'_m, we may again apply Lemma 3.2. The elements of $\mathfrak{p}^m$ are of the form $\sum_{i=m+1}^{\infty} a_i\pi^i$, and these elements map exactly to the elements in B'_m. Thus ρ is a homeomorphism. □

Finally, we have the following description of non-archimedean local fields.

Theorem 3.2. *Let F be a field which is complete with respect to a non-archimedean absolute value $|\cdot|_v$, and let $\mathcal{O}$ be the ring of integers with maximal ideal $\mathfrak{p}$. Then F is locally compact (so a non-archimedean local field) if and only if $|\cdot|_v$ is discrete and $\mathcal{O}/\mathfrak{p}$ is finite.*

Proof. First suppose that F is locally compact. Then $|\cdot|_v$ is discrete by Proposition 3.2, and $\mathcal{O}$ is compact by part (1) of Lemma 3.1. Since $|\cdot|_v$ is discrete, then $\mathfrak{p}$ is open in $\mathcal{O}$. Since $\mathfrak{p}$ is an additive open subgroup of the compact group $\mathcal{O}$, then it must have finite index, and so $\mathcal{O}/\mathfrak{p}$ is finite.

Now suppose that $|\cdot|_v$ is discrete and $\mathcal{O}/\mathfrak{p}$ is finite. By part (3) of Proposition 3.3, for each $n \geq 1$, $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$ is also finite. Then $\mathcal{O}/\mathfrak{p}^n$ is also finite for every $n \geq 1$. By Theorem 3.1, $\mathcal{O}$ under addition is a profinite group, and is thus compact (and totally disconnected). Since $\mathcal{O}$ is compact, each $\mathfrak{p}^n$ is compact also, and then every neighborhood of 0 in F contains some $\mathfrak{p}^n$ as a compact neighborhood of 0. Thus F is locally compact. □

Example 4: The p-adic rationals. On $\mathbb{Q}$, we have the non-archimedean p-adic absolute value $|\cdot|_p$. The image of $|\cdot|_p$ on $\mathbb{Q}^\times$ is exactly $\{p^n \mid n \in \mathbb{Z}\}$, and so $|\cdot|_p$ is discrete. The ring of integers in $\mathbb{Q}$ with respect to $|\cdot|_p$ is exactly

$$\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}, (b, p) = 1\},$$

which is called *the ring $\mathbb{Z}$ localized at p*. The unique maximal ideal of $\mathbb{Z}_{(p)}$ is exactly $p\mathbb{Z}_{(p)}$, and the ideals of $\mathbb{Z}_{(p)}$ are all of the form $p^n\mathbb{Z}_{(p)}$ for $n \geq 1$. Define a map $f : \mathbb{Z} \to \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ by $f(m) = m + p^n\mathbb{Z}_{(p)}$. Then f is a ring homomorphism with $\ker(f) = p^n\mathbb{Z}$. Also, if $a/b \in \mathbb{Z}_{(p)}$, then since $(b, p^n) = 1$, we can write $a = bk + p^n l$ for some $k, l \in \mathbb{Z}$. Then $a/b = k + p^n l/b$, where $p^n l/b \in p^n\mathbb{Z}_{(p)}$. That is, $f(k) = a/b + p^n\mathbb{Z}_{(p)}$ and f is surjective, so $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$.

Completing $\mathbb{Q}$ with respect to $|\cdot|_p$ gives us the field $\mathbb{Q}_p$ of p-adic rationals. The extended absolute value on $\mathbb{Q}_p$ is non-archimedean and discrete, and let $\mathcal{O}$ be the ring of integers in $\mathbb{Q}_p$, which has maximal ideal $p\mathcal{O}$, and all ideals of the form $p^n\mathcal{O}$. From Proposition 3.4 and the above discussion, we have $\mathcal{O}/p\mathcal{O} \cong \mathbb{Z}/p\mathbb{Z}$, which is of course finite. Since the absolute value is discrete, then by Theorem 3.2, $\mathbb{Q}_p$ is locally compact. Again by Proposition 3.4 and the above calculation, we have for every $n \geq 1$, $\mathcal{O}/p^n\mathcal{O} \cong \mathbb{Z}/p^n\mathbb{Z}$. Then from Theorem 3.1, we have

$$\mathcal{O} \cong \varprojlim_n \mathcal{O}/p^n\mathcal{O} \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

That is, the ring of integers of $\mathbb{Q}_p$ is exactly the ring of p-adic integers $\mathbb{Z}_p$, constructed as an inverse limit. Now, note that the set $\{0, 1, 2, \ldots, p-1\}$ is a set of representatives of the residue field $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$. Applying Lemma 3.2, every element of $\mathbb{Q}_p^\times$ may be written uniquely as $p^m \sum_{i=0}^\infty a_i p^i$, where $m \in \mathbb{Z}$ and each $a_i \in \{0, 1, \ldots p-1\}$, $a_0 \neq 0$, and each element of $\mathbb{Z}_p$ may be written uniquely as $\sum_{i=0}^\infty b_i p^i$, where each $b_i \in \{0, 1, \ldots, p-1\}$.

4. Classification of local fields

In this section we give an outline of the proof of the classification of local fields. One of the main steps is to analyze finite extensions of local fields.

Let K/F be a finite extension of fields, and let $x \in K$. Viewing K as a vector space over F, multiplication of elements in K by x is an F-linear transformation, which we denote by μ_x. Define the *norm of x from K to F*, denoted $\mathrm{N}_{K/F}(x)$, as the determinant of the F-linear transformation $\mu_x : K \to K$, so $\mathrm{N}_{K/F}(x) = \det(\mu_x)$. It is immediate from this definition that for any $x \in K$, we have $\mathrm{N}_{K/F}(x) \in F$. If the extension K/F is Galois, then the norm of x is in fact just the product of the Galois conjugates of x. The next result uses the norm to extend absolute values of complete fields to finite extensions. See [N, Theorem 4.8] for a proof, which requires just a bit more algebraic number theory.

Theorem 4.1. *Let F be a field which is complete with respect to an absolute value $|\cdot|_v$, and let K be a finite extension of F of degree n. The absolute value $|\cdot|_v$ may be extended uniquely to an absolute value $|\cdot|_w$ of K, given by the formula*

$$|x|_w = (|\mathrm{N}_{K/F}(x)|_v)^{1/n}.$$

Furthermore, K is complete with respect to the absolute value $|\cdot|_w$.

Using Theorem 4.1 and the previous results on local fields, we have the following.

Proposition 4.1. *If F is a local field, and K is a finite extension of F given the unique absolute value extended from F, then K is a local field.*

Proof. First, if F is an archimedean local field, then by Theorem 2.2, F is either $\mathbb{R}$ or $\mathbb{C}$. Since $\mathbb{C}$ has no proper finite extensions, and the only one for $\mathbb{R}$ is $\mathbb{C}$, then the statement follows in this case and we may assume that F is a non-archimedean local field.

If $|\cdot|_v$ is a non-archimedean absolute value on F, then the extended absolute value $|\cdot|_w$ from Theorem 4.1 must be non-archimedean on K, since it is still bounded on the prime subring, applying Proposition 1.1. Let $\mathcal{O}_F$ be the ring of integers of F with maximal ideal $\mathfrak{p}_F$, and let $\mathcal{O}_K$ be the ring of integers of K with maximal ideal $\mathfrak{p}_K$. By Theorem 3.2, K is a local field if and only if $|\cdot|_w$ is discrete and $\mathcal{O}_K/\mathfrak{p}_K$ is finite.

From the formula in $|\cdot|_w$ in Theorem 4.1, the discreteness of $|\cdot|_w$ follows from the discreteness of $|\cdot|_v$. Since we have $\mathcal{O}_F \subset \mathcal{O}_K$ and $\mathfrak{p}_F \subset \mathfrak{p}_K$, the map $\mathcal{O}_F \to \mathcal{O}_K/\mathfrak{p}_K$ defined by $a \mapsto a + \mathfrak{p}_K$ has kernel exactly $\mathfrak{p}_F$, and so we may view $\mathcal{O}_K/\mathfrak{p}_K$ as an extension of $\mathcal{O}_F/\mathfrak{p}_F$. Now let $x_1, \dots, x_n \in \mathcal{O}_K$, and suppose these are linearly dependent over F, so that there are $\alpha_1, \dots, \alpha_n \in F$, not all 0, such that $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$. Divide this equation by whichever α_i has the largest absolute value, and then we obtain an equation $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$, where each $\lambda_i \in \mathcal{O}_F$, but not all λ_i are in $\mathfrak{p}_F$. Reducing modulo $\mathfrak{p}_K$, we obtain $\sum_{i=1}^n \bar{\lambda}_i \bar{x}_i = \bar{0}$, where $\bar{y} = y + \mathfrak{p}_K$, which gives a linear dependence of elements in $\mathcal{O}_K/\mathfrak{p}_K$ over $\mathcal{O}_F/\mathfrak{p}_F$. In other words, if any n elements of $\mathcal{O}_K/\mathfrak{p}_K$ are linearly independent over $\mathcal{O}_F/\mathfrak{p}_F$, then they may be pulled back to elements of $\mathcal{O}_K$ which are linearly indepedent over F. So, we have $[\mathcal{O}_K/\mathfrak{p}_K : \mathcal{O}_F/\mathfrak{p}_F] \leq [K : F] < \infty$. Since $\mathcal{O}_F/\mathfrak{p}_F$ is a finite field, then the finite extension $\mathcal{O}_K/\mathfrak{p}_K$ is also finite, and thus K is local. □

Let F be a topological field. A *topological vector space over* F is a vector space over V which is a topological group as a group under addition, and such that scalar multiplication $F \times V \to V$ is continuous. We next state a key result on topological vector spaces over locally compact fields, a proof of which can be found in [RV, Proposition 4-13] and uses some machinery of the Haar measure.

Theorem 4.2. *Let V be a topological vector space over a nondiscrete locally compact field F. If V is locally compact, then V is finite dimensional over F.*

We now have the following characterization of extensions of local fields.

Corollary 4.1. *Let F be a local field, and let K be an extension of F, where K has some absolute value which extends that of F. Then K is a local field if and only if K is a finite extension of F.*

Proof. If K/F is a finite extension, then we know K is a local field from Proposition 4.1. If we assume K is a local field, then it is in particular locally compact. But then we have that K is a locally compact topological vector space over F, which is locally compact. By Theorem 4.2, K must be finite dimensional as an F-vector space, so that K/F is a finite extension. □

The last set of examples of local fields are of characteristic p. There is no non-trivial absolute value on any finite field $\mathbb{F}_q$, since the multiplicative group $\mathbb{F}_q^\times$ is cyclic, and also no non-trivial absolute value on any algebraic extension of $\mathbb{F}_q$, since it is a union of finite fields. So, we must look at a transcendental extension $\mathbb{F}_q(t)$, where q is a power of some prime p, and t is a transcendental element over $\mathbb{F}_q$.

We have $\mathbb{F}_q[t]$ is a principal ideal domain, and is a subring of $\mathbb{F}_q(t)$, and so we define an abolute value based on the same idea as the p-adic absolute value on $\mathbb{Q}$. Let $f(t) \in \mathbb{F}_q[t]$ be an irreducible polynomial. For any $g(t)/h(t) \in \mathbb{F}_q(t)$, write $g(t)/h(t) = f(t)^m(a(t)/b(t))$, where $f(t)$ does not divide $a(t)$ or $b(t)$. Define the *$f(t)$-adic absolute value* on $\mathbb{F}_q(t)$ by

$$\left|\frac{g(t)}{h(t)}\right|_{f(t)} = (q^{d(f)})^{-m}, \quad \text{where } d(f) = \deg(f).$$

Then $|\cdot|_{f(t)}$ is a discrete non-archimedean absolute value on $\mathbb{F}_q(t)$ (where $f(t)$ is a uniformizer) for the exact same reason that $|\cdot|_p$ is a discrete non-archimedean absolute value on $\mathbb{Q}$. Now define the *degree absolute value* on $\mathbb{F}_q(t)$, denoted $|\cdot|_\infty$, by

$$\left|\frac{g(t)}{h(t)}\right|_\infty = q^{\deg(g)-\deg(h)}.$$

Then $|\cdot|_\infty$ is also a discrete non-archimedean absolute value on $\mathbb{F}_q(t)$, where $1/t$ is a uniformizer. In fact, these are all of the possible inequivalent absolute values on $\mathbb{F}_q(t)$.

Theorem 4.3. *Every absolute value on $\mathbb{F}_q(t)$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_{f(t)}$ for some irreducible polynomial $f(t) \in \mathbb{F}_q[t]$.*

Proof. See Problem set 2. □

To understand the completions of $\mathbb{F}_q(t)$ with respect to these absolute values, we can apply Lemma 3.2. First we need the residue fields.

Lemma 4.1. *The residue field of $\mathbb{F}_q(t)$ with respect to the absolute value $|\cdot|_\infty$ is isomorphic to $\mathbb{F}_q$, and the residue field of $\mathbb{F}_q(t)$ with respect to the absolute value $|\cdot|_{f(t)}$ is isomorphic to $\mathbb{F}_{q^{d(f)}}$, where $d(f) = \deg(f)$.*

Proof. See Problem set 2. □

So, by Theorem 3.2, the completions of $\mathbb{F}_q(t)$ with respect to these absolute values are local fields. Now, according to Lemma 3.2 and Lemma 4.1, the completion of $\mathbb{F}_q(t)$ with respect to $|\cdot|_{f(t)}$ is isomorphic algebraically to $\mathbb{F}_{q^{d(f)}}((f(t)))$, the field of Laurent series in $f(t)$ with coefficients in $\mathbb{F}_{q^{d(f)}}$. In particular, if we specialize to the irreducible polynomial $f(t) = t$, then the completion of $\mathbb{F}_q(t)$ with the absolute value $|\cdot|_t$ is just the field $\mathbb{F}_q((t))$ of Laurent series in t over $\mathbb{F}_q$. Similarly, the completion of $\mathbb{F}_q(t)$ with respect to the absolute value $|\cdot|_\infty$ is isomorphic to $\mathbb{F}_q((1/t))$, the field of Laurent series in $1/t$ over $\mathbb{F}_q$. It turns out that these are, in fact, all basically same as topological fields.

Proposition 4.2. *If $\mathbb{F}_q((1/t))$ is given the topology from $|\cdot|_\infty$ and $\mathbb{F}_q((t))$ is given the topology from $|\cdot|_t$, then $\mathbb{F}_q((1/t)) \cong \mathbb{F}_q((t))$ as topological fields. If $\mathbb{F}_{q^{d(f)}}((f(t)))$ is given the topology from $|\cdot|_{f(t)}$, and $\mathbb{F}_{q^{d(f)}}((t))$ is given the topology from $|\cdot|_t$, then $\mathbb{F}_{q^{d(f)}}((f(t))) \cong \mathbb{F}_{q^{d(f)}}((t))$ as topological fields.*

Proof. See Problem set 2. □

We are finally at the point where we may list all local fields.

Theorem 4.4 (Classification of Local Fields)**.** *The only archimedean local fields are $\mathbb{R}$ and $\mathbb{C}$, the only characteristic 0 non-archimedean local fields are finite extensions of $\mathbb{Q}_p$, and the only characteristic p non-archimedean local fields are finite extensions of $\mathbb{F}_p((t))$.*

Proof. The archimedean local fields were classified in Theorem 2.2, so assume that F is a non-archimedean local field. If $\mathrm{char}(F) = 0$, then we have $\mathbb{Q} \subset F$, and from Theorem 1.1, we may replace the absolute value of F by an equivalent one so that it restricts to $\mathbb{Q} \subset F$ as the p-adic absolute value $|\cdot|_p$ for some prime p. Since F is complete, then we have $\mathbb{Q}_p \subset F$. By Corollary 4.1, we must have F is a finite extension of $\mathbb{Q}_p$.

Now assume that F is a non-archimedean local field of positive characteristic p. Then we have $\mathbb{F}_p \subset F$, and since we have a non-trivial absolute value on F, we must have $\mathbb{F}_p(t) \subset F$ for some element t which is transcendental over $\mathbb{F}_p$. Theorem 4.3 tells us that

we may replace the absolute value on F by one which restricts to $\mathbb{F}_p(t)$ as either $|\cdot|_\infty$ or $|\cdot|_{f(t)}$ for some irreducible $f(t) \in \mathbb{F}_p[t]$. By Proposition 4.2, and since F is complete, we see that F must contain $\mathbb{F}_q((t))$ for some q a power of p. If $\mathbb{F}_q = \mathbb{F}_p(\gamma)$, then in fact $\mathbb{F}_q((t)) = \mathbb{F}_p((t))(\gamma)$ (Exercise), and so $\mathbb{F}_q((t))$ is a finite extension of $\mathbb{F}_p((t))$. By Corollary 4.1, we must have that F is a finite extension of $\mathbb{F}_q((t))$, and is therefore a finite extension of $\mathbb{F}_p((t))$. □

5. Definition and examples of p-adic groups

Let F be a non-archimedean local field, and consider the group $\mathrm{GL}(n, F)$ of invertible n-by-n matrices over F, given the subspace topology in $M_n(F)$ (which has the product topology of F^{n^2}). Since F is locally compact and totally disconnected, then so is $M_n(F)$. The determinant map $\det : M_n(F) \to F$ is a continuous function, and $\mathrm{GL}(n, F)$ is the inverse image of the open set $F^\times$ under this map, and so $\mathrm{GL}(n, F)$ is an open subset of $M_n(F)$. Thus $\mathrm{GL}(n, F)$ is a locally compact totally disconnected group. If $\mathcal{O}$ is the ring of integers of F, then we know that $M_n(\mathcal{O})$ is compact and totally disconnected, since $\mathcal{O}$ is. Now $\mathrm{GL}(n, \mathcal{O})$ is the intersection of $M_n(\mathcal{O})$ with $\mathrm{GL}(n, F)$, and so $\mathrm{GL}(n, \mathcal{O})$ is a compact totally disconnected subgroup of $\mathrm{GL}(n, F)$.

Another way to prove that $\mathrm{GL}(n, F)$ is a locally compact disconnected group is to give explicit compact open subgroups of $\mathrm{GL}(n, F)$ which are contained in arbitarily small neighborhoods of the identity. If π is a uniformizer for F, and I is the identity matrix, then such subgroups are given by $K_m = I + \pi^m M_n(\mathcal{O})$, which are also normal subgroups of $\mathrm{GL}(n, \mathcal{O})$ (see Problem set 2). In the case $n = 1$, then $\mathrm{GL}(1, F) = F^\times$, and $K_m = 1 + \mathfrak{p}^m$, where $\mathfrak{p} = \pi\mathcal{O}$. In Section 3, we saw that the K_m are arbitarily small compact open subgroups of $F^\times$.

An *algebraic subgroup* of $\mathrm{GL}(n, F)$ is a subgroup H such that there are a finite number of polynomials $f_1, f_2, \cdots, f_k \in F[x_{11}, x_{12}, \ldots, x_{nn}]$ with

$$H = \{g = (g_{ij}) \in \mathrm{GL}(n, F) \mid f_1(g_{ij}) = \cdots = f_k(g_{ij}) = 0\}.$$

For example, $\mathrm{SL}(n, F)$ is an algebraic subgroup of $\mathrm{GL}(n, F)$ since its elements (g_{ij}) are defined such that the entries g_{ij} satisfy the polynomial $\det((x_{ij})) - 1$. Also, $\mathrm{GL}(n, F)$ is an algebraic subgroup of itself since the entries of each element are the zeros of the zero polyonmial. A *p-adic group* over a non-archimedean local field F is defined to be a closed algebraic subgroup of $\mathrm{GL}(n, F)$. Note that since a p-adic group is a closed subgroup of the locally compact disconnected group $\mathrm{GL}(n, F)$, then every p-adic group is a locally compact totally disconnected group.

Below are just a few important examples of p-adic groups.

General and Special Linear Groups: We have mentioned that $\mathrm{GL}(n, F)$ is an algebraic subgroup of itself, and since it is also closed, then it is a p-adic group. Since $\mathrm{SL}(n, F)$ is an algebraic subgroup of $\mathrm{GL}(n, F)$, and it is the inverse image under the determinant map of the closed subset $\{1\}$ of F, then it is a p-adic group as well.

Borel and Unipotent Subgroups: The *Borel subgroup* of $\mathrm{GL}(n, F)$, denoted $B(n, F)$, is the subgroup of upper triangular matrices in $\mathrm{GL}(n, F)$. In other words, the elements of $B(n, F)$ are exactly the elements (g_{ij}) of $\mathrm{GL}(n, F)$ such that $g_{ij} = 0$ whenever $i > j$, $1 \leq i, j \leq n$, making $B(n, F)$ an algebraic subgroup of $\mathrm{GL}(n, F)$. Since this may be

viewed as the intersection of a copy of $F^{(n^2+n)/2}$ in F^{n^2} with $\mathrm{GL}(n,F)$, then $B(n,F)$ is a closed subgroup of $\mathrm{GL}(n,F)$, and so it is a p-adic group. The *unipotent subgroup* of $\mathrm{GL}(n,F)$, denoted $N(n,F)$, is the subgroup of $B(n,F)$ which has only 1's on the diagonal entries. That is, in addition to being in $B(n,F)$, the elements (g_{ij}) of $N(n,F)$ also satisfy $g_{ii}-1=0$ for each $1\leq i\leq n$. Topologically, $N(n,F)$ may be viewed as the intersection of a copy of $F^{(n^2-n)/2}$ in F^{n^2} with $\mathrm{GL}(n,F)$, making it a closed algebraic subgroup of $\mathrm{GL}(n,F)$, and thus a p-adic group.

Orthogonal and Symplectic Groups: Consider the vector space F^n, and let $S(\cdot,\cdot)$ be a non-degenerate symmetric form on F^n, so that $S(v,w)=S(w,v)$ for all $v,w\in F^n$ (symmetric), and if $S(v,w)=0$ for all $w\in F^n$, then $v=0$ (non-degenerate). The *orthogonal group* for the form S, denoted $\mathrm{O}_S(n,F)$, or just $\mathrm{O}(n,F)$ if the form S is implicit, is the subgroup of $\mathrm{GL}(n,F)$ consisting of elements g such that $S(gv,gw)=S(v,w)$ for all $v,w\in F^n$. Choosing a basis for F^n, one can find an invertible symmetric matrix A such that $\mathrm{O}_S(n,F)$ is exactly $\{g\in\mathrm{GL}(n,F)\ \mid\ {}^tgAg=A\}$, where ${}^tg$ denotes the transpose of g. That is, if $g=(g_{ij})$ in $\mathrm{O}_S(n,F)$, then $(g_{ji})A(g_{ij})A^{-1}-I=0$. Considering each entry of this matrix equation, we get a set of n^2 polynomials which g_{ij} must satisfy, making the orthogonal group an algebraic subgroup of $\mathrm{GL}(n,F)$. Since the map $g\mapsto {}^tgAgA^{-1}$ is a continuous map on $\mathrm{GL}(n,F)$, and $\mathrm{O}_S(n,F)$ is the inverse image of the identity under this map, then the orthgonal group is also closed, and thus a p-adic group.

Now consider the vector space F^{2n}, and let $T(\cdot,\cdot)$ be a non-degenerate skew-symmetric form on F^{2n}, so that $T(v,v)=0$ for all $v\in F^{2n}$ (or if $\mathrm{char}(F)\neq 2$, $T(v,w)=-T(w,v)$ for all $v,w\in F^{2n}$), and if $T(v,w)=0$ for all $w\in F^{2n}$, then $v=0$. One may check that in order to have a non-degenerate skew-symmetric form on a finite-dimensional vector space, the space must have even dimension. The *symplectic group* for the form T, denoted $\mathrm{Sp}_T(2n,F)$, or $\mathrm{Sp}(2n,F)$ if T is understood, is the set of elements g in $\mathrm{GL}(2n,F)$ such that $T(gv,gw)=T(v,w)$ for all $v,w\in F^{2n}$. One may choose a basis for F^{2n}, and find an invertible skew-symmetric matrix J such that $\mathrm{Sp}_T(2n,F)=\{g\in\mathrm{GL}(2n,F)\ \mid\ {}^tgJg=J\}$. Similar to the orthogonal case, one can use this definition to see that the symplectic group is a p-adic group (Exercise).

The orthogonal and symplectic groups are both examples of *classical groups*, a classification of which over arbitrary fields may be found in [G].

References

[FT] A. Fröhlich and M.J. Taylor, Algebraic Number Theory. Cambridge Studies in Advanced Mathematics, 27. *Cambridge University Press, Cambridge*, 1993.

[G] L.C. Grove, Classical Groups and Geometric Algebra. Graduate Studies in Mathematics, 39. *American Mathematical Society, Providence, RI*, 2002.

[L] S. Lang, Algebraic Number Theory. Second edition. Graduate Texts in Mathematics, 110. *Springer-Verlag, New York*, 1994.

[N] J. Neukirch, Algebraic Number Theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. *Springer-Verlag, Berlin*, 1999.

[RV] D. Ramakrishnan and R.J. Valenza, Fourier Analysis on Number Fields. Graduate Texts in Mathematics, 186. *Springer-Verlag, New York*, 1999.

[S] J.-P. Serre, Local Fields. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. *Springer-Verlag, New York-Berlin*, 1979.