BMST 2025: INTRODUCTION TO p-ADIC NUMBERS

ADRIEN MORIN

Contents

1. Normed fields

Definition 1.1. *An absolute value on a field K is a map $|\cdot| : K \to \mathbb{R}_+$ such that*

(1) $|x| = 0$ *if and only if* $x = 0$,
(2) $|xy| = |x|\,|y|$ *for all* x,$y \in K$,
(3) $|x + y| \leq |x| + |y|$ *for all* $x, y \in K$.

If moreover, the absolute value satisfies the following strong triangle inequality

$$(3') \quad |x + y| \leq \max(|x|, |y|) \quad \text{for all } x, y \in K$$

then we say that it is ultrametric or non-archimedean. A normed field is a field equipped with an absolute value[1]*, an ultrametric or nonarchimedean (valued) field is a field equipped with an ultrametric absolute value.*

Observe that we have $|1|^2 = \left|1^2\right| = |1|$, the only positive real solution of which is 1, so $|1| = 1$. Moreover, $|-1|^2 = \left|(-1)^2\right| = |1| = 1$, so that $|-1| = 1$.

Example 1. The usual absolute value $|\cdot|_\infty$ on $\mathbb{Q}$ or $\mathbb{R}$, defined by $|x|_\infty = x$ if $x \geq 0$ and $|x|_\infty = -x$ if $x < 0$.

Example 2. The trivial absolute value $|\cdot|_{\text{triv}}$, with $|x|_{\text{triv}} = 1$ if $x \neq 0$ and 0 if $x = 0$.

Example 3. Let $v_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ be the map that sends 0 to ∞ and $n \neq 0$ to $\max\left\{k, p^k \text{ divides } n\right\}$. Then v_p satisfies

(1) $v_p(n) = \infty$ if and only if $n = 0$,
(2) $v_p(nm) = v_p(n) + v_p(m)$,
(3) $v_p(n + m) \geq \min(v_p(n), v_p(m))$

We say that v_p is a (discrete) valuation on $\mathbb{Z}$. The map v_p extends uniquely to a map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ satisfying the same properties by letting $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$. Then if we let $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ such that $|x|_p = p^{-v_p(x)}$, we observe readily that $|\cdot|_p$ is an ultrametric absolute value on $\mathbb{Q}$, called the p-adic absolute value.

Example 4. Let K be a field. We can define $v_T : K[T] \to \mathbb{N} \cup \{\infty\}$ by $v_T(P) = \max\left\{k, \quad T^k \text{ divides } P\right\}$ and $v_T(0) = \infty$. It satisfies (1) – (3) in the example above and so again, it extends to a map on the field of fractions $K(T)$. The function v_T on $K(T)$ measures the order of vanishing at 0 of a rational function: for a rational function $R(T) = T^k S(T)$ with $k \in \mathbb{Z}$ and S a rational fraction that has no pole or zero at $T = 0$, i.e. that can be written with a numerator and denominator that do not vanish at 0, then $v_T(R) = k$. For any $\rho > 1$, the function $|R|_{T,\rho} = \rho^{-v_T(P)}$ is an absolute value on $K(T)$. More generally, this works for a prime element P in a principal ideal domain A, to define an absolute value $|\cdot|_{P,\rho}$ on its field of fractions $\text{Frac}(A)$.

Example 5. The degree function on $K[T]$ satisfies

(1) $\deg(P) = -\infty$ if and only if $P = 0$,
(2) $\deg(PQ) = \deg(P) + \deg(Q)$ and
(3) $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$.

Hence $-\deg$ satisfies (1) – (3) above and by the same argument we get an absolute value $|\cdot|_{\deg,\rho}$ on $K(T)$. If we put the formal variable $S = T^{-1}$ then we have an identification $K(S) = K(T)$ and using the above notation, we find $|\cdot|_{\deg,\rho} = |\cdot|_{S,\rho} = |\cdot|_{T^{-1},\rho}$. Thus in a sense $-\deg$ measures the order of vanishing at $T^{-1} = 0$, i.e. at $T = \infty$.

[1]Sometimes this is called a normed field, to distinguish with the case where we only require $|xy| \leq |x|\,|y|$ instead of (2), but we will reserve that term for something else later.

Example 6. We will see later that given a non-trivial non-archimedean absolute value $|\cdot|_K$ on a field K and $\rho > 0$, the functions

$$|\cdot|_\rho : \begin{cases} K[T] & \longrightarrow & \mathbb{R}_+ \\ \sum_{i=0}^n a_i T^i & \mapsto & \max(|a_i|_K \, \rho^i), \end{cases}$$

usually called Gauss norms, extend uniquely to an absolute value on $K(T)$ that agrees with $|\cdot|_K$ on constants $K \subset K(T)$.

Definition–Proposition 1.2. *We say that two absolute values $|\cdot|_1$ and $|\cdot|_2$ on K are equivalent if any of the following equivalent conditions holds:*

(1) a sequence in K converges for $|\cdot|_1$ if and only if converges for $|\cdot|_2$;
(2) the topologies induced by the two absolute values are the same;
(3) for all $x \in K$, $|x|_1 < 1$ if and only if $|x|_2 < 1$;
(4) there exists $\alpha > 0$ such that $|\cdot|_1 = |\cdot|_2^\alpha$.

In item 4 above, be careful that the converse does not always hold: if $|\cdot|_\infty$ is the standard absolute value on $\mathbb{Q}$, then $|\cdot|_\infty^\alpha$ is not an absolute value for $\alpha > 1$, but it is for $0 < \alpha \leq 1$. On the other hand, if $|\cdot|$ is an ultrametric absolute value on a field, then any power of it is still an ultrametric absolute value.

The reader might wonder what are the possible absolute values on $\mathbb{Q}$. The following theorem states that there are not so many, up to equivalence:

Theorem 1.3 (Ostrowski)**.** *Every non-trivial absolute values on $\mathbb{Q}$ is equivalent to either the archimedean absolute value $|\cdot|_\infty$ or the p-adic absolute value $|\cdot|_p$ for some prime number p; moreover the latter are pairwise non-equivalent.*

An absolute value on a field K defines a metric on K by letting $d(x, y) = |x - y|$. If $|\cdot|$ is ultrametric, then that metric satisfies the strong triangle inequality $d(x, z) \leq \max(d(x, y), d(y, z))$ for all $x, y, z \in K$. More generally, there is a similar notion of ultrametric space, which is a set X equipped with a metric d satisfying the above strong triangle inequality.

In an ultrametric space, the balls do not behave as usual.

Lemma 1.4. *Let (X, d) be an ultrametric space and let $x, y, z \in X$. If $d(x, y) \neq d(y, z)$ then $d(x, z) = \max(d(x, y), d(y, z))$.*

Proof. Without loss of generality, let us assume that $d(x, y) < d(y, z)$. By the strong triangle inequality, we have

$$d(x, z) \leq \max(d(x, y), d(y, z)) = d(y, z).$$

On the other hand,

$$d(y, z) \leq \max(d(x, y), d(x, z)).$$

If we had $d(x, y) \geq d(x, z)$, we would find $d(y, z) \leq d(x, y)$, a contradiction. Therefore $\max(d(x, y), d(x, z)) = d(x, z)$ and piecing everything together we find

$$d(y, z) \leq d(x, z) \leq d(y, z),$$

whence the result. □

We will denote by $B(x,r)$ the open ball around x of radius r, $\bar{B}(x,r)$ the closed ball, and $C(x,r) := \{y \in X, \quad d(x,y) = r\}$ the "boundary" of the closed ball.

Proposition 1.5. *Let (X,d) be an ultrametric space and let $x \in X$, $r > 0$.*

(1) For all $y \in B(x,r)$, we have $B(x,r) = B(y,r)$.
(2) For all $y \in \bar{B}(x,r)$ then $\bar{B}(x,r) = \bar{B}(y,r)$.
(3) If $y \in C(x,r)$ then $\bar{B}(y,r') \subset C(x,r)$ for any $0 < r' < r$.
(4) For $y \notin B(x,r)$, put $\varepsilon := d(y,x) \geq r > 0$. Then $B(y,\varepsilon) \subset X \backslash B(x,r)$.
(5) Let $B(x,r)$ and $B(y,r')$ are two open balls with non-empty intersection, then $B(x,r) \subseteq B(y,r')$ or $B(y,r') \subset B(x,r)$.

Proof. We will prove (1), (3) and (5).

(1) Let $y \in B(x,r)$, and let $z \in B(y,r)$. Then

$$d(z,x) \leq \max(d(z,y), d(y,x)) < r$$

so $z \in B(x,r)$, showing $B(y,r) \subseteq B(x,r)$. But $x \in B(y,r)$ so the symmetric argument shows the reverse inclusion.

(3) Let $y \in C(x,r)$, that is $d(y,x) = r$, let $r' < r$ and let $z \in \bar{B}(y,r')$. Since $d(z,y) \leq r' < r = d(y,x)$, the lemma above tells us that $d(z,x) = d(y,x) = r$, so $z \in C(x,r)$, as we claimed.

(5) Let $z \in B(x,r) \cap B(y,r')$. Without loss of generality, we can assume that $r \geq r'$. But then by (1) we find $B(x,r) = B(z,r) \supseteq B(z,r') = B(y,r')$.

□

The above says that any point of an open or closed ball is the center of that ball, and any point in the boundary of a closed ball has a closed ball with non-zero radius around it. In particular, the closed balls and their "boundary" are open. The fourth point says that open balls are closed.

Proposition 1.6. *Let (X,d) be an ultrametric space with at least two elements, and let $T \subset X$ be a subset with at least two elements, with the induced topology. Then T is not connected.*

Proof. Let $x \neq y \in T$ and put $r = d(x,y)/2$. Note that T inherits the metric from X and that the induced topology on T from X is also the topology induced by the metric. Then $B(x,r)$ is non-empty, open and closed, and its completement is also non-empty because it contains y, showing that T is not connected. □

We say that a topological space with the above property is *totally disconnected*.

2. Completions

Definition 2.1. *Let (X, d) be a metric space. Recall that a sequence $(x_n)_{n\in\mathbb{N}}$ in X is called a Cauchy sequence if for all $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$, $d(x_n, x_m) \leq \varepsilon$.*

A metric space (X, d) is called complete if every Cauchy sequence in X admits a limit.

A Cauchy sequence is a sequence whose terms get arbitrarily close together.

Definition 2.2. *Let $(K, |\cdot|_K)$ be a normed field. A completion of K is a normed field $(L, |\cdot|_L)$ together with an isometric field embedding $\iota : K \to L$ (i.e., ι is an injective ring morphism such that $|\iota(x)|_L = |x|_K$ for all $x \in K$) such that $\iota(K)$ is a dense subset in L and L is complete for the metric induced by $|\cdot|_L$ (meaning that any Cauchy sequence converges in L).*

As an example, $\mathbb{R}$ with the usual absolute value $|\cdot|_\infty$ is a completion of $\mathbb{Q}$ with the usual absolute value. In the above definition, we talk about *a* completion, but as we explain below, completions are essentially unique, so going forward we will speak about *the* completion of a normed field. Recall that on a metric space (X, d), and in particular on normed fields, the metric $d : X \times X \to R_{\geq 0}$ is uniformly continuous for the product topology (i.e. for the sup metric d_∞) because of the reverse triangle inequality

$$\forall x, y, z \in X, \quad |d(x, y) - d(y, z)| \leq d(x, z),$$

which implies that for all (x, y), $(x', y') \in X$:

$$\begin{aligned}
\big|d(x, y) - d(x', y')\big| &= \big|d(x, y) - d(x, y') + d(x, y') - d(x', y')\big| \\
&\leq \big|d(x, y) - d(x, y')\big| + \big|d(x, y') - d(x', y')\big| \\
&\leq d(x, x') + d(y, y') \\
&\leq 2\max(d(x, x), d(y, y')) =: 2 \cdot d_\infty((x, x'), (y, y')).
\end{aligned}$$

Proposition 2.3. *Let $(K, |\cdot|_K)$ be a normed field, let $(L, |\cdot|_L, \iota)$ be a completion of K and let $(E, |\cdot|_E)$ be a complete normed field with an isometric field homomorphism $f : (K, |\cdot|_K) \to (E, |\cdot|_E)$. Then f extends uniquely through ι to an isometric field homomorphism $g : (L, |\cdot|_L) \to (E, |\cdot|_E)$.*

Proof. Let $x \in L$. Observe that if g exists, then g is isometric so in particular continuous, and thus if $x = \lim \iota(x_n)$ for $x_n \in K$, then $g(x) = \lim g(\iota(x_n)) = \lim f(x_n)$, so g is completely determined by f, which shows the uniqueness.

Let us abuse notation and consider ι as an inclusion of sets. Since K is dense in L, any x in L is the limit of a sequence in K, and we define

$$g(x) := \lim_{n\to\infty} f(x_n)$$

We have to show that the limit exists and that this expression does not depend of the choice of a sequence in K converging to x. First, since $(x_n)_{n\in\mathbb{N}}$ converges in L, it is a Cauchy sequence in K. Then $(f(x_n))_{n\in\mathbb{N}}$ is a Cauchy

sequence in E: for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $|x_n - x_m|_K \leq \varepsilon$ for all $n, m \geq N$; but f is an isometric field morphism, so we get also

$$|f(x_n) - f(x_m)|_E = |f(x_n - x_m)|_E = |x_n - x_m|_K \leq \varepsilon$$

for all $n, m \geq N$. Since E is complete, the Cauchy sequence $(f(x_n))_{n\in\mathbb{N}}$ converges. If now $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ are two sequences in K converging to x in L, then $|x_n - y_n| \xrightarrow[n\to\infty]{} 0$ so also $|f(x_n) - f(y_n)|_L \xrightarrow[n\to\infty]{} 0$, showing that their image under f have the same limit $g(x)$.

The map g is an isometry: if $x \in L$ is the limit $x = \lim x_n$ of a sequence $(x_n)_{n\in\mathbb{N}}$ in K, we find

$$\begin{aligned} |g(x)|_E = \left|\lim_{n\to\infty} f(x_n)\right|_E = \lim_{n\to\infty} |f(x_n)|_E = \lim_{n\to\infty} |x_n|_K = \lim_{n\to\infty} |x_n|_L \\ = \left|\lim_{n\to\infty} x_n\right|_L \\ = |x|_L \end{aligned}$$

because absolute values are continuous. In particular g is (uniformly) continuous.

Finally, we show that g is a field homomorphism. Since 1 and 0 are already in K we have $g(0) = 0$ and $g(1) = 1$. If x and y are in L, choose sequences $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ in X converging respectively to x and y. Then $x_n + y_n \xrightarrow[n\to\infty]{} x + y$ and $x_n y_n \xrightarrow[n\to\infty]{} xy$, so applying the field homomorphism f and passing to the limit we find $g(x + y) = g(x) + g(y)$, resp. $g(xy) = g(x)g(y)$. □

This proposition tells us that the completion of a normed field K is "the smallest" complete normed field containing K isometrically. Conversely, if K is contained isometrically in a complete normed field L, then the closure of K in L will be a completion of K.

Corollary 2.4. *A completion of a normed field is unique up to a unique isometric field isomorphism.*

Proof. Let $(E, |\cdot|_E, \iota_E)$ and $(F, |\cdot|_F, \iota_F)$ be two completions of K. Then $\iota_F : K \to E$ extends uniquely to an isometric field embedding $\varphi : E \to F$ because F is complete, and similarly ι_E extends uniquely to an isometric field embedding $\psi : F \to E$. Let us show that φ and ψ are inverse to each other. We have $\psi \circ \varphi \circ \iota_E = \psi \circ \iota_F = \iota_E = \mathrm{id_E} \circ \iota_E$ so $\psi \circ \varphi$ and id_E are two isometric field embeddings $E \to E$ extending $\iota_E : K \to E$. By uniqueness, we find $\psi \circ \varphi = \mathrm{id}_E$, and the same argument shows that $\varphi \circ \psi = \mathrm{id}_F$. □

The argument of the corollary always applies to an object defined by a universal property, more generally.

Theorem 2.5. *Let $(K, |\cdot|_K)$ be a normed field. Then $(K, |\cdot|_K)$ admits a completion.*

Before doing the proof, we need a lemma:

Lemma 2.6. *Let (Y,d) be a metric space with a dense subspace X. If every Cauchy sequence in X converges in Y then Y is complete.*

Proof. Let $(y_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in Y. Since X is dense in Y, for every $n\in\mathbb{N}$ we can find an element $x_n\in X$ such that $d(y_n,x_n)\leq 2^{-n}$. Then $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence: for every $\varepsilon>0$, there exists an $N\in\mathbb{N}$ such that both $d(y_n,y_m)\leq\varepsilon$ and $d(x_k,y_k)\leq\varepsilon$ for all $n,m,k\geq N$, whence $d(x_n,x_m)\leq 2\varepsilon$ for all $n,m\geq N$. Therefore $(x_n)_{n\in\mathbb{N}}$ converges in Y to an element $y\in Y$, and we find that (y_n) converges also to y: for every $\varepsilon>0$, there exists an $N\in\mathbb{N}$ such that both $d(x_n,y)\leq\varepsilon$ and $d(x_n,y_n)\leq\varepsilon$ for all $n\geq N$, and thus $d(y_n,y)\leq 2\varepsilon$ for all $n\geq N$. □

Proof of the theorem. Consider the commutative ring $\mathcal{C}$ of sequences $(x_n)_{n\in\mathbb{N}}\in K^{\mathbb{N}}$ that are Cauchy, with pointwise ring operations. The unit is the constant sequence equal to 1. Let us observe that a Cauchy sequence is bounded: there exists an $N\in\mathbb{N}$ such that for all $n,m\geq N$, $|y_n-y_m|\leq 1$, and thus for all $n\geq N$, $|x_n|=|x_n-x_N+x_N|\leq 1+|x_N|$ so that for all $n\in\mathbb{N}$, $|x_n|\leq\max(|x_0|,\dots,|x_{N-1}|,|x_N|+1)$.

We first show that the subset $\mathfrak{m}$ of sequences that converge to 0 is an ideal. The sum of two sequences converging to 0 still converges to 0. Let $(x_n)_{n\in\mathbb{N}}$ be a sequence converging to 0, and let $(y_n)_{n\in\mathbb{N}}$ be a Cauchy sequence. Let $C>0$ be a bound for $(|y_n|)_{n\in\mathbb{N}}$. Then for every $\varepsilon>0$, there exists an $N\in\mathbb{N}$ such that $|x_n|\leq\varepsilon/C$ for all $n\geq N$, and thus $|x_ny_n|\leq\varepsilon$ for all $n\geq N$. Note that two Cauchy sequences $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ are equal in $\mathcal{C}/\mathfrak{m}$ if and only if $|x_n-y_n|\xrightarrow[n\to\infty]{}0$.

Let us now show that $\mathcal{C}/\mathfrak{m}$ is a field. We have to show that every non-zero element is invertible. Thus, let $(x_n)_{n\in\mathbb{N}}\notin\mathfrak{m}$. By definition, there exists $\varepsilon>0$ such that for all $k\in\mathbb{N}$, there exists $M_k\geq k$ with $|x_{M_k}|>\varepsilon$. There exists also $N\in\mathbb{N}$ such that for all $n,m\geq N$, $|x_n-x_m|\leq\varepsilon/2$. Thus for all $n\geq M_N$, we find

$$|x_n|=|x_n-x_{M_n}+x_{M_n}|=|x_{M_n}-(x_{M_N}-x_n)|\geq\big||x_{M_N}|-|x_{M_N}-x_n|\big|>\varepsilon/2$$

so that $x_n\neq 0$ for all $n\geq M_N$. Put

$$y_n=\begin{cases}1 & \text{if } x_n=0\\ 0 & \text{otherwise}\end{cases}$$

Then by the above, $(y_n)_{n\in\mathbb{N}}\in\mathfrak{m}$ and x_n+y_n never vanishes. If we define $z_n=\frac{1}{x_n+y_n}$, we find that $(x_nz_n)_{n\in\mathbb{N}}$ is eventually constant equal to 1, which means that the class of $(z_n)_{n\in\mathbb{N}}$ is an inverse for the class of $(x_n)_{n\in\mathbb{N}}$ in $\mathcal{C}/\mathfrak{m}$. However, we still have to check that $(z_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. For $n\geq M_N$, $z_n=1/x_n$ and we find for $n,m\geq M_N$:

$$|z_m-z_n|=\Big|\frac{1}{x_m}-\frac{1}{x_n}\Big|=\Big|\frac{x_n-x_m}{x_mx_n}\Big|\leq\frac{|x_n-x_m|}{\frac{1}{4}\varepsilon^2}\xrightarrow[n,m\to\infty]{}0.$$

Let us now define an absolute value on $\mathcal{C}/\mathfrak{m}$. The triangle equality implies that $|\cdot|$ is uniformly continuous on K: we have $\big||x|-|y|\big|\leq|x-y|$. Thus

if $(x_n)_{n\in\mathbb{N}} \in \mathcal{C}$, we find that $(|x_n|)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{R}$ hence converges, and so we put

$$|(x_n)_{n\in\mathbb{N}}| := \lim_{n\to\infty} |x_n|$$

If $(x_n)_{n\in\mathbb{N}} \in \mathcal{C}$ and $(y_n)_{n\in\mathbb{N}} \in \mathfrak{m}$, then $|(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}}| = |(x_n)_{n\in\mathbb{N}}|$, so this induces a well-defined absolute value on $\mathcal{C}/\mathfrak{K}$. We skip the verification of the axioms.

The field K embeds into $\mathcal{C}/\mathfrak{m}$ by sending $x \in K$ to the class modulo $\mathfrak{m}$ of the constant sequence $(x)_{n\in\mathbb{N}}$. Let us denote $\iota : x \mapsto (x)_{n\in\mathbb{N}} \mod \mathfrak{m}$ this embedding. The image of K under ι is dense in $\mathcal{C}/\mathfrak{m}$: given an element $y \in \mathcal{C}/\mathfrak{m}$ represented by $(x_n)_{n\in\mathbb{N}}$ and $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $|x_n - x_N| \leq \varepsilon$. Thus we find

$$|y - \iota(x_N)| = \lim_{n\to\infty} |x_n - x_N| \leq \varepsilon$$

i.e. the element $\iota(x_N)$ is close enough to the element $y \in \mathcal{C}/\mathfrak{m}$.

It remains to show that $\mathcal{C}/\mathfrak{m}$ is complete. For this we apply the above lemma, whence it suffices to show that (the image under ι of) a Cauchy sequence in K converges in $\mathcal{C}/\mathfrak{m}$. Let us show that a Cauchy sequence $(x_n)_{n\in\mathbb{N}}$ in K converges to its class y modulo $\mathfrak{m}$ in $\mathcal{C}/\mathfrak{m}$. Let $\varepsilon > 0$; there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $|x_n - x_m| \leq \varepsilon$. But then, for all $n \geq N$:

$$|\iota(x_n) - y| = \lim_{k\to\infty} |x_n - x_k| \leq \varepsilon,$$

so $(\iota(x_n))_{n\in\mathbb{N}}$ converges to y in $\mathcal{C}/\mathfrak{m}$. □

More generally and also less generally in a sense, any metric space admits a completion, that is a complete metric space in which it embedds densely and isometrically. Completions of metric spaces have a similar universal property as above, and thus are unique up to unique isometry. Therefore, the completion of a normed field is its completion as a metric space, which tells us that somehow its completion as a metric space inherits a field structure compatible with the absolute value "for free". It is interesting to work out how this happens using the universal property of the completion of a metric space.

Definition 2.7. *We define $\mathbb{Q}_p$, the field of p-adic numbers, as the completion of $(\mathbb{Q}, |\cdot|_p)$.*

Remark. Let K be a normed field. Then the absolute value on its completion L is continuous and K is dense in L, so the value group $|L|_L \subseteq \mathbb{R}_+$ satisfies

$$|K|_K \subseteq |L|_L \subseteq \overline{|K|_K} \subseteq \mathbb{R}_+.$$

In particular, the value group of $|\cdot|_p$ on $\mathbb{Q}$ is $\{0\} \cup \{p^n, \quad n \in \mathbb{Z}\}$ so the value group of the p-adic absolute value on $\mathbb{Q}_p$ is also $\{0\} \cup \{p^n, \quad n \in \mathbb{Z}\}$. Therefore the map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ also extends to a map $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ satisfying $|x|_p = p^{-v_p(x)}$.

We end this section with a criterion for the convergence of series in a complete non-archimedean normed field.

Proposition 2.8. *Let K be an non-archimedean normed field. Then a sequence $(x_n)_{n\in\mathbb{N}}$ in K is Cauchy if and only if $|x_{n+1}-x_n| \xrightarrow[n\to\infty]{} 0$. In particular, if K is a complete non-archimedean normed field then*

(1) a sequence $(x_n)_{n\in\mathbb{N}}$ converges if and only if $|x_{n+1}-x_n| \xrightarrow[n\to\infty]{} 0$;
(2) a series $\sum_{n\geq 0} x_n$ converges if and only if $x_n \xrightarrow[n\to\infty]{} 0$.

Proof. We check that if a sequence $(x_n)_{n\in\mathbb{N}}$ in K is such that $|x_{n+1}-x_n| \xrightarrow[n\to\infty]{} 0$, then it is Cauchy, and leave the remainder of the proof to the reader. Thus, let $\varepsilon > 0$, and let $N \in \mathbb{N}$ such that $|x_{n+1}-x_n| \leq \varepsilon$ for all $n \geq N$. Then for $n, m \geq N$, without loss of generality we can assume $m \geq n$, and then from the strong triangle inequality we get

$$\begin{aligned} |x_m - x_n| &= |x_m - x_{m-1} + (x_{m-1} - x_{m-2}) + \cdots + (x_{n+1} - x_n)| \\ &\leq \max(|x_m - x_{m-1}|, \ldots, |x_{n+1} - x_n|) \\ &\leq \varepsilon. \end{aligned}$$

□

3. The ring of p-adic integers

Let K be an non-archimedean normed field with a non-trivial absolute value, and denote by $\mathcal{O}_K := \bar{B}(0,1) = \{x \in K, |x| \leq 1\}$ be its unit ball. It turns out that in the presence of the strong triangle inequality, $\mathcal{O}_K$ behaves nicely:

Proposition 3.1. *Let K be an non-archimedean normed field with a non-trivial absolute value.*

(1) The subset $\mathcal{O}_K$ is a subring of K.
(2) The ring $\mathcal{O}_K$ is a local ring with maximal ideal $\mathfrak{m} := B(0,1) = \{x \in K, |x| < 1\}$, so its set of units is $\mathcal{O}_K^\times = \{x \in K, |x| = 1\}$.
(3) The ring $\mathcal{O}_K$ is an integral domain with fraction field K.
(4) For any $t \in \mathfrak{m}\setminus\{0\}$, we have $K = \mathcal{O}_K[1/t]$.

Recall that a local ring is a commutative ring R with a unique maximal ideal $\mathfrak{m}$, or equivalently such that $\mathfrak{m}$ is an ideal and every element in $R\setminus\mathfrak{m}$ is invertible. The subring $\mathcal{O}_K$ is usually called the valuation ring of K, and the quotient field $k := \mathcal{O}_K/\mathfrak{m}$ is called the residue field of k.

Proof. We have $0, 1 \in \mathcal{O}_K$. For $x, y \in \mathcal{O}_K$, we find $|xy| = |x|\,|y| \leq 1$ so $xy \in \mathcal{O}_K$, and

$$|x + y| \leq \max(|x|, |y|) \leq 1$$

by the strong triangle inequality. This shows that $\mathcal{O}_K$ is a subring of K. The same argument shows that $\mathfrak{m}$ is an ideal in $\mathcal{O}_K$.

Let $x \in \mathcal{O}_K \backslash \mathfrak{m}$. Then x is non-zero, so is already invertible in K and it suffices to show that $x^{-1} \in \mathcal{O}_K$. But $\left|x^{-1}\right| = |x|^{-1} = 1^{-1} = 1$, so we are done.

Finally, $\mathcal{O}_K$ is an integral domain since it is a subring of a field: if $xy = 0$ and $x \neq 0$ then x is invertible in K and thus $y = 0$. Moreover, since the absolute value is non-trivial, there exists $t \in \mathfrak{m} \backslash \{0\}$, that is $0 < |t| < 1$. Then for any $x \in K$, there exists $n \geq 0$ such that $|t^n x| = |t|^n |x| \leq 1$, and thus for $y = t^n x \in \mathcal{O}_K$ we have $x = \frac{y}{t^n}$, where both numerators and denominators are in K. This shows that K is the fraction field of $\mathcal{O}_K$ and equal to $\mathcal{O}_K[1/t]$. □

Example 7. Let $K = \mathbb{Q}$ with the p-adic absolute value. Then $\mathcal{O}_K = \mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q}, p \text{ does not divide } b\}$, the localization of $\mathbb{Z}$ at the prime ideal (p), its maximal ideal is $p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q}, p \text{ does not divide } b \text{ and } p \text{ divides } a\}$ and its residue field is $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, the field with p elements. Let us show more generally that there is a canonical isomorphism $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$: there is a natural map $\mathbb{Z} \to \mathbb{Z}_{(p)}$, and the ideal $p^n\mathbb{Z}$ is sent into $p^n\mathbb{Z}_{(p)}$ so all its elements become zero in the quotient $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$. We thus get a factorization:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}_{(p)} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \end{array}$$

and the bottom map is injective because the kernel of the composite map $\mathbb{Z} \to \mathbb{Z}_{(p)} \to \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ is $p^n\mathbb{Z}_{(p)} \cap \mathbb{Z} = p^n\mathbb{Z}$. It thus suffices to show that the bottom map is surjective, i.e. that any element $x \in \mathbb{Z}_{(p)}$ is in the same class modulo $p\mathbb{Z}_{(p)}$ as an element $n \in \mathbb{Z}$. Thus let $x = a/b \in \mathbb{Z}_{(p)}$. Then b is prime to p so there exists $u, v \in \mathbb{Z}$ such that $ub + vp = 1$. Multiplying by x in $\mathbb{Z}_{(p)}$, we find $ua + vpx = x$ so $x \in ua + p\mathbb{Z}_{(p)}$ is in the same class as the integer ua. Alternatively, we could have appealed to the more general fact that localizations and quotients commute.

Observe that in the above, we have shown that for any $x \in \mathbb{Z}_{(p)}$ and $n \geq 1$, there is an $\alpha_n \in \mathbb{Z}$ with $x - \alpha_n \in p^n\mathbb{Z}_{(p)}$, i.e. $|x - \alpha_n|_p \leq p^{-n}$. This shows that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$ for the p-adic topology.

When specializing to $K = \mathbb{Q}_p$, we thus define

Definition 3.2. *The valuation ring of* $\mathbb{Q}_p$*,*

$$\mathbb{Z}_p := \bar{B}(0,1) = \{x \in \mathbb{Q}_p, |x| \leq 1\},$$

is called the ring of p-adic integers.

Taking $t = p$ in the previous proposition, we find $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. We have further good properties in this case, coming from the fact that the map $v_p : \mathbb{Z}_p \backslash \{0\} \to \mathbb{Z}$ has image $\mathbb{Z}$, which is discrete.

Proposition 3.3. *The maximal ideal $\mathfrak{m}$ of $\mathbb{Z}_p$ is the principal ideal $p\mathbb{Z}_p$, and every ideal of $\mathbb{Z}_p$ is either 0 or of the form $p^n\mathbb{Z}_p$ for some $n \geq 0$.*

Proof. If you know the proof that $\mathbb{Z}$ is a principal ideal domain, then this proof should be similar.

Let $x \in \mathbb{Q}_p \setminus \{0\}$ and let $n = v_p(x)$. Then $y := p^{-n}x$ satisfies $|y|_p = p^{-(-n)}p^{-n} = 1$ so $y \in \mathbb{Z}_p^\times$. Thus x is of the form $p^n y$ for an integer $n \in \mathbb{Z}$ and a unit $y \in \mathbb{Z}_p^\times$, and this decomposition is unique: if $y, y' \in \mathbb{Z}_p^\times$ and $n, m \in \mathbb{Z}$ satisfy $p^n y = p^m y'$ in $\mathbb{Q}_p$, then applying v_p we find $n = m$ and thus $y = y'$.

Now $p\mathbb{Z}_p \subset \mathfrak{m}$ since $|p|_p = |p|_p < 1$. Conversely, if $x \in \mathfrak{m}$, we have $|x|_p < 1$ so $|x|_p \leq 1/p = |p|_p$ so for $y = x/p$ we find $|y|_p \leq 1$ and hence $y \in \mathbb{Z}_p$ and $x = py \in p\mathbb{Z}_p$.

Similarly, let I be a non-zero ideal in $\mathbb{Z}_p$. Let $x \in I \setminus \{0\}$ and write $x = p^k y$ with $y \in \mathbb{Z}_p^\times$. Then $|x|_p = p^{-k} \leq 1$ so $k \geq 0$, and $p^k = y^{-1}x \in I$. We now let $n = \min\{k, p^k \in I\}$, which is well-defined by the previous observation. Then clearly $p^n\mathbb{Z}_p \subset I$, and conversely if $x \in I$ we write $x = p^k y$ and find as before $p^k = y^{-1}x \in I$, which by the minimality of n implies $k \geq n$. But then $x = p^n \cdot (p^{k-n}y) \in p^n\mathbb{Z}_p$, which shows the reverse inclusion. □

Proposition 3.4. *We have:*

1. *$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$;*
2. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$; equivalently, given $x \in \mathbb{Z}_p$, for all $n \geq 1$, there exists $\alpha_n \in \mathbb{Z}$ such that $|x - \alpha_n| \leq p^{-n}$, i.e. $x - \alpha_n \in p^n\mathbb{Z}_p$; equivalently, the canonical map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ induced from the inclusion $\mathbb{Z} \to \mathbb{Z}_p$ is an isomorphism. In particular the residue field of $\mathbb{Q}_p$ is the finite field $\mathbb{F}_p$ with p elements.*

Proof. The first assertion follows from the fact that $\mathbb{Z}_{(p)}$ is the valuation ring for the p-adic absolute value on $\mathbb{Q}$. Let $x \in \mathbb{Z}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we can find for all $n \geq 1$ an element $\beta_n \in \mathbb{Q}$ with $|x - \beta_n|_p \leq p^{-n} \leq 1$. In particular by the strong triangle inequality we find $|\beta_n|_p \leq 1$, so $\beta_n \in \mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$. But we already know that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$, so we can find $\alpha_n \in \mathbb{Z}$ with $|\alpha_n - \beta_n|_p \leq p^{-(n+1)}$, which implies by the strong triangle inequality $|x - \alpha_n|_< p^{-n}$, or equivalently $x \in \alpha_n + p^n\mathbb{Z}_p$. The previous discussion around $\mathbb{Z}_{(p)}$ shows the equivalence of the different claims. □

Corollary 3.5. *There is an isomorphism of rings*

$$\mathbb{Z}_p \xrightarrow{\simeq} \varprojlim \mathbb{Z}/p^n\mathbb{Z} := \{(x_n \in \mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}^*}, \quad x_{n+1} \equiv x_n \mod (p^n)\} \subseteq \prod \mathbb{Z}/p^n\mathbb{Z}.$$

Remark. We can define a p-adic valuation on $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ as $v_p((x_n)) = \max(n, x_n = 0)$, and it coincides with the p-adic valuation on $\mathbb{Z}_p$ under the

above isomorphism. It induces a topology on $\lim \mathbb{Z}/p^n\mathbb{Z}$ which can be identified as the subspace topology of $\lim \mathbb{Z}/p^n\mathbb{Z} \subset \prod \mathbb{Z}/p^n\mathbb{Z}$, where the latter has the product topology where each term is considered as a discrete topological space. Since each $\mathbb{Z}/p^n\mathbb{Z}$ is discrete and finite, it is compact. Tychonov's theorem states that a product of compact Hausdorff topological spaces, with the product topology, is compact Hausdorff[2]. This can be used to show that $\mathbb{Z}_p$ is compact, because $\lim \mathbb{Z}/p^n\mathbb{Z}$ is a closed subset of $\prod \mathbb{Z}/p^n\mathbb{Z}$, hence also compact Hausdorff. This tells us that we could have started with the above definition to define $\mathbb{Z}_p$ as a topological ring, and then put $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. We will not choose this route to show the compactness of $\mathbb{Z}_p$, but instead take a more direct approach.

Proof. Given an element $x \in \mathbb{Z}_p$, we map it to the family $(x \mod (p^n\mathbb{Z}_p))$ which gives an element of $\lim \mathbb{Z}/p^n\mathbb{Z}$. We leave to the reader to check that this is a morphism of rings. Now if x is sent to 0, this means that $x \in p^n\mathbb{Z}_p$ for all $n \geq 1$, and hence that $|x|_p \leq p^{-n}$ for all $n \geq 1$, so $x = 0$. This shows the injectivity. If $(x_n) \in \lim \mathbb{Z}/p^n\mathbb{Z}$, choose a lift $\widetilde{x_n} \in \mathbb{Z}$ of the class $x_n \in \mathbb{Z}/p^n\mathbb{Z}$. Then $\widetilde{x_{n+1}} - \widetilde{x_n} \equiv x_{n+1} - x_n \equiv x_n - x_n \equiv 0 \mod (p^n)$ so $(\widetilde{x_n})_{n\in\mathbb{N}}$ is a Cauchy sequence (because $|\cdot|_p$ is ultrametric!) hence converges in $\mathbb{Z}_p$ to an element $x \in \mathbb{Z}_p$. But then for any $n \geq 1$, taking $\varepsilon = p^{-n}$ gives the existence of $N \geq n$ such that for all $m \geq N$, $|x - \widetilde{x_m}|_p \leq p^{-n}$. In particular

$$x \equiv \widetilde{x_N} \equiv x_N \equiv x_n \mod (p^n)$$

so x is the required lift. □

Observe that in the above proof, we could have asked that $\widetilde{x_n} \in \{0, \dots, p^n - 1\}$ in which case $\widetilde{x_n}$ would have been uniquely determined by x_n. Thus, because the above is an isomorphism of ring, any $x \in \mathbb{Z}_p$ is the limit of a *unique* sequence of integers $(\alpha_n)_{n\in\mathbb{N}^*}$ with $\alpha_n \in \{0, \dots, p^n - 1\}$ and $|x - \alpha_n|_p \leq p^{-n}$. If we now write $\alpha_n = a_0^{(n)} + a_1^{(n)}p + \cdots + a_{n-1}^{(n)}p^{n-1}$ the expansion in base p with $a_i^{(n)} \in \{0, \dots, p-1\}$, we find for $n \geq m$ that $|\alpha_n - \alpha_m|_p \leq p^{-n}$, so $\alpha_n \equiv \alpha_m \mod (p^m)$ which implies $a_0^{(n)} = a_0^{(m)}$, …, $a_{m-1}^{(m)} = a_{m-1}^{(n)}$. Thus, put $a_m = a_m^{(n)}$ for any $n \geq m$. Then the series $\sum_{n\geq 0} a_n p^n$ converges to $\lim \alpha_n = x$, i.e. any element $x \in \mathbb{Z}_p$ has a unique expansion in base p with potentially infinitely many digits on the left (contrarily to the decimal expansion of a rational number where you get infinitely many digits on the right). Any element of $\mathbb{Q}_p$ can be made to land in $\mathbb{Z}_p$ after multiplying by a big enough power of p, so similarly elements in $\mathbb{Q}_p$ have a unique p-adic expansion $x = \sum_{n\geq -m} a_n p^n$ for some $m \geq 0$.

Proposition 3.6. *Let X be a complete metric space. Then X is compact if and only if it for every $\varepsilon > 0$, X can be covered by finitely many balls of radius $\leq \varepsilon$.*

[2]Tychonov's theorem in its general version is equivalent to the axiom of choice, but in our case we only need a version for countable products which is weaker.

The latter condition is called being *totally bounded*.

Proof. If X is compact, then we can consider the cover $X = \bigcup_{x \in X} B(x, \varepsilon)$, which admits a finite subcover. Conversely, since X is a metric space it suffices to show that any sequence has a convergent subsequence, and because X is complete it suffices to show that any sequence has a Cauchy subsequence. Thus let $(x_n)_{n \in \mathbb{N}}$ be a sequence in X. Construct inductively strictly increasing functions $\varphi_k : \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$, $x_{\varphi_0 \circ \cdots \circ \varphi_k(n)}$ is in a single ball of radius 2^{-k}; this is done by observing that if φ_0 to φ_{k-1} have already been constructed, we can cover X by finitely many balls of radius 2^{-k}, and thus the sequence $(x_{\varphi_0 \circ \cdots \circ \varphi_{k-1}(n)})_{n \in \mathbb{N}}$ must have infinitely many terms in one of them, and we can choose a strictly increasing function $\varphi_k : \mathbb{N} \to \mathbb{N}$ such that $(x_{\varphi_0 \circ \cdots \circ \varphi_k(n)})_{n \in \mathbb{N}}$ is the subsequence picking those elements.

We now use a diagonal argument to extract a single subsequence: consider the strictly increasing function

$$\varphi(n) := \varphi_0 \circ \cdots \circ \varphi_n(n).$$

Then by construction, for all $n \geq k$, the terms $x_{\varphi(n)}$ are in a single ball of radius 2^{-k}, because for those n we have

$$\varphi(n) = \varphi_0 \circ \cdots \circ \varphi_k(\varphi_{k+1} \circ \cdots \circ \varphi_n(n)) = \varphi_0 \circ \cdots \circ \varphi_k(\text{something}).$$

Put in other terms, for all $n, m \geq k$ the terms $x_{\varphi(n)}$, $x_{\varphi(m)}$) are in a ball $B(y, 2^{-k})$ and thus

$$d(x_{\varphi(n)}, x_{\varphi(m)})) \leq d(x_{\varphi(n)}, y) + d(y, x_{\varphi(m)}) \leq 2 \cdot 2^{-k}$$

which shows that $(x_{\varphi(n)})_{n \in \mathbb{N}}$ is the sought-after Cauchy subsequence. □

Remark. More generally, a metric space is compact if and only if it is complete and totally bounded.

Corollary 3.7. *$\mathbb{Z}_p$ is compact for its natural topology, $\mathbb{Q}_p$ is locally compact.*

Proof. Since $\mathbb{Z}_p$ is the closed unit ball in the complete space $\mathbb{Q}_p$, $\mathbb{Z}_p$ is a complete space. Hence it suffices to show that for any $n \geq 1$, $\mathbb{Z}_p$ is covered by finitely many balls of radius p^{-n}. Observe now that any ball $B(x, p^{-n})$ of radius p^{-n} and center $x \in \mathbb{Z}_p$ is exactly the coset $x + p^n\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is the disjoint union of its cosets modulo $p^n\mathbb{Z}_p$, we have to show equivalently that there are finitely many cosets, which we already proved since the set of cosets is the finite quotient ring $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$. Finally, any closed ball in $\mathbb{Q}_p$ is of the form $x + p^n\mathbb{Z}_p$ for some $x \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$, so is compact because dilation and translation are continuous thus preserve compacts. □

Remark. The above proof shows more generally that if K is a complete non-archimedean normed field with a non-trivial discrete valuation, then the following are equivalent:

(1) K is locally compact;
(2) the valuation ring $\mathcal{O}_K$ is compact;
(3) the residue field $\mathcal{O}_K/\mathfrak{m}$ is finite

Indeed the argument above shows (2) $\Leftrightarrow$ (3) and (2) $\implies$ (1), and if K is locally compact, then there is a neighbourhood of 0 that is compact; since it is a neighbourhood of 0, it must contain an open ball around 0 of non-zero radius, so also a closed ball of smaller radius $r > 0$, and that closed ball must be compact as a closed subset of a compact Hausdorff space. We can always choose $r > 0$ small enough such that $r = |y|$ for some $y \in \mathcal{O}_K$, but then $B(0, r) = y\mathcal{O}_K$ is homeomorphic to $\mathcal{O}_K$ so the latter is also compact. This shows (1) $\implies$ (2).

Remark. It can be shown, using the previous remark among other things, that the following list is up to isometric isomorphism the complete list of complete locally compact normed field with a non-trivial absolute value:

- the field of Laurent series $\mathbb{F}_q((T))$ over a finite field $\mathbb{F}_q$ with q elements, with the T-adic valuation; this is the fraction field of the ring of formal power series, and the completion of the field $\mathbb{F}_q(T)$ of rational fractions for the absolute value induced by the T-adic valuation;
- $\mathbb{R}$ and $\mathbb{C}$ with the usual absolute value $|\cdot|_\infty$;
- $\mathbb{Q}_p$ and its finite extensions (we will see later that on those, there exists a unique absolute value extending that on $\mathbb{Q}_p$).

4. Aside: route through Tychonov's theorem

Warning, notations are horrible.

Theorem 4.1 (Tychonov's theorem, very weak version)**.** *A countable product of finite discrete spaces is compact and Hausdorff.*

Recall that open sets for the product topology are generated by subsets of the form $\prod_{i\in I} \Omega_i \times \prod_{i\notin I} X_i$ where I is a finite set of indices and Ω_i is open in X_i. Here, this means that Ω_i is any subset of X_i; thus we can further restrict to Ω_i being a singleton without changing the generated topology, because any subset of X_i is a union of its elements.

Before doing the proof, we need the following lemma:

Lemma 4.2. *Let $(X_i)_{i\in\mathbb{N}}$ be a countable family of finite discrete spaces. Then the function*

$$d : \begin{cases} \prod X_i \times \prod X_i & \longrightarrow & \mathbb{R}_+ \\ (x^{(i)}), (y^{(i)}) & \mapsto & \sum_{i\geq 0} \frac{1}{2^i} d(x_i, y_i) \end{cases}$$

is a metric on $\prod X_i$ inducing the product topology. In particular, the product topology on $\prod X_i$ is metrizable and Hausdorff.

Proof. We leave the verification that it is a metric to the reader. Since $\sum_{i\geq n} \frac{1}{2^i} = 2^{-n+1}$, we have that

$$d((x^{(i)}), (y^{(i)})) \leq 2^{-n+1} \text{ whenever } x^{(i)} = y^{(i)} \text{ for all } i < n.$$

We have observed that the generating opens for the product topology are of the form $\left\{x^{(0)}\right\} \times \cdots \times \left\{x^{(n-1)}\right\} \times \prod_{i\geq n} X_i$; choosing furthermore elements

$x^{(i)} \in X_i$ for $i \geq n$, we find that such a generating open is included in the open ball $B((x^i), 2^{-n+1})$.

Conversely, if $(x^{(i)}) \in \prod X_i$ and $r > 0$, for an element $(y^{(i)}) \in B((x^{(i)}), r)$, taking $r' = \frac{r - d((x^{(i)}),(y^{(i)}))}{2}$ we find that the open ball around $(y^{(i)})$ of radius $r' < r$ is completely included in $B((x^{(i)}), r)$. There exists an integer $n \geq 1$ such that $2^{-n+1} < r'$, which then shows that the generating open $\{y^{(0)}\} \times \cdots \times \{y^{(n-1)}\} \times \prod_{i \geq n} X_i$ contains $(y^{(i)})$ and is included in $B((y^{(i)}), r')$ and thus also in $B((x^{(i)}), r)$. □

Proof of the theorem. Since the topology is induced by a metric, the space is Hausdorff, and is compact if it is sequentially compact.

Let $(x_n)_{n \in \mathbb{N}} = ((x_n^{(i)}))$ be a sequence in $\prod X_i$. We will use a diagonal argument to extract a converging subsequence. Observe that since X_0 is finite, there must be infinitely many terms $x_n \in \prod X_i$ that share the same value $x_n^{(0)} \in X_0$. Thus we find a strictly increasing function $\varphi_0 : \mathbb{N} \to \mathbb{N}$ such that $(x^{(0)}_{\varphi_0(n)})v$ is constant. We now proceed by induction. Assume we have constructed strictly increasing functions $\varphi_0, \ldots, \varphi_{n-1} : \mathbb{N} \to \mathbb{N}$ such that $(x^{(k)}_{\phi_0 \circ \cdots \circ \phi_k(n)})$ is constant for all $0 \leq k \leq n-1$. Then $(x^{(n)}_{\varphi_0 \circ \cdots \circ \varphi_{n-1}(n)})$ can take only finitely many values since X_n is finite, thus we can find a strictly increasing function $\varphi_n : \mathbb{N} \to \mathbb{N}$ such that $(x^{(n)}_{\varphi_0 \circ \circ \cdots \circ \varphi_n(n)})$ is constant.

Now, put

$$\varphi(n) := \varphi_0 \circ \cdots \circ \varphi_n(n)$$

Then the subsequence $(x_{\varphi(n)})$ is by construction such that its k-th component $(x^{(k)}_{\varphi(n)})$ is constant for $n \geq k$, because for such an n we have

$$\varphi(n) = \varphi_0 \circ \cdots \circ \varphi_k(\varphi_{k+1} \circ \cdots \circ \varphi_n(n)) = \varphi_0 \circ \cdots \circ \varphi_k(\text{something}).$$

Let $y^{(k)} \in X_k$ denote the common constant value of $(x^{(k)}_{\varphi(n)})$ is for $n \geq k$. Then since $y^{(k)} = x^{(k)}_{\varphi(n)}$ for all $k \geq n$, we have

$$d((y^{(k)}), x_{\varphi(n)}) \leq 2^{-n}$$

(as we observed in the previous proof) and so $(x_{\varphi(n)})$ converges to $(y^{(k)}) \in \prod X_i$. □

Before showing that $\lim \mathbb{Z}/p^n\mathbb{Z}$ is compact, we need a reminder on Hausdorff topological spaces.

Proposition 4.3. *Let X be a topological space and let $\Delta_X \subset X \times X$ denote the diagonal $\{(x, x) \in X \times X\}$ in $X \times X$. Endow $X \times X$ with the product topology. Then X is Hausdorff if and only if Δ_X is closed in X.*

Proof. If X is Hausdorff, for a point $(x, y) \in (X \times X) \backslash \Delta_X$ we have $x \neq y$, so there exists open U, V containing respectively x, y such that $U \cap V = \emptyset$. Thus we find that $U \times V$ is an open of $X \times X$ containing (x, y) but $(U \times V) \cap \Delta_X = \emptyset$, since any point (x, x) in that intersection would have $x \in U$ and $x \in V$.

Conversely, if Δ_X is closed then for any $x \neq y$ in X, $(x,y) \notin \Delta_X$ so we can find a generating open $U \times V \subset (X \times X) \backslash \Delta_X$ with $(x,y) \in U \times V$. Unwrapping the definitions we find that $x \in U, y \in V$ and $U \cap V = \emptyset$. □

Proposition 4.4. *Let X be a topological space and let Y be a Hausdorff topological space with two continuous maps $f, g : X \to Y$. Then the subset $S = \{x \in X, f(x) = g(x)\}$ is closed in X.*

Proof. Consider the map $(f,g) : X \to Y \times Y$. Then (f,g) is continuous since $(f,g)^{-1}(U \times V) = f^{-1}(U) \cap g^{-1}(V)$ is open in X for any two opens U, V of Y. Therefore the set

$$S = (f,g)^{-1}(\Delta_Y)$$

is closed in X. □

Corollary 4.5. *The ring $\lim \mathbb{Z}/p^n\mathbb{Z}$ is compact for the subspace topology.*

Proof. We have to show that $\lim \mathbb{Z}/p^n\mathbb{Z}$ is closed in $\prod \mathbb{Z}/p^n\mathbb{Z}$. Consider the map

$$\text{shift} : \left\{ \begin{array}{ccc} \prod \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \prod \mathbb{Z}/p^n\mathbb{Z} \\ (x_n)_{n\in\mathbb{N}} & \mapsto & (x_{n+1} \mod (p^n))_{n\in\mathbb{N}}. \end{array} \right.$$

This is continuous, since its composition with the projection $\prod_n \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ identifies with the composition $\prod_n \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ where the first map is a projection hence continuous and the second map is a map of discrete spaces. Observe now that we have

$$\lim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_n \mathbb{Z}/p^n\mathbb{Z}, \quad \text{shift}((x_n)_{n\in\mathbb{N}}) = (x_n)_{n\in\mathbb{N}} \right\}.$$

We are done by the previous proposition. □

Proposition 4.6. *The restriction of the p-adic valuation to $\mathbb{Z}_p$ induces a p-adic valuation v_p on $\lim \mathbb{Z}/p^n\mathbb{Z}$ via the isomorphism $\mathbb{Z}_p \simeq \lim \mathbb{Z}/p^n\mathbb{Z}$, computed as $v_p((x_n)_{n\in\mathbb{N}}) = \max(k \in \mathbb{N}, \quad x_k = 0)$.[3] Similarly, we get an induced metric on $\lim \mathbb{Z}/p^n\mathbb{Z}$ given by $d((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) = p^{-v_p((x_n - y_n))_{n\in\mathbb{N}}}$. The topology induced by that metric is the subspace topology of the product topology on $\prod \mathbb{Z}/p^n\mathbb{Z}$. In other words, the isomorphism of rings*

$$\mathbb{Z}_p \xrightarrow{\simeq} \lim \mathbb{Z}/p^n\mathbb{Z}$$

is a homeomorphism, for the topology induced by the p-adic absolute value on $\mathbb{Q}_p$ on the left, and the subspace topology of the product topology on $\prod \mathbb{Z}/p^n\mathbb{Z}$ on the right. In particular, $\mathbb{Z}_p$ is compact.

Proof. We leave the proof of the first claim to the reader. Recall that the product topology is induced by

$$d_{\text{prod}}((x_n),(y_n)) = \sum_{n\geq 1} 2^{-n} d_{\text{triv}}(x_n, y_n)$$

[3] with the convention $x_0 = 0$.

Since the trivial distance d_{triv} is induced by the trivial absolute value $|\cdot|_{\text{triv}}$ on $\mathbb{Z}/p^n\mathbb{Z}$ (this notion of absolute value also makes sense for a commutative ring !), we can define a "weak absolute value" (not necessarily multiplicative but still satisfying the triangle inequality, and sending -1 to 1) $|\cdot|_{\text{prod}}$ on $\prod \mathbb{Z}/p^n\mathbb{Z}$ by

$$|(x_n)_{n\in\mathbb{N}}|_{\text{prod}} = \sum_{n\geq 1} 2^{-n} |x_n|_{\text{triv}}$$

Since we have

$$d_{\text{prod}}((x_n),(y_n)) = \sum_{n\geq 1} 2^{-n} |x_n - y_n|_{\text{triv}} = |(x_n) - (y_n)|_{\text{prod}},$$

this weak absolute value induces our metric hence the product topology. Hence we are reduced to showing that open balls around 0 for the restriction of $|\cdot|_{\text{prod}}$ to $\lim \mathbb{Z}/p^n$ and for $|\cdot|_p$ are interlocked.

Observe that for $(x_n)_{n\in\mathbb{N}} \in \lim \mathbb{Z}/p^n$, if $x_n = 0$ then $x_k = 0$ for all $k \leq n$. The first index n such that $x_n \neq 0$ is by definition $v_p((x_n)) + 1$. Hence we find

$$|(x_n)|_{\text{prod}} = \sum_{i=1}^{v_p((x_n))} 2^{-i} \cdot 0 + \sum_{i > v_p((x_n))} 2^{-i} \cdot 1 = 2^{-v_p((x_n))}$$

It is now clear that $|(x_n)|_{\text{prod}} = |(x_n)|_p^{\ln(2)/\ln(p)}$, which shows that $|\cdot|_{\text{prod}}$ is an absolute value on $\lim \mathbb{Z}/p^n$ equivalent to $|\cdot|_p$, so we are done. □

5. Hensel's lemma

In real analysis, we have Newton's method to try and find a zero of some $\mathcal{C}^1$-function $f : I \to \mathbb{R}$. We start at a point $x_0 \in I$ such that the slope of f at x_0 is non-zero, i.e. $f'(x_0) \neq 0$. We then go down the affine line of that slope from the point of coordinate $(x_0, f(x_0))$ to a new point $(x_1, 0)$. Then we can try to iterate the process, and sometimes it will converge to a zero of f. The affine line passing through $(x_0, f(x_0))$ of slope $f'(x_0)$ has equation $y = f'(x_0)(x - x_0) + f(x_0)$. Thus its intersection with the line $y = 0$ gives

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

However, in some cases it does not converge: see for instance fig. I.2 p. 18 in Koblitz's book. In a complete non-archimedean normed field however, it will converge:

Theorem 5.1 (Hensel's lemma)**.** *Let K be a complete non-archimedean normed field, valuation ring $\mathcal{O}_K$ and maximal ideal $\mathfrak{m}$. Let $P \in \mathcal{O}_K[X]$ and suppose that there exists an element $\alpha_0 \in \mathcal{O}_K$ with*

$$|P(\alpha_0)| < \left|P'(\alpha_0)\right|^2.$$

Then, in the open ball $B(\alpha_0, |P'(\alpha_0)|)$, there exists a unique $\alpha \in \mathcal{O}_K$ such that $P(\alpha) = 0$. Moreover:

(1) *Newton's method for P starting from α_0 converges to α with an exponentially decreasing error term;*
(2) $|\alpha - \alpha_0| = |P(\alpha_0)/P'(\alpha_0)|$;
(3) $|P'(\alpha)| = |P'(\alpha_0)|$.

Proof. Note that $|P'(\alpha_0)|^2 > |P(\alpha_0)| \geq 0$ so $P'(\alpha_0) \neq 0$. Let us start by observing what happens when doing one iteration of Newton's method; thus, put

$$\alpha_1 = \alpha_0 - P(\alpha_0)/P'(\alpha_0).$$

Since $\alpha_0 \in \mathcal{O}_K$, we have $P'(\alpha_0) \in \mathcal{O}_K$, and the hypothesis then gives

$$\left|\frac{P(\alpha_0)}{P'(\alpha_0)}\right| < \left|P'(\alpha_0)\right| \leq 1$$

so that $P(\alpha_0)/P'(\alpha_0) \in \mathcal{O}_K$ and thus $\alpha_1 \in \mathcal{O}_K$. We will need a polynomial identity:

$$P(X+Y) = P(X) + P'(X)Y + Q(X,Y)Y^2,$$

for some polynomial $Q \in \mathcal{O}_K[X,Y]$. To prove it, take the binomial expansion of $(X+Y)^k$ and collect only the first two terms X^k and $kX^{k-1}Y$, giving

$$\begin{aligned} P(X+Y) = \sum a_k(X+Y)^k &= \sum a_k(X^k + kX^{k-1}Y + Y^2(\cdots)) \\ &= (\sum a_k X^k) + (\sum k a_k X^{k-1})Y + Y^2(\cdots) \\ &= P(X) + P'(X)Y + Y^2(\cdots). \end{aligned}$$

Put $t = \left|P(\alpha_0)/P'(\alpha_0)^2\right| < 1$. We apply our polynomial identity to α_1:

$$\begin{aligned} P(\alpha_1) &= P(\alpha_0 - \frac{P(\alpha_0)}{P'(\alpha_0)}) \\ &= P(\alpha_0) - P'(\alpha_0)\cdot\frac{P(\alpha_0)}{P'(\alpha_0)} + Q\big(\alpha_0, -\frac{P(\alpha_0)}{P'(\alpha_0)}\big)\cdot\big(-\frac{P(\alpha_0)}{P'(\alpha_0)}\big)^2 \end{aligned}$$

hence

$$P(\alpha_1) = Q\big(\alpha_0, -\frac{P(\alpha_0)}{P'(\alpha_0)}\big)\cdot\big(\frac{P(\alpha_0)}{P'(\alpha_0)}\big)^2$$

Taking absolute values, we find

$$|P(\alpha_1)| = \left|Q\big(\alpha_0, \frac{P(\alpha_0)}{P'(\alpha_0)}\big)\right|\left|\big(\frac{P(\alpha_0)}{P'(\alpha_0)}\big)^2\right| \leq \left|\frac{P(\alpha_0)}{P'(\alpha_0)}\right|^2 = \left|P'(\alpha_0)\right|^2\cdot t^2. \tag{5.1}$$

By definition, $|\alpha_1 - \alpha_0| = \left|\frac{P(\alpha_0)}{P'(\alpha_0)}\right| = |P'(\alpha_0)|\cdot t$. Moreover, applying our polynomial identity to P', we find in particular

$$P'(X+Y) = P'(X) + YR(X,Y)$$

for some polynomial $R(X,Y) \in \mathcal{O}_K[X,Y]$. Again, we apply this to α_1 and find

$$P'(\alpha_1) = P'(\alpha_0) - \frac{P(\alpha_0)}{P'(\alpha_0)}\cdot R\big(\alpha_0, -\frac{P(\alpha_0)}{P'(\alpha_0)}\big).$$

We have

$$\begin{aligned}\left|\frac{P(\alpha_0)}{P'(\alpha_0)}\cdot R\big(\alpha_0,-\frac{P(\alpha_0)}{P'(\alpha_0)}\big)\right| &\leq \left|\frac{P(\alpha_0)}{P'(\alpha_0)}\right| \\ &< \left|P'(\alpha_0)\right|\end{aligned}$$

by the hypothesis, and thus by the equality case of the ultrametric inequality:

$$\left|P'(\alpha_1)\right| = \left|P'(\alpha_0)\right|;$$

in particular $P'(\alpha_1) \neq 0$. To be able to iterate further with α_1, we look at the new ratio $P(\alpha_1)/P'(\alpha_1)^2$ and use (5.1):

$$\left|\frac{P(\alpha_1)}{P'(\alpha_1)^2}\right| = \frac{|P(\alpha_1)|}{|P'(\alpha_0)|^2} \leq t^2. \tag{5.2}$$

The above analysis shows, by induction, that the sequence from Newton's method

$$\alpha_{n+1} = \alpha_n - \frac{P(\alpha_n)}{P'(\alpha_n)}.$$

is well-defined, has terms $\alpha_n \in \mathcal{O}_K$, and satisfies

$$\left|P'(\alpha_n)\right| = \left|P'(\alpha_0)\right| \tag{5.3}$$

for all $n \in \mathbb{N}$. We will show moreover by induction that

$$|P(\alpha_n)| \leq \left|P'(\alpha_0)\right|^2 \cdot t^{2^n}. \tag{5.4}$$

This is equivalent to showing that

$$\frac{|P(\alpha_n)|}{|P'(\alpha_n)|^2} \leq t^{2^n}.$$

But the analysis above, combined with the induction hypothesis, shows

$$\frac{|P(\alpha_{n+1})|}{|P'(\alpha_{n+1})|^2} \leq \big(\frac{|P(\alpha_n)|}{|P'(\alpha_n)|^2}\big)^2 \leq (t^{2^n})^2 = t^{2^{n+1}}$$

and we are done. Finally, we get

$$|\alpha_{n+1} - \alpha_n| = \left|\frac{P(\alpha_n)}{P'(\alpha_n)}\right| = \frac{|P(\alpha_n)|}{|P'(\alpha_0)|} \leq \left|P'(\alpha_0)\right| \cdot t^{2^n}$$

so the sequence $(\alpha_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathcal{O}_K$ and thus converges to some $\alpha \in \mathcal{O}_K$. First, by continuity, taking the limit in eqs. (5.3) and (5.4) we get

$$P(\alpha) = 0, \quad \left|P'(\alpha)\right| = \left|P'(\alpha_0)\right|.$$

This shows that α is a root of P and claim (3).

Moreover, by the strong triangle inequality we have for all $m \geq n$:

$$|\alpha_m - \alpha_n| \leq \left|P'(\alpha_0)\right| \cdot t^{2^n}$$

and thus by continuity of the absolute value

$$|\alpha - \alpha_n| \leq \left|P'(\alpha_0)\right| \cdot t^{2^n},$$

which shows claim (1) about the rate of convergence. Additionally, for $n > 0$ we have

$$|\alpha_1 - \alpha_0| = \left|\frac{P(\alpha_0)}{P'(\alpha_0)}\right|$$

$$|\alpha_{n+1} - \alpha_n| \leq \left|P'(\alpha_0)\right| \cdot t^{2^n} < \left|P'(\alpha_0)\right| \cdot t = \left|\frac{P(\alpha_0)}{P'(\alpha_0)}\right|.$$

Therefore the equality case of the strong triangle inequality gives

$$|\alpha_n - \alpha_0| = \left|\frac{P(\alpha_0)}{P'(\alpha_0)}\right|$$

and we get claim (2) by continuity.

It remains to show the uniqueness of a solution α to $P(\alpha) = 0$ satisfying $|\alpha - \alpha_0| < |P'(\alpha_0)|$. Suppose $\beta \in \mathcal{O}_K$ is another solution. Then

$$|\beta - \alpha| \leq \max(|\beta - \alpha_0|, |\alpha - \alpha_0|) < \left|P'(\alpha_0)\right|.$$

Write $\beta = \alpha + h$ with $|h| < |P'(\alpha_0)|$. Using our above polynomial identity, we find

$$0 = P(\beta) = P(\alpha) + hP'(\alpha) + h^2Q(\alpha, h) = hP'(\alpha) + h^2Q(\alpha, h).$$

Thus if $h \neq 0$ we find $P'(\alpha) = -hQ(\alpha, h)$ and thus

$$\left|P'(\alpha)\right| \leq |h| < \left|P'(\alpha_0)\right|,$$

contrarily to what we proved. In conclusion, $h = 0$ and $\beta = \alpha$. □

Remark. Newton's method has a multivariate version, using the differential of a $\mathcal{C}^1$ function $f : \mathbb{R}^n \to \mathbb{R}^n$ to figure out which direction to go to in order to find a zero (i.e. an element sent to $(0, \ldots, 0)$). Similarly, there is a version of Hensel's lemma for d polynomials in d variables; google[4] Keith Conrad's note *A multivariate Hensel lemma* to find out more.

Corollary 5.2 (Hensel's lemma, simple root version)**.** *In the above setting, suppose that* $P(\alpha_0) \equiv 0 \mod \mathfrak{m}$ *and* $P'(\alpha_0) \not\equiv 0 \mod \mathfrak{m}$*, then the same conclusions hold, and in particular the root* α *is the unique root of* P *satisfying* $\alpha \equiv \alpha_0 \mod \mathfrak{m}$.

Proof. The hypothesis says that $|P(\alpha_0)| < 1$ and $|P'(\alpha_0)| = 1$, hence

$$|P(\alpha_0)| < \left|P'(\alpha_0)\right|^2.$$

□

In other words, if the reduction of P mod $\mathfrak{m}$ has a simple root in the residue field $k = \mathcal{O}_K/\mathfrak{m}$, then we can lift it to a root of P in $\mathcal{O}_K$; moreover, this is done by choosing an arbitrary lift of the root of the reduction of P, then applying Newton's method to it, which converges very fast: for instance, working with $\mathbb{Z}_p$, knowing the root modulo p means knowing its 0-th digit

[4]Or go to `https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf`

in base p, and Newton's method will double the number of correct digits at each step.

Remark. In the case where the valuation is discrete, the above corollary can also be proven directly by finding successive lifts modulo π^n, where π is an element of minimum non-zero valuation. See e.g. Gouvêa's book.

Here are some examples:

Example 8. 2 has a unique cubic root in $\mathbb{Z}_5$: indeed, we need to find a root of the polynomial $f(X) = X^3 - 2 \in \mathbb{Z}_5[X]$. Reducing modulo 5, we find that

$$f(3) \equiv 3^2 \cdot 3 - 2 \equiv 9 \cdot 3 - 2 \equiv 4 \cdot 3 - 2 \equiv 12 - 2 \equiv 2 - 2 \equiv 0 \mod (5)$$

and $f'(X) = 3X^2$ so $f'(3) = 27 \not\equiv 0 \mod (5)$. Hensel's lemma concludes that there exists a unique $\alpha \in \mathbb{Z}_5$ with $\alpha^3 = 2$ and $\alpha \equiv 3 \mod (5)$. Moreover, we can compute $f(0) \equiv 3 \mod (5)$, $f(1) \equiv 4 \mod (5)$, $f(4) \equiv 16 \cdot 4 - 2 \equiv 4 - 2 \equiv 2 \mod (5)$ so f has no other root in $\mathbb{Z}_5/(5)$, thus also necessarily no other root in $\mathbb{Z}_5$.

Example 9. 5 has no cubic roots in $\mathbb{Z}_3$. If it did, we would have a solution to $X^3 \equiv 5 \mod (9)$. But we can compute the cubes modulo 9:

$x \mod (9)$	0	1	2	3	4	5	6	7	8
$x^3 \mod (9)$	0	1	8	0	1	8	0	1	8

hence 5 is not a cube modulo 9.

Example 10. 10 has a cubic root in $\mathbb{Z}_3$. Since $10 \equiv 1 \equiv 1^3 \mod (3)$, we have the factorization $X^3 - 10 \equiv (X-1)^3 \mod (3)$. But then 1 is not a simple root of $P(X) = X^3 - 10$ modulo 3 so we cannot apply the corollary directly and we need the stronger version. Modulo 9, referring to the table from the previous example we find that 1, 4 and 7 are cubic roots of $10 \equiv 1 \mod (9)$. We then compute

$$\begin{aligned} P(1) &= -9 = -3^2, \\ P'(1) &= 3, \\ P(4) &= 54 = 2 \cdot 3^3, \\ P'(4) &= 4^2 \cdot 3, \\ P(7) &= 333 = 37 \cdot 3^2, \\ P'(7) &= 7^2 \cdot 3 \end{aligned}$$

so

$$\begin{aligned} v_3(P(1)) &= 2 = 2v_3(P'(1)), \\ v_3(P(4)) &= 3 > 2 = 2v_3(P'(4)), \\ v_3(P(7)) &= 2 = v_3(P'(7)) \end{aligned}$$

i.e.

$$|P(1)|_3 = \left|P'(1)\right|_3^2$$
$$|P(4)|_3 < \left|P'(4)\right|_3^2$$
$$|P(7)|_3 = \left|P'(7)\right|_3^2$$

We obtain from Hensel's lemma that there is a unique root $\alpha \in \mathbb{Z}_3$ with $|\alpha - 4|_3 < |P'(4)|_3 = 3^{-1}$, hence equivalently with $|\alpha - 4|_3 \leq 3^{-2}$ or $\alpha \equiv 4 \mod (9)$.

On the other hand, modulo 27 we find that none of the lifts $(1 \mod (27))$, $(10 \mod (27))$, $(19 \mod (27))$ of $(1 \mod (9))$ are roots of $X^3 - 10$: we can[5] compute

$$7^3 - 10 \equiv 18 \mod (27)$$
$$16^3 - 10 \equiv 18 \mod (27)$$
$$25^3 - 10 \equiv 18 \mod (27)$$

so 1 cannot be close to a root in $\mathbb{Z}_3$: if $\beta \in \mathbb{Z}_3$ is a root of $X^3 - 10$ and $\beta \equiv 1 \mod (9)$, then $(\beta \mod (27))$ is a lift of $(1 \mod (9))$ that is a root of $X^3 - 10$, a contradiction. Hence necessarily $\beta \not\equiv 1 \mod (9)$ or equivalently $|\beta - 1|_3 \geq 1/9$.

We can argue similarly for 7, finding that no lift of $(7 \mod (9))$ can be a root. Thus a cube root of 10 in $\mathbb{Z}_3$ has to be a lift of $(4 \mod (9))$ and by the uniqueness, it is α.

Exercise 1. Let $u \in \mathbb{Q}_p \backslash \{0\}$ and write $u = p^k v$, $k \in \mathbb{Z}$, $v \in \mathbb{Z}_p^\times$. Show that u is a square if and only if

(1) for p odd, k is even and v is a square modulo p;
(2) for $p = 2$, k is even and $v \equiv 1 \mod (8)$.

Proposition 5.3. *The roots of unity in $\mathbb{Q}_p$ are*

(1) For p odd, the $(p-1)$-th roots of unity;
(2) for $p = 2$, $\{\pm 1\}$.

Proof. By Fermat's little theorem, the polynomial $X^{p-1} - 1$ has $p-1$ distinct roots modulo p, namely the elements of $\mathbb{F}_p^\times$. All those roots modulo p are thus simple, and lift by Hensel's lemma to at least $p-1$ distinct roots of $X^{p-1} - 1$ in $\mathbb{Z}_p$. Since conversely $X^{p-1} - 1$ has at most $p-1$ roots, this shows that $\mathbb{Q}_p$ has all $(p-1)$-th roots of unity, and each one is the lift of a unique root mod p.

If ζ_1 and ζ_2 are two roots of unity of order prime to p, let m be the lcm of their order. Suppose that $\zeta_1 \equiv \zeta_2 \mod (p)$. The polynomial $P(X) := X^m - 1$ has only simple roots modulo p: it is coprime to its derivative $P'(X) = mX^{m-1}$, which is non-zero because $m \not\equiv 0 \mod (p)$. We thus find by the uniqueness in Hensel's lemma that $\zeta_1 = \zeta_2$.

[5]Here, a calculator start being helpful...

Now, let ζ be a root of unity of order prime to p. We have $\zeta \not\equiv 0 \mod (p)$ so by the previous discussion, ζ is equal to one of the $p-1$-th roots of unity, because those all have order prime to p and their classes modulo p cover all of the non-zero elements of $\mathbb{Z}/p\mathbb{Z}$.

We now look at roots of unity of order a power of p. We start with the case where p is odd. If $\zeta^p = 1$ and $\zeta \neq 1$, using Fermat's little theorem we find

$$1 \equiv \zeta^p \equiv \zeta \mod (p).$$

Thus, write $\zeta = 1 + px$ for some $x \in \mathbb{Z}_p$. By the binomial theorem, we find $\zeta^k \equiv 1 + kpx \mod (p^2)$ for all $k \geq 0$. All roots of $X^p - 1$ in $\mathbb{Z}_p$ must be simple, and $\zeta \neq 1$ so ζ is a root of

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

Therefore,

$$0 \equiv 1 + \zeta + \cdots + \zeta^{p-1} \equiv \sum_{k=0}^{p-1} (1 + pky) \equiv p + py\frac{p(p-1)}{2} \mod (p^2)$$

and since p is odd, $(p-1)/2$ is an integer so we finally get $0 \equiv p \mod (p^2)$, a contradiction. We have shown that the only p-th root of unity in $\mathbb{Q}_p$ is 1. Now if ζ was a root of unity of order p^k in $\mathbb{Q}_p$, then we would find that $\zeta^{p^{k-1}}$ is of order p, a contradiction. So there are no roots of unity of p-power order.

If $p = 2$, let us show that the only 4th roots of unity are ± 1. This will, as above, imply that there are no roots of unity of order a power of 2 greater or equal to 4. Let $\zeta \in \mathbb{Z}_2^\times$ be a 4-th root of unity and suppose $\zeta \neq \pm 1$. Then $\zeta^2 = -1$. But since $\zeta \in \mathbb{Z}_2^\times$, it cannot be 0 modulo 2 hence $\zeta \equiv 1$ or 3 mod (4). But then $-1 = \zeta^2 \equiv 1 \mod (4)$, a contradiction.

Finally, if ζ is a root of unity in $\mathbb{Q}_p$ of order $n = p^k \cdot m$ with m prime to p, we can find $u, v \in \mathbb{Z}$ such that $1 = up^k + vm$. Then

$$\zeta = (\zeta^{p^k})^u \cdot (\zeta^m)^v$$

where $(\zeta^{p^k})^u$ is of order dividing m so is a $(p-1)$-th root of unity, while $(\zeta^m)^v$ is of p-power order. Combining this observation with the previous discussion finishes the proof. □

6. Equivalence of norms on finite extensions of a complete normed field

Definition 6.1. *Let K be a normed field and let V be a K-vector space. A norm on V is a map $\|\cdot\| : V \to \mathbb{R}_+$ satisfying*

(1) $\|x\| = 0$ if and only if $x = 0$,
(2) for all $\alpha \in K$ and $x \in V$, $\|\alpha \cdot x\| = |\alpha| \, \|x\|$,
(3) for all $x, y \in V$, $\|x + y\| \leq \|x\| + \|y\|$.

A normed K-vector space is a K-vector space equipped with a norm.

A norm $\|\cdot\|$ on a K-vector space V defines a metric on V, and hence a topology, by letting $d(x,y) = \|x-y\|$.

Example 11. Let K be a normed field. We have the usual ℓ^p norms $\|\cdot\|_p$ on K^n for all $p \geq 1$, given by

$$\|(x_1,\ldots,x_n)\|_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}.$$

Example 12. In the same setting, we have the usual sup norm

$$\|(x_1,\ldots,x_n)\|_\infty = \max(|x_1|,\ldots,|x_n|).$$

If K is a complete normed field, then K^n with the sup norm is also complete as a metric space, since for the sup norm being a Cauchy sequence or converging to an element can be checked on each component.

Definition 6.2. *Let K be a normed field, V a K-vector space, and let $\|\cdot\|_1$ and $\|\cdot\|_2$ be two norms on V. We say that $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent if $\|\cdot\|_1$ and $\|\cdot\|_2$ induce the same topology on V.*

Proposition 6.3. *Let K be a normed field with a non-trivial absolute value, V a K-vector space, and let $\|\cdot\|_1$ and $\|\cdot\|_2$ be two norms on V. Then $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent if and only if there exists constants $C > 0$, $D > 0$ such that $\|x\|_1 \leq C\|x\|_2$ and $\|x\|_2 \leq D\|x\|_1$ for all $x \in V$. If K is equipped with the trivial absolute value, then the reverse implication still holds.*

Proof. We first show the reverse implication. Let U be an open of V for $\|\cdot\|_1$; we want to show that U is open for $\|\cdot\|_2$. Thus let $x \in U$; by definition, there is an open ball $B_{\|\cdot\|_1}(x,r) \subset U$ of nonzero radius r. But then for all $y \in V$, $\|y-x\|_2 < \frac{1}{C}r$ implies $\|y-x\|_1 < r$, hence $B_{\|\cdot\|_2}(x, \frac{1}{C}r) \subset B_{\|\cdot\|_1}(x,r) \subset U$ is an open ball for $\|\cdot\|_2$ around x contained in U, showing that U is open for $\|\cdot\|_2$. The argument is symmetric so we are done.

Conversely, assume that the absolute value is non-trivial and that $\|\cdot\|_1$ is equivalent to $\|\cdot\|_2$. The open ball $B_{\|\cdot\|_1}(0,1)$ is open for $\|\cdot\|_1$, hence it is also open for $\|\cdot\|_2$ by hypothesis, so it must contain a small open ball $B_{\|\cdot\|_2}(0,r)$ for $\|\cdot\|_2$ of non-zero radius r around its point 0. Now pick $\gamma \in K$ with $|\gamma| > 1$. Then $|\gamma|^n \xrightarrow[n\to\infty]{} \infty$ and $|\gamma|^n \xrightarrow[n\to-\infty]{} 0$, so for every non-negative real number α, we can find an (unique) integer $n \in \mathbb{Z}$ such that $|\gamma|^n \leq \alpha < |\gamma|^{n+1}$: namely, this equation is equivalent to

$$n\ln(|\gamma|) \leq \ln(\alpha) < (n+1)\ln(|\gamma|) \Leftrightarrow n \leq \frac{\ln(\alpha)}{\ln(|\gamma|)} < n+1 \Leftrightarrow n = \lfloor \frac{\ln(\alpha)}{\ln(|\gamma|)} \rfloor.$$

Now, let $v \in V$ and find $n \in \mathbb{Z}$ such that

$$|\gamma|^n \leq \frac{\|v\|_2}{r} < |\gamma|^{n+1}$$

Then $\|\frac{v}{\gamma^{n+1}}\|_2 < r$ so $\|\frac{v}{\gamma^{n+1}}\|_1 < 1$. This implies that

$$\|v\|_1 < |\gamma|^{n+1} = |\gamma|\,|\gamma|^n \leq \frac{|\gamma|}{r}\|v\|_2$$

and we obtain the constant $C = \frac{|\gamma|}{r}$. The argument is again symmetric, which concludes the proof. □

Theorem 6.4. *Let K be a complete normed field and V a finite dimensional K-vector space. Any two norms on V are equivalent, and V is complete for any norm.*

Proof. We will show the result by induction on the dimension of V. If $\dim V = 0$, then $V = \{0\}$ is complete and any two norms on V are equal. Suppose now that the theorem is true for any K-vector space of dimension $\leq d$, and let V be a K-vector space of dimension $d+1$ with a norm $\|\cdot\|$. Fix a basis $(e_1, \ldots, e_{d+1})$ of V; we will show that $\|\cdot\|$ is equivalent to the sup norm $\|\cdot\|_\infty$ coming from that choice of basis. In particular, since V is always complete for the sup norm, V will also be complete for $\|\cdot\|$.

Let $x \in V$. Writing $x = \sum_{i=1}^{d+1} a_i e_i$ we find the triangle inequality:

$$\|x\| = \|\sum_{i=1}^{dn+1} a_i e_i\| \leq \sum_{i=1}^{d+1} |a_i|_K \|e_i\| \leq (\sum_{i=1}^{d+1} \|e_i\|) \cdot \max |a_i|_K = C \cdot \|x\|_\infty$$

for $C = \sum_{i=1}^{d+1} \|e_i\| > 0$ a constant not depending on x. Notice that here we did not use the induction hypothesis.

Let us show conversely that there exists $D > 0$ with $\|x\|_\infty \leq D\|x\|$ for all $x \in V$. Let us assume for the sake of contradiction that such a D does not exist. Thus, for all $D = n > 0$, $n \in \mathbb{N}$, there exists an $x_n \in V$ with $\|x_n\|_\infty > n\|x_n\|$. For every $n \in \mathbb{N}$ one of the coordinates of x_n in the basis $\underline{e}$ has maximal absolute value ; call that coordinate $\alpha_n \in K$. Then by construction $\|x_n\|_\infty = |\alpha_n|$ and thus after renormalizing $y_n := \frac{x_n}{\alpha_n}$ we find that y_n has one of its coordinates equal to 1 and $\|y_n\|_\infty = 1$. Moreover, we had $\|x_n\|_\infty > n\|x_n\|$ so we deduce $\|y_n\| < 1/n\|y_n\|_\infty = 1/n$, so the sequence $(y_n)_{n\in\mathbb{N}}$ converges to 0 for $\|\cdot\|$.

Consider the hyperplanes $H_i = \mathrm{Vect}(e_1, \ldots, \widehat{e_i}, \ldots, e_{d+1})$ generated by a choice of d basis vectors. Then each H_i is of dimension d, hence they are complete for $\|\cdot\|$ by the induction hypothesis. In particular they are closed for $\|\cdot\|$: if $(x_n)_{n\in\mathbb{N}}$ is a sequence in H_i converging to $x \in V$ for $\|\cdot\|$, then $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in H_i, so it converges in H_i, which implies $x \in H_i$. Therefore, the finite union $T = \bigcup_{i=1}^{n+1} e_i + H_i$ is closed, so its complement is open for $\|\cdot\|$. But T consists exactly of those vectors which in the basis (e_i) have at least one coordinate that is exactly one, so $(y_n)_{n\in\mathbb{N}}$ is a sequence in T. We now reach the contradiction: on the one hand we have $0 \notin T$, while on the other hand T is closed for $\|\cdot\|$ and $y_n \xrightarrow[n\to\infty]{} 0$ for $\|\cdot\|$ which implies that $0 \in T$. □

Corollary 6.5. *Let K be a complete normed field and V be a normed vector space over K. Any finite-dimensional subspace of V is closed.*

Proof. We've actually seen the proof in the previous proof: let $W \subseteq V$ be finite-dimensional. Then W is complete for $\|\cdot\|$. Therefore, any sequence $(x_n)_{n\in\mathbb{N}} \in W^{\mathbb{N}}$ converging to $x \in V$ is a Cauchy sequence in W so it converges in W, and by uniqueness of limits we get $x \in W$. We are done by the sequential criterion for closedness. □

Corollary 6.6. *Let K be a complete normed field and let L be an algebraic extension of K. There exists at most one absolute value on L extending that on K.*

We will see later that there always exists an absolute value on L extending that on K.

Proof. Since L is an union of finite extensions of K, we can assume that L is a finite extension of K. Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on L, extending $|\cdot|_K$. Observe that those two absolute values are norms when considering L as a K-vector space, where K acts by multiplication. Thus $|\cdot|_1$ and $|\cdot|_2$ are equivalent as norms, so they induce the same topology, so they are equivalent as absolute values, and we find that there exists $\alpha > 0$ with $|\cdot|_1 = |\cdot|_2^\alpha$.

We now distinguish two cases: if $|\cdot|_K$ is non-trivial, there is an $x \in K$ with $|x| \neq 0, 1$ and applying the previous equation to x we find $|x|_K = |x|_K^\alpha$, which implies $\alpha = 1$.

If now the absolute value on K is trivial, then the trivial absolute value on L extends the absolute value on K, so by the above argument there exists $\alpha > 0$ such that $|\cdot|_1 = |\cdot|_{\text{triv}}^\alpha$. But since the trivial absolute value only takes values in $\{0, 1\}$, any power of the trivial absolute value is equal to it. □

Notice that if K is a normed field with the trivial absolute value, then it is complete: if $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, then there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$, $|x_n - x_n|_{\text{triv}} < 1$; but then this means $|x_n - x_n|_{\text{triv}} = 0$ so $x_n = x_m$. Therefore $(x_n)_{n\in\mathbb{N}}$ converges to its common value $x_N = x_{N+1} = \ldots$. We noticed during the proof that for a finite extension L of K, the trivial absolute value on L extends that on K, so it is the unique extension.

7. Extensions of absolute values, part 1: the field norm

Let K be a complete normed field and let L/K be a finite extension. We have seen that there is at most one absolute value on L extending that on K; we will now show that there exists one. We will concentrate on the case where K is a complete normed field with a non-trivial non-archimedean valuation. The case of a trivial valuation has already been treated; as for the archimedean case, another theorem of Ostrowski classifies completely (up to equivalence of norms) complete archimedean normed fields:

Theorem 7.1 (Ostrowski)**.** *Let K be a complete archimedean normed field. Then $K \simeq \mathbb{R}$ or $K \simeq \mathbb{C}$, and under this isomorphism the absolute value on K is equivalent to the usual absolute value $|\cdot|_\infty$ on $\mathbb{R}$ or $\mathbb{C}$.*

So in that case we already know that the absolute value extends from $\mathbb{R}$ to $\mathbb{C}$!

From now on we will abuse terminology and call a non-archimedean normed field simply a non-archimedean field. We fix a complete non-archimedean field K with a non-trivial absolute value and a finite extension L. From the uniqueness of a potential extension, we will deduce an explicit expression for an extension of $|\cdot|$ to L, and then show that this expression defines an absolute value that does extend that on K. But first, we need to build some theory around field extensions.

Definition 7.2. *Let $x \in L$. Then multiplication by x is a K-linear map $\ell_x : L \to L$. We denote by $N_{L/K}(x) \in K$ its determinant, called the (field) norm of x.*

It is unfortunate that this is also called the norm, it is not a norm in the topology sense.

Proposition 7.3. *Let $x, y \in L$. We have:*

(1) $N_{L/K}(x) = 0$ if and only if $x = 0$;
(2) $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$;
(3) if $x \in K$ then $N_{L/K}(x) = x^{[L:K]}$ where $[L : K] := \dim_K L$.

Proof. (1) If $x = 0$ then ℓ_x is the 0 map so $N_{L/K}(x) = \det(\ell_x) = 0$. Conversely if $x \neq 0$ then ℓ_x has the inverse $\ell_{x^{-1}}$ so has non-zero determinant.

(2) We have $\ell_{xy}(z) = xyz = \ell_x \circ \ell_y(z)$ hence the result by taking determinants.

(3) If $x \in K$, since K acts on L by multiplication it follows that ℓ_x is in any basis the diagonal matrix with entries x, so $\det(\ell_x) = x^{\dim_K L} = x^{[L:K]}$.

□

Example 13. Let K be a field and let $d \in K$ such that x is not a square in K. Then $X^2 - x$ has no root in K hence is irreducible, and the extension $L := K(\sqrt{d})$ of K is of degree 2. It has the basis $\left\{1, \sqrt{d}\right\}$, and the matrix in that basis of the multiplication by an arbitrary element $x = a + b\{d\}$ is

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}$$

of determinant $N_{L/K}(x) = a^2 - db^2$.

Before saying more about the norm, we recall some facts from field theory:

Definition 7.4. *Let L/K be a field extension. An element $x \in L$ is said to be* algebraic *if there exists a non-zero polynomial $P \in K[X]$ such that $P(x) = 0$*

in L. In that case, the kernel of the evaluation map $\mathrm{ev}_x : K[X] \to L, \quad X \to x$ *is a non-zero principal ideal; moreover the image is the subring $K[x]$ of L, the smallest subring containing x. This ring is an integral domain, as a subring of L. Therefore* $\ker(ev_x) = (\mu_{K,x})$ *for a unique monic irreducible polynomial $\mu_{K,x} \in K[X]$, called the* minimal polynomial *of x. In particular, we get that $K[x] = K(x)$ is a field, the smallest subfield of L containing x, and an isomorphism $K[X]/(\mu_{K,x}) \xrightarrow{\simeq} K(x)$.*

Definition 7.5. *A field extension L/K is called* algebraic *if every $x \in L$ is algebraic over K.*

If L/K is a finite extension, it is algebraic. Indeed, for any $x \in L$, the infinite family $\left\{x^k\right\}_{k\in\mathbb{N}}$ cannot be linearly independent, so there exists a non-trivial linear combination $a_0 x^{k_0} + \ldots + a_l x^{k_l} = 0$ giving a non-zero polynomial annihilating x. Now if L/K is an arbitrary extension, we've seen that for $x \in L$ algebraic, the extension $K(x) \simeq K[X]/(\mu_{K,x})$ is finite, of degree $\deg(\mu_{K,x})$. More generally, if $x_1, \ldots x_n$ are algebraic over K, then the smallest subfield $K(x_1, \ldots, x_n)$ of L containing (x_i) is a finite extension of K; this is proven by induction using the multiplicativity of degrees.

If L/K is an algebraic extension, then

$$L = \bigcup_{\substack{K \subseteq E \subseteq L \\ E/K \text{ finite}}} E.$$

Indeed, any $x \in L$ is in the finite subextension $K(x)$.

We come now to our second characterization of the norm:

Proposition 7.6. *Let L/K be a finite extension and let $x \in L$.*

(1) If $L = K(x)$ then $N_{L/K}(x) = (-1)^{[L:K]}\mu_{K,x}(0)$.

(2) In general,

$$N_{L/K}(x) = (N_{K(x)/K}(x))^{[L:K(x)]} = (-1)^{[L:K]}\mu_{K,x}(0)^{[L:K(x)]}.$$

Proof. Let (e_i) be an ordered basis of $L/K(x)$ and let $1, x, \ldots, x^{d-1}$ be the natural (ordered) basis of $K(x)/K$, where $d = \deg \mu_{K,x} = [K(x) : K]$. Write $\mu_{K,x}(X) = X^d + \sum_{k=0}^{d-1} a_k X^k$. Then $(e_i x^k)$, ordered with the lexicographic order, is an ordered basis of L/K, and we find that $\ell_x(e_i x^k) = e_i x^{k+1}$ for $k < d-1$ and

$$\ell_x(e_i x^{d-1}) = e_i x^d = -\sum_{k=0}^{d-1} a_k e_i x^k.$$

Denote by

$$\mathrm{Comp}(\mu_{K,x}) = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & \ddots & \ddots & & \vdots \\ & & & 0 & -a_{d-2} \\ & & & 1 & -a_{d-1} \end{pmatrix}$$

the companion matrix of $\mu_{K,x}$. We find that in the chosen basis,

$$\mathrm{Mat}(\ell_x) = \begin{pmatrix} \mathrm{Comp}(\mu_{K,x}) & & \\ & \ddots & \\ & & \mathrm{Comp}(\mu_{K,x}) \end{pmatrix}$$

with $\#\{e_i\} = [L : K(x)]$ blocks. The result then follows from the computation, obtained by expanding on the last column

$$\begin{aligned} &\det \mathrm{Comp}(\mu_{K,x}) \\ &= (-1)^{d-1+0}(-a_o)\det(I_{d-1}) + \sum_{i>0}(-1)^{d-1+i}(-a_i)\det \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix} \\ &= (-1)^d a_0. \end{aligned}$$

□

Example 14. Let K be a field and $d \in K$ not a square. For $x = a + b\sqrt{d} \in K(\sqrt{d})$, we have either $x \in K$, which is equivalent to $b = 0$, or $x \notin K$, in which case $K \subset K(x) \subseteq K(\sqrt{d})$ implies $K(x) = K(\sqrt{d})$ and thus x is of degree 2 over K. If $x = a \in K$, its minimal polynomial is $X - a$ so $N_{K(\sqrt{d})/K}(x) = (-1)^2(-a)^2 = a^2$. If $x \notin K$, we find that $X^2 - 2aX + (a^2 - db^2) \in K[X]$ has x as its root so it is its minimal polynomial over K, and thus $N_{K(\sqrt{d})/K}(x) = (-1)^2(a^2 - db^2) = a^2 - db^2$. In both cases we find $N_{K(\sqrt{d})/K}(x) = a^2 - db^2$.

We now introduce without proofs the basic notion of Galois theory, namely Galois extensions:

Definition 7.7. *Let K be a field. A (finite) Galois extension L/K is a finite extension with exactly $[L : K]$ K-linear automorphisms. The group $\mathrm{Aut}_K(L)$ is then called the Galois group $\mathrm{Gal}(L/K)$ of L/K.*

If L/K is a finite Galois extension, we have a third formula for the field norm of an element $x \in L$, namely

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x).$$

Proposition 7.8. *Let L/K be a finite extension, with $L = K(x_1, \dots x_n)$. If each μ_{K,x_i} has no multiple roots and splits completely over L, i.e. has all its roots in L, then L/K is Galois.*

Example 15. Let K be a field not of characteristic 2 and let $d \in K$ not a square. Then $X^2 - d$ is separable irreducible so $L := K(\sqrt{d})$ is a separable extension of K. Moreover it is Galois as the other root $-\sqrt{d}$ of $X^2 - d$ is also in L. The extension L has two K-linear automorphisms, the

identity and the one sending $\sqrt{d}$ to $-\sqrt{d}$; those are well-defined because $L = K(\sqrt{d}) \simeq K[X]/(X^2 - d)$ and are the only possibilities since any K-linear automorphism of L leaves $X^2 - d$ fixed so has to permute its roots. Thus

$$N_{L/K}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Proposition 7.9. *Let L/K be a finite extension generated by elements $x_1, \dots, x_n$ whose minimal polynomials have no multiple roots (such an extension is called* separable*). There exists a finite Galois extension F/K containing L.*

Sketch of proof. Add inductively the roots of $\mu_{K,x_1}, \dots, \mu_{K,x_n}$ that are not already present. □

We now come to the discussion of extensions of absolute values, as promised. To extend the absolute value to a finite (separable) extension L/K, we might as well extend it to a bigger, Galois extension F/K, and so we can assume that L/K is Galois. But then we observe that if $|\cdot|_L$ is an extension to L of $|\cdot|_K$, then for any $\sigma \in \mathrm{Gal}(L/K)$, $|\sigma(\cdot)|_L$ is still an extension of $|\cdot|_K$:

- If $|\sigma(x)|_L = 0$ then $\sigma(x) = 0$ so $x = 0$;
- $|\sigma(xy)|_L = |\sigma(x)\sigma(y)|_L = |\sigma(x)|_L\,|\sigma(y)|_L$;
- $|\sigma(x + y)|_L = |\sigma(x) + \sigma(y)|_L \leq |\sigma(x)| + |\sigma(y)|_L$;
- Since σ preserves K by definition, for any $x \in K$ we have $|\sigma(x)|_L = |x|_L = |x|_K$.

By the uniqueness of extensions, we thus get $|\sigma(\cdot)|_L = |\cdot|_L$, i.e. any K-linear automorphism is an isometry of L. But then for all $x \in L$

$$\begin{aligned}\left|N_{L/K}(x)\right|_K = \left|N_{L/K}(x)\right|_L = \left|\prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma(x)\right|_L &= \prod_{\sigma\in\mathrm{Gal}(L/K)} |\sigma(x)|_L \\ &= \prod_{\sigma\in\mathrm{Gal}(E/K)} |x|_L \\ &= |x|_L^{[L:K]}\end{aligned}$$

and thus

$$|x|_L = \left|N_{L/K}(x)\right|_K^{\frac{1}{[L:K]}} = \left|N_{K(x)/K}(x)\right|_K^{\frac{1}{[K(x):K]}} = |\mu_{K,x}(0)|_K^{\frac{1}{[K(x):K]}}.$$

the second and last equality coming from our second point in prop. 7.6.

Using Galois theoretic arguments, we have thus identified a formula for $|x|_L$.

Proposition 7.10. *Let K be a complete non-archimedean field with a non-trivial absolute value, and let L/K be a finite extension*[6]*. Then the map*

$$f : x \mapsto \left|N_{L/K}(x)\right|_K^{\frac{1}{[L:K]}}$$

[6]We do not assume anymore that L is separable over K.

satisfies the first two axioms of an absolute value.

Proof. First, let $x \in K$. Then $N_{L/K}(x) = x^{[L:K]}$ so $\left|N_{L/K}(x)\right|_K^{1/[L:K]} = |x|_K$. Let $x, y \in L$. As $N_{L/K}$ respects multiplication, we find

$$\begin{aligned} f(xy) = \left|N_{L/K}(xy)\right|_K^{\frac{1}{[L:K]}} &= \left|N_{L/K}(x)N_{L/K}(y)\right|_K^{\frac{1}{[L:K]}} \\ &= \left|N_{L/K}(x)\right|_K^{\frac{1}{[L:K]}} \left|N_{L/K}(y)\right|_K^{\frac{1}{[L:K]}} \\ &= f(x)f(y). \end{aligned}$$

□

We will finish showing that f defines an absolute value in a second part, after we have developed some more theory. We finally mention some results that we did not get to earlier:

Lemma 7.11. *Let $|\cdot|$ be an absolute value on a field K. Then the following are equivalent:*

(1) for all $n \in \mathbb{N}$, $|n| \leq 1$;
(2) there exits $B > 0$ such that $|n| \leq B$ for all $n \in \mathbb{N}$;
(3) for all $x \in K$, if $|x| \leq 1$ then $|1 + x| \leq 1$;
(4) $|\cdot|$ is ultrametric;
(5) the closed unit ball in K is a subring of K.

Proof. We have (1) $\implies$ (2) with $B = 1$. Let us suppose (2). Then for any $x \in K$ with $|x| \leq 1$, we find

$$|1 + x|^n = |(1 + x)^n| = \left|\sum_{i=0}^{n} \binom{n}{k} x^k 1^{n-k}\right| \leq B \sum_{i=0}^{n} |x|^k \leq B(n + 1).$$

Taking n-th roots and letting $n \to \infty$, we find

$$|1 + x| \leq \lim_{n\to\infty} (B(n + 1))^{1/n} = 1.$$

Suppose (3). Then for all $x, y \in K$, without loss of generality with $|x| \geq |y|$, we find

$$|x + y| = |x| \left|1 + \frac{y}{x}\right| \leq |x| = \max(|x|, |y|)$$

because $|y/x| \leq 1$. This shows (4).

The implication (4) $\implies$ (5) has already been seen earlier. Finally, if (5) holds then the unit ball is a ring containing 1, so it also contains $n = 1 + \cdot + 1 \in \mathbb{N}$, hence (1) holds. □

Observe that in the proof of (4) $\implies$ (5), we showed that a function $f : K \to \mathbb{R}_+$ satisfying

(1) $f(x) = 0$ if and only if $x = 0$;
(2) $f(xy) = f(x)f(y)$;
(3) if $f(x) \leq 1$ then $f(x + 1) \leq 1$;

is already an ultrametric absolute value.

Corollary 7.12. *If K is a normed field of characteristic $p > 0$ (meaning that $p := 1 + \ldots + 1 = 0$ in K) then its absolute value is ultrametric.*

Proof. For any $n \in \mathbb{N}$, since $p = 0$ we have $n = r$ for a unique $r \in \{0, \ldots, p-1\}$. Thus $|n| \leq \max(|0|, \ldots, |p-1|)$ is bounded. □

Remark. On a *finite* field, the only possible absolute value is the trivial one: indeed, it is known that the group of invertible elements of a finite field is cyclic, so all non-zero elements are roots of unity. But a root of unity can only have absolute value one: if $\zeta^n = 1$, then $1 = |\zeta^n| = |\zeta|^n$, so $|\zeta|$ is an n-th root of unity in $\mathbb{R}_+$, hence it must be one.

8. Aside: separable and Galois extensions

9. Aside: local compactness in normed vector spaces

Let us record some observations on local compactness for normed fields:

Proposition 9.1. *Let K be a normed field with a non-trivial absolute value. Then*

1. *K is locally compact if and only if every closed ball is compact, if and only if the closed unit ball around 0 is compact;*
2. *if K is locally compact, then K is complete;*

Note that in (1)*, if K is non-archimedean this means that the valuation ring is compact.*

Remark. A normed field with a trivial absolute value is locally compact, since every point $x \in K$ has the compact open neighbourhood $\{x\}$.

Proof. (1). If the closed unit ball is compact then every point x has the neighbourhood $\bar{B}(x, 1) = x + \bar{B}(0, 1)$ which is compact because it is the continuous image under translation of the compact $\bar{B}(0, 1)$. Clearly, if every closed ball is compact then the closed unit ball around 0 is compact. So it remains to show that if K is locally compact then every closed ball is compact. Since the valuation is non-trivial, there exists $\gamma \in K$ with $|\gamma| > 1$. Then for any $r > 0$, there exists $n \in \mathbb{N}$ with $|\gamma^n| \geq r$, so any closed ball is a subset of a closed ball of the form $\bar{B}(x, |\gamma^n|)$, i.e. of radius belonging to $|K| \subseteq \mathbb{R}_+$. Therefore, it suffices to show that such a closed ball is compact, because then any closed ball will be a closed subset of a compact Hausdorff space and thus also compact. Now, a ball $\bar{B}(x, |\alpha|)$ for $\alpha \in K \setminus \{0\}$ is the subset $x + \alpha\bar{B}(0, 1)$, which is homeomorphic to $\bar{B}(0, 1)$ because translation and non-zero scalar multiplication are homeomorphisms (with inverse the translation by the additive inverse, or scalar multiplication by the multiplicative inverse). So it suffices to show that the closed unit ball around 0 is compact, or equivalently that there is a small closed ball of non-zero radius $r \in |K|$ around 0 that is compact. Since K is locally compact, 0 admits a compact neighbourhood K, so by definition there exists an open ball $B(0, r)$ with $r > 0$ around 0 with $B(0, r) \subseteq K$. We can then find $n \in \mathbb{Z}$ with $0 < |\gamma|^n < r$,

and then $\bar{B}(0, |\gamma^n|) \subseteq B(0, r) \subseteq K$ is a closed subset of a compact Hausdorff space, so it is compact.

(2). Recall that any Cauchy sequence is bounded. Therefore if $(x_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ is a Cauchy sequence, there is some $C > 0$ such that x_n is in the compact space $\bar{B}(0, C)$ for all $n \in \mathbb{N}$. Thus $(x_n)_{n\in\mathbb{N}}$ has a convergent subsequence, and the Cauchy property implies that the whole sequence converges to the limit of that subsequence. □

Earlier, we stated a classification of locally compact normed fields. Here we prove a weaker statement:

Theorem 9.2 (Classification of locally compact normed fields)**.** *Let K be a normed field. Then K is locally compact if and only if*

(1) if K is archimedean, $K = \mathbb{R}$ or $\mathbb{C}$ with an absolute value equivalent to the usual one;
(2) the absolute value is trivial, or;
(3) if K is non-archimedean, then K is complete with a non-trivial discrete valuation (i.e. there is an element of maximal absolute value strictly less than 1) and finite residue field.

Proof. If K is archimedean, then it is a complete archimedean normed field so we conclude with Ostrowski's theorem; conversely, it is well-known that $\mathbb{R}$ and $\mathbb{C}$ with the usual absolute value are locally compact.

If the absolute value on K is trivial, we've already seen that K is locally compact.

If K is non-archimedean complete with a non-trivial discrete valuation and finite residue field, to show that it is locally compact we have to show that the valuation ring is compact, or equivalently complete and totally bounded. Since the valuation ring is closed in K, it is complete. The valuation is discrete, so we can fix a non-zero element $\pi \in \mathcal{O}_K$ with maximal absolute value strictly less than one; equivalently, we have a valuation $v : K^\times \to \mathbb{Z}$ such that the absolute value is given by $|x| = |\pi|^{-v(x)}$. For any $\varepsilon > 0$, we have to cover $\mathcal{O}_K$ with finitely many open balls of radius $\leq \varepsilon$. But there exists $n \in \mathbb{N}$ with $|\pi^n| = |\pi|^n < \varepsilon$, and then for $x \in \mathcal{O}_K$,

$$\bar{B}(x, \pi^n) = x + \pi^n \bar{B}(0, 1) = x + \pi^n \mathcal{O}_K \subseteq B(x, \varepsilon)$$

is the coset of x for the ideal $\pi^n\mathcal{O}_K$ in $\mathcal{O}_K$. But we know that $\mathcal{O}_K$ is the disjoint union of its distinct cosets, so we have to show that the number of distinct cosets is finite, i.e. that the quotient ring $\mathcal{O}_K/(\pi^n)\mathcal{O}_K$ is finite. Observe that by definition we have $\mathfrak{m} = B(0, 1) = \bar{B}(0, \pi) = \pi\mathcal{O}_K$. Denote by $k := \mathcal{O}_K/\mathfrak{m} = \mathcal{O}_K/\pi\mathcal{O}_K$ the residue field; it is finite by hypothesis. Let q denote the cardinal of k. We will show by induction on $n \geq 1$ that $\#(\mathcal{O}_K/\pi^n\mathcal{O}_K) = q^n$, hence showing in particular that is finite, which will conclude the argument. The claim holds by definition for $n = 1$. Suppose we

have proven the claim for some $n \geq 1$. Consider the map of abelian groups

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{O}_K & \to & \mathcal{O}_K \\ x & \mapsto & \pi^n x \end{array} \right. .$$

We have $x \in \pi\mathcal{O}_K$ if and only if $\pi^n x \in \pi^{n+1}\mathcal{O}_K$, so φ induces a well-defined injective map

$$\overline{\varphi} : \left\{ \begin{array}{ccc} k & \to & \mathcal{O}_K/\pi^{n+1}\mathcal{O}_K \\ x \mod (\pi) & \mapsto & \pi^n x \mod (\pi^{n+1}) \end{array} \right. .$$

Consider the canonical projection $p : \mathcal{O}_K/\pi^{n+1}\mathcal{O}_K \to \mathcal{O}_K/\pi^n\mathcal{O}_K$. We claim that $\ker(p) = \mathrm{im}(\overline{\varphi})$. Indeed, if $(y \mod (\pi^{n+1}) \in \mathrm{im}(\overline{\varphi})$ then $y \equiv \pi^n x \mod (\pi^{n+1})$ for some $x \in \mathcal{O}_K$, and thus $y \equiv 0 \mod (\pi^n)$. Conversely, if $y \equiv 0 \mod (\pi^n)$ we can write $y = \pi^n x$ for some $x \in \mathcal{O}_K$ and then $(y \mod (\pi^{n+1})) = \overline{\varphi}(x \mod (\pi))$. Since $\overline{\varphi}$ is injective, $\mathrm{im}(\overline{\varphi}) = \ker(p)$ is isomorphic to k, which is finite of cardinal q. Also, $\mathcal{O}_K/\pi^n\mathcal{O}_K$ is finite of cardinal q^n by the induction hypothesis so we get that $\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K$ is finite, and by the first isomorphism theorem of cardinal $\#\ker(p) \cdot \#\mathrm{im}(p) = q \cdot q^n = q^{n+1}$.

We now show the converse: if K is non-archimedean, locally compact, and with a non-trivial absolute value then it must be complete, with a discrete valuation and a finite residue field. We already know that K must be complete, and its valuation ring is compact, hence totally bounded. In particular, $\mathcal{O}_K$ can be covered by finitely many open balls of radius 1, which means that in the disjoint union of $\mathcal{O}_K$ into cosets $B(x,1) = x + B(0,1)$ for the ideal $\mathfrak{m} = B(0,1)$, there are only finitely many terms. This is exactly saying that the quotient ring $k = \mathcal{O}_K/\mathfrak{m}$ is finite. Let us show that the valuation is discrete; by contradiction, assume that there is a sequence $(\gamma_n)_{n\in\mathbb{N}} \in \mathcal{O}_K^{\mathbb{N}}$ such that $|\gamma_n| \xrightarrow[n\to\infty]{} 1$ but $|\gamma_n| < 1$ for all $n \in \mathbb{N}$. Since $\mathcal{O}_K$ is compact, we can extract a converging subsequence and thus assume that $\gamma_n \xrightarrow[n\to\infty]{} \gamma \in \mathcal{O}_K$. By continuity of the absolute value, we find $|\gamma| = 1$; on the other hand, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, we have $|\gamma_n - \gamma| < 1$; then by the equality case of the strong triangle inequality, for $n \geq N$

$$|\gamma_n| = |\gamma_n - \gamma + \gamma| = |\gamma| = 1$$

which is a contradiction. □

The statement we gave earlier further classified non-archimedean locally compact normed field with a non-trivial absolute value as being either of characteristic p, isomorphic to the ring of Laurent series $\mathbb{F}_q((T))$ (with the T-adic absolute value) over the finite field $\mathbb{F}_q$ with $q = p^n$ elements for some $n \geq 1$, or of characteristic 0, isomorphic to a finite extension of $\mathbb{Q}_p$. This further statement requires more work so we will not tackle it for now. See exercise 9 of exercise sheet 2 for a guided proof.

We previously discussed normed vector spaces over a complete normed field K, and proved the equivalence of norms on finite-dimensional vector spaces in that case. In particular, when K is locally compact, we get:

Proposition 9.3. *Every finite-dimensional normed vector space V over a locally compact normed field K is locally compact, and its closed balls are compact.*

Proof. Translation and scalar multiplication are continuous so by the same argument as for normed fields, it suffices to show that some small closed ball around 0 is compact. Fix a basis $(e_i)_{i=1}^n$ of V and consider the sup norm $\|\cdot\|_\infty$ on V relative to that basis. We showed in the proof of the theorem on equivalence of norms that there is some constant $C > 0$ with $\|\cdot\|_\infty \leq C\|\cdot\|$. In particular we have the inclusion of the closed ball $\bar{B}_{\|\cdot\|}(0, 1/C) \subseteq \bar{B}_{\|\cdot\|_\infty}(0, 1)$ inside the unit closed ball around 0 for $\|\cdot\|_\infty$. The latter is compact, since a sequence in it has its of its coordinates in the closed unit ball in K, and then we can extract a subsequence so that all coordinates converge in K, so that the sequence will converge in V for $\|\cdot\|_\infty$. The closed ball $\bar{B}_{\|\cdot\|}(0, 1/C)$ is thus compact as a closed subset of a compact Hausdorff space. □

There is a converse to that theorem:

Theorem 9.4 (Riesz)**.** *Let V be a normed vector space over a complete normed field K with a non-trivial absolute value. If V is locally compact then V is finite dimensional and K is locally compact.*

Proof. K is complete so for any $x \in V \setminus \{0\}$, the subspace $\mathrm{Vect}(x)$ is finite-dimensional hence closed, so it is locally compact, and it is homeomorphic to K through the map $\alpha \mapsto \alpha \cdot x$ so K is locally compact.

Since V is locally compact, the closed unit ball $\bar{B}(0, 1)$ in V is compact. Let $\gamma \in K$ with $0 < |\gamma| < 1$. Then we have the open covering

$$\bar{B}(0, 1) \subseteq \bigcup_{x \in \bar{B}(0,1)} \bar{B}(x, |\gamma|)$$

so by compactness we find a finite set $S \subseteq V$ such that

$$\bar{B}(0, 1) \subseteq \bigcup_{x \in S} \bar{B}(x, |\gamma|).$$

We can rewrite $\bar{B}(x, |\gamma|) = x + \gamma\bar{B}(0, 1)$ and the above becomes

$$\bar{B}(0, 1) \subseteq S + \gamma\bar{B}(0, 1) \subseteq \mathrm{Vect}(S) + \gamma\bar{B}(0, 1).$$

Put $W = \mathrm{Vect}(S)$; since S is finite, W is finite-dimensional so it is closed in V. We can iterate the above to get

$$\begin{aligned}\bar{B}(0, 1) \subseteq W + \gamma\bar{B}(0, 1) \subseteq W + \gamma(W + \gamma\bar{B}(0, 1)) \subseteq W + \gamma \cdot W + \gamma^2\bar{B}(0, 1) \\ = W + \gamma^2\bar{B}(0, 1).\end{aligned}$$

and thus by induction, $\bar{B}(0, 1) \subseteq W + \gamma^n\bar{B}(0, 1)$ for all $n \geq 1$. This implies that $\bar{B}(0, 1) \subseteq \overline{W} = W$: indeed, for any $x \in \bar{B}(0, 1)$ we can write $x =$

$y_n + \gamma^n z_n$ with $y_n \in W$ and $z_n \in \bar{B}(0,1)$; but then $\|x - y_n\| = \|\gamma^n z_n\| \leq |\gamma|^n \xrightarrow[n\to\infty]{} 0$ so $x \in \overline{W}$. We now conclude that $V = W$: for any $x \in V$, we can find $n \in \mathbb{Z}$ such that $\|x\| \leq |\gamma|^n$; but then $\|\frac{x}{\gamma^n}\| \leq 1$ so $\frac{x}{\gamma^n} \in \bar{B}(0,1) \subseteq W$, which implies that $x \in W$. Since W is finite-dimensional, we are done. □

Here is a counterexample in case K is not complete. Consider $\mathbb{Q}$ with the usual absolute value. Then $\mathbb{R}$ with the usual absolute value defines a normed vector space over $\mathbb{Q}$, it is locally compact as usual, but it is absolutely not of finite dimension over $\mathbb{Q}$, and $\mathbb{Q}$ is not locally compact as it is not even complete.

Here is another strange phenomenon: there exists a subfield K of $\mathbb{C}$ that is dense in $\mathbb{C}$ for the usual topology and such that $[\mathbb{C} : K] = 2$. K is constructed, via a "strange" embedding of $\mathbb{R}$ into $\mathbb{C}$ obtained through the axiom of choice; see `https://mathoverflow.net/a/13381`. This means in particular that K is a normed field (using the restriction of the usual absolute value to K) whose completion $\mathbb{C}$ is of degree 2 over K !

The above actually holds for any topological vector space over K. Recall that a topological vector space V over K is a vector space equipped with a topology such that the addition and scalar multiplication $V \times V \to V, (x,y) \mapsto x + y$ and $K \times V \to V, (\alpha, x) \mapsto \alpha \cdot x$ are continuous for the product topology on $V \times V$ and $K \times V$, respectively.

Theorem 9.5. *Let V be a Hausdorff topological vector space space over a locally compact normed field K. If V is locally compact then V is finite dimensional.*

The proof we gave generalizes nicely to that case. We also have the following result in the finite-dimensional case which generalizes the theorem on equivalence of norms:

Theorem 9.6. *Let V be a finite-dimensional Hausdorff topological space. Then any choice of basis $(e_i)_{i=1}^n$ of V gives a bijective K-linear* homeomorphism *$V \simeq K^n$, i.e. V has the product topology for any choice of basis.*

For proofs, we defer to `https://terrytao.wordpress.com/2011/05/24/locally-compact-topological-vector-spaces/`.

10. Hensel's lemma for polynomials

We start with a few general observations. Let R be a ring and let $I \subset R$ be an ideal. Then we can consider the ideal $IR[X]$ generated by I in the polynomial ring $R[X]$; by construction, we will have $f(X) = \sum a_i X^i \in IR[X]$ if and only if $a_i \in I$ for all i. Indeed, if $a_i \in I$ then $a_i X^i \in IR[X]$ so we get the converse direction, and if $f \in IR[X]$, by definition we can write $f = \sum \alpha_k Q_k$ with $\alpha_k \in I$ and $Q_k(X) = \sum b_i^{(k)} X^i \in R[X]$. Looking coefficient by coefficient, we find

$$a_i = \sum_k \alpha_k b_i^{(k)} \in I.$$

The canonical projection $R \to R/I$ induces a surjective ring map $R[X] \to (R/I)[X]$, obtained by reducing each coefficient modulo I. The kernel of that map is by the previous observation $IR[X]$, and so we get a canonical isomorphism $R[X]/IR[X] \simeq (R/I)[X]$. We will abuse notation and denote by $(f \mod I) := (f \mod IR[X])$ the class of a polynomial $f \in R[X]$ in the quotient $(R/I)[X]$.

Let K be a non-archimedean field. Consider the (infinite-dimensional) vector space $K[X]$ of polynomials over K. We equip it with the sup norm coming from the canonical basis $\{1, X, X^2, \ldots\}$, i.e. for $f(X) = \sum a_i X^i \in K[X]$ we put

$$\|f\| = \sup |a_i|$$

We have

$$f \in \mathcal{O}_K[X] \Leftrightarrow |a_i| \leq 1 \text{ for all } i \Leftrightarrow \|f\| \leq 1$$

and $f \in \mathfrak{m}\mathcal{O}_K[X] \Leftrightarrow \|f\| < 1$. Similarly, let $\pi \in \mathfrak{m} \setminus \{0\}$. For $f(X) = \sum a_i X^i \in \mathcal{O}_K[X]$, we have

$$\begin{aligned} \|f\|_\infty \leq |\pi| \Leftrightarrow |a_i| \leq |\pi| \text{ for all } i &\Leftrightarrow |a_i/\pi| \leq 1 \text{ for all } i \\ &\Leftrightarrow a_i/\pi \in \mathcal{O}_K \text{ for all } i \\ &\Leftrightarrow a_i \in \pi\mathcal{O}_K \text{ for all } i \\ &\Leftrightarrow f(X) \equiv 0 \mod (\pi) \end{aligned}$$

By definition, the convergence of a sequence of polynomials $(f_n(X))_{n\in\mathbb{N}} = (\sum a_i^{(n)} X^i)_{n\in\mathbb{N}}$ is the uniform convergence of the sequences $(a_i^{(n)})_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ of coefficients. If K is complete and we look at the subspace $K[X]_{\leq d}$ of polynomials of degree less than $d \in \mathbb{N}$, this subspace is finite-dimensional hence complete for $\|\cdot\|$.

Recall that over any commutative ring R, we can form the division with remainder $A = QB + R$ of a polynomial A by a *monic* polynomial B with unique quotient Q and remainder R satisfying $\deg(R) < \deg(B)$. The proof is the same as the usual proof for Euclidean division with coefficients in a field. Moreover, the degree of a polynomial does not satisfy $\deg(PQ) = \deg(P)+\deg(Q)$ in general[7] but only $\deg(PQ) \leq \deg(P)+\deg(Q)$. However, we still have equality *if P is monic*. Thus if $P, \widetilde{P}$ are monic polynomials of the same degree such that $P = \widetilde{P}Q$ for some polynomial Q, then first $\deg(Q) + \deg(\widetilde{P}) = \deg(P)$ so $\deg(Q) = 0$ and Q is a constant $Q = c$, and then looking at the top coefficient we find $1 = c \cdot 1$ hence $Q = 1$.

Theorem 10.1 (Hensel's lemma for polynomials, precise version)**.** *Let K be a complete non-archimedean field. Let $f \in \mathcal{O}_K[X]$, and assume that there exists polynomials $g_1, h_1 \in \mathcal{O}_K[X]$ and an element $\pi \in \mathfrak{m}$ such that*

(1) g_1 is monic,

[7] If R contains an element $a \neq 0$ such that $a^2 = 0$, then aX^n is of degree n but $(aX^n) \cdot (aX^m) = a^2 X^{m+n} = 0$ is of degree $-\infty$.

(2) the ideal generated by $(g_1 \mod (\pi))$ *and* $(h_1 \mod (\pi))$ *is the unit ideal* $(1) = \mathcal{O}_K[X]/\pi\mathcal{O}_K[X]$,
(3) $f \equiv g_1 h_1 \mod \pi$.

Then there exists unique polynomials $g, h \in \mathcal{O}_K[X]$ *such that*

(1) g *is monic,*
(2) $g \equiv g_1 \mod (\pi)$ *and* $h \equiv h_1 \mod (\pi)$,
(3) $f = gh$.

We can reformulate condition (2) above as the existence of polynomials $(u \mod (\pi)), (v \mod (\pi))$ such that $ug_1 + vh_1 \equiv 1 \mod (\pi)$.

Proof. We can act as if our valuation was discrete using the element π, and do the standard proof as found e.g. in Gouvêa's book.

Let $t = |\pi|$. Condition (3) means that there exists $u, v \in \mathcal{O}_K[X]$ such that $ug_1 + vh_1 \equiv 1 \mod (\pi)$, or equivalently

$$\|ug_1 + vh_1 - 1\| \leq t,$$

while condition (2) is equivalent to the upper bound $\|f - g_1 h_1\| \leq t$. Let $d = \deg f$, $m = \deg g_1$. We will construct by induction a sequence g_n, h_n satisfying

(1) g_n is monic of degree m and h_n is of degree $\leq d - m$,
(2) $|g_{n+1} - g_n| \leq t^n$ and $|h_{n+1} - h_n| \leq t^n$ (equivalently $g_{n+1} \equiv g_n \mod (\pi^n)$, $h_{n+1} \equiv h_n \mod (\pi^n)$),
(3) $|f - g_n h_n| \leq t^n$ (equivalently $f \equiv g_n h_n \mod (\pi^n)$).

Condition (ii) implies that $(g_n)_{n\in\mathbb{N}}$ and $(h_n)_{n\in\mathbb{N}}$ are Cauchy sequence; since we bound the degree, they will converge to polynomials g and h of degree $\leq m$ and $\leq d - m$. Then condition (iii) gives by continuity that $f = gh$, which forces $\deg g = m$, $\deg h = d - m$. Finally g will be monic: since each g_n has a leading coefficient 1 in degree d, so does g.

Assume that g_n and h_n have already been constructed. If there exists g_{n+1} and h_{n+1} satisfying the above conditions, then $g_{n+1} \equiv g_n \mod (\pi^n)$, and similarly for h_{n+1} and h_n. Therefore, write $g_{n+1} = g_n + \pi^n r$ and $h_{n+1} = h_n + \pi^n s$ for $r, s \in \mathcal{O}_K[X]$. We then have

$$g_{n+1}h_{n+1} = g_n h_n + \pi^n(g_n s + h_n r) + \pi^{2n} rs$$

On the other hand, we already know that $f \equiv g_n h_n \mod (\pi^n)$, so we can also write $f = g_n h_n + \pi^n w$ for some $w \in \mathcal{O}_K[X]$. Since $n \geq 1$, $2n \geq n + 1$ so we have

$$\begin{aligned} & f \equiv g_{n+1}h_{n+1} \mod (\pi^{n+1}) \\ \Leftrightarrow\ & g_n h_n + \pi^n w \equiv g_n h_n + \pi^n(g_n s + h_n r) \mod (\pi^{n+1}) \\ \Leftrightarrow\ & w \equiv g_n s + h_n r \mod (\pi) \\ \Leftrightarrow\ & w \equiv g_1 s + h_1 r \mod (\pi). \end{aligned}$$

We thus find that to obtain g_{n+1} and h_{n+1} iteratively from g_n and h_n, we have to find $r, s \in \mathcal{O}_K[X]$ such that

(1) $g_n + \pi^n r$ is monic of degree m and $h_n + \pi^n s$ is of degree $\leq d - m$,
(2) $w \equiv g_1 s + h_1 r \mod (\pi)$.

We have been provided with polynomials $u, v \in \mathcal{O}_K[X]$ such that $ug_1 + vh_1 \equiv 1 \mod (\pi)$. Multiplying this by w, we find that

$$w \equiv g_1 uw + h_1 vw \mod (\pi).$$

To ensure the condition on the degrees, we can perform the division with remainder of vw by the monic polynomial g_n and let $r \in \mathcal{O}_K[X]$ be the remainder, writing $vw = qg_n + r$ with $q \in \mathcal{O}_K[X]$, $\deg r < \deg g_n = m$. Then $g_{n+1} := g_n + \pi^n r$ has same degree and top coefficient as g_n, so it is monic of degree m. We then let $s = uw + qh_n$ and find

$$\begin{aligned} g_1 s + h_1 r &= g_1(uw + qh_n) + h_1(vw - qg_n) \\ &\equiv g_1(uw + qh_1) + h_1(vw - qg_1) \mod (\pi) \\ &\equiv g_1 uw + qg_1 h_1 + h_1 vw - qg_1 h_1 \mod (\pi) \\ &\equiv g_1 uw + h_1 vw \mod (\pi) \\ &\equiv w \mod (\pi). \end{aligned}$$

Finally, $(f \mod (\pi^n))$ is of degree less than d and $f \equiv g_{n+1}(h_n + \pi^n s) \mod (\pi^{n+1})$ with g_{n+1} monic of degree m. Thus $(g_{n+1} \mod (\pi^{n+1}))$ is also monic of degree m, so $(h_n + \pi^n s \mod (\pi^{n+1}))$ is of degree less than $d - m$. Since we only care about $(h_{n+1} \mod (\pi^{n+1}))$ in order to have (ii) and (iii), we can choose a lift $h_{n+1} \in \mathcal{O}_K[X]$ of $(h_n + \pi^n s \mod (\pi^{n+1}))$ of degree less than $d - m$, and we are done.

Let us conclude by showing the uniqueness. If $\widetilde{g}, \widetilde{h}$ is another solution, we will show that necessarily $\widetilde{g} \equiv g \mod (\pi^n)$, $\widetilde{h} \equiv h \mod (\pi^n)$, which will give $\widetilde{g} = g$, $\widetilde{h} = h$. This is true for $n = 1$ by definition. From $\widetilde{g} \equiv g \mod (\pi^n)$ and $\widetilde{h} \equiv h \mod (\pi^n)$ we can write $\widetilde{g} = g + a\pi^n$, $\widetilde{h} = h + b\pi^n$ for some $a, b \in \mathcal{O}_K[X]$. But then

$$\begin{aligned} &\widetilde{g}\widetilde{h} \equiv f \equiv gh \mod (\pi^{n+1}) \\ \Leftrightarrow\ &gh + \pi^n(ah + bg) \equiv gh \mod (\pi^{n+1}) \\ \Leftrightarrow\ &\pi^n(ah + bg) \equiv 0 \mod (\pi^{n+1}) \\ \Leftrightarrow\ &ah + bg \equiv 0 \mod (\pi) \\ \Leftrightarrow\ &ah_1 \equiv -bg_1 \mod (\pi). \end{aligned}$$

From $ug_1 + vh_1 \equiv 1 \mod (\pi)$, we find $a \equiv aug_1 + avh_1 \equiv aug_1 - bvg_1 \mod (\pi)$ so $(g_1 \mod (\pi)) = (g \mod (\pi))$ divides $(a \mod (\pi))$. Writing this relation as

$$a = zg + \pi t$$

for some $z, t \in \mathcal{O}_K[X]$, we find

$$\widetilde{g} \equiv g + a\pi^n \equiv g(1 + z) + \pi^{n+1} t \equiv g(1 + z) \mod (\pi^{n+1})$$

so $(g \mod (\pi^{n+1}))$ divides $(\widetilde{g} \mod (\pi^{n+1}))$. Since $\widetilde{g}$ and g are monic of the same degree we find $\widetilde{g} \equiv g \mod (\pi^{n+1})$. Then $(h \mod (\pi^{n+1}))$ is the unique quotient in the division with remainder of $(f \mod (\pi^{n+1}))$ by the monic polynomial $(g \mod (\pi^{n+1}) = (\widetilde{g} \mod (\pi^{n+1})$, so $h \equiv \widetilde{h} \mod (\pi^{n+1})$. □

Corollary 10.2 (Hensel's lemma for polynomials, version modulo the maximal ideal)**.** *Let K be a complete non-archimedean field. Let $f \in \mathcal{O}_K[X]$, and assume that there exists polynomials $g_0, h_0 \in \mathcal{O}_K[X]$ such that*

(1) g_1 is monic,
(2) $(g_1 \mod \mathfrak{m})$ and $(h_1 \mod \mathfrak{m})$ are relatively prime,
(3) $f \equiv g_1 h_1 \mod \mathfrak{m}$.

Then there exists polynomials $g, h \in \mathcal{O}_K[X]$ such that

(1) g is monic,
(2) $g \equiv g_1 \mod \mathfrak{m}$ and $h \equiv h_1 \mod \mathfrak{m}$,
(3) $f = gh$.

Proof. Note that $\mathcal{O}_K/\mathfrak{m}$ is a field, so $\mathcal{O}_K/\mathfrak{m}[X]$ is a Euclidean domain and it makes sense to ask that $(g_1 \mod \mathfrak{m})$ and $(h_1 \mod \mathfrak{m})$ are relatively prime. This means that there exists $u \in \mathcal{O}_K[X]$, $v \in \mathcal{O}_K[X]$ such that $ug_1 + vh_1 \equiv 1 \mod \mathfrak{m}$. Now put $t = \max(\|f - g_1 h_1\|, \|ug_1 + vh_1 - 1\|) < 1$. If $t = 0$ there is nothing to do. Otherwise, since t is a maximum, it is the absolute value of an element $\pi \in \mathfrak{m} \setminus \{0\}$, and by construction

$$\|f - g_1 h_1\| \leq |\pi|$$
$$\|ug_1 + vh_1 - 1\| \leq |\pi|.$$

We conclude with the theorem by observing that being equivalent modulo π implies being equivalent modulo $\mathfrak{m}$. □

Remark. We furthermore get from the proof that with $t := \max(\|f - g_1 h_1\|, \|ug_1 + vh_1 - 1\|) < 1$, g and h are the unique polynomials such that g is monic, $f = gh$, and $\|g - g_1\| \leq t$, $\|h - h_1\| \leq t$.

11. Extension of absolute values, part 2: Gauss norms and the lemma of Hensel-Kurschak

Let us come back to the norm we defined on polynomials:

Definition 11.1. *Let K be a non-archimedean field and let $r > 0$. The (r)-Gauss norm on $K[X]$ is the map $\|\cdot\|_r : K[X] \to \mathbb{R}_+$ given by*

$$\|\sum a_k X^k\|_r = \max(|a_k|\, r^k).$$

We also put

$$\|\sum a_k X^k\| := \|\sum a_k X^k\|_1 = \max(|a_k|).$$

which we call the Gauss norm.

Proposition 11.2 (Gauss' lemma)**.** *The Gauss norms are absolute values on $K[T]$ extending that on K, and they extend uniquely to absolute values on $K(T)$ extending that on K.*

Proof. The second statement is routine, so we focus on the first. The triangle inequality, the fact that $\|f\|_r = 0$ if and only if $f = 0$ and that the restriction of $\|\cdot\|_r$ to K is $|\cdot|$ is clear. Thus we have to show that $\|\cdot\|_r$ is multiplicative. We show the case $r = 1$. It suffices to show that if $\|f\| = 1$ and $\|g\| = 1$ then $\|fg\| = 1$; this will turn out to be some version of Gauss' lemma. Indeed, $\|f\|$ and $\|g\|$ are maxima, so there exists $\gamma, \delta \in K$ such that $\|f\| = |\gamma|$, $\|g\| = |\delta|$. Thus $\|f/\gamma\| = 1$, $\|g/\delta\| = 1$ and then

$$\frac{\|fg\|}{\|f\|\|g\|} = \|\frac{f}{\gamma} \cdot \frac{g}{\delta}\| = 1.$$

Observe that $\|f\| = 1$ is equivalent to $f \in \mathcal{O}_K[X]$, together with the existence of a coefficient of f with absolute value exactly 1. In other words,

$$\|f\| = 1 \Leftrightarrow f \not\equiv 0 \mod \mathfrak{m} \Leftrightarrow f \notin \mathfrak{m}\mathcal{O}_K[X].$$

Thus if $\|f\| = 1$ and $\|g\| = 1$, the product of the two non-zero polynomials ($f \mod \mathfrak{m}$) and ($g \mod \mathfrak{m}$) with coefficients in the field $\mathcal{O}_K/\mathfrak{m}$ is the non-zero polynomial ($fg \mod \mathfrak{m}$), i.e. $\|fg\| = 1$. □

Remark. One can show more generally that the similarly-defined Gauss norm $\|\cdot\|_r$ defines an absolute value on the subring of power series $K\langle X\rangle_r := \left\{\sum a_k X^k \in K[[X]], \quad |a_k|\, r^k \xrightarrow[n\to\infty]{} 0\right\} \subseteq K[[X]]$ converging on the closed unit disk of radius r, and the latter is moreover complete for that absolute value. However, one has to be careful: this absolute value extends the absolute value on K, and thus has nothing to do with the T-adic absolute value on $K[[T]]$!

Corollary 11.3. *Let K be a non-archimedean field and let $f \in \mathcal{O}_K[X]$. Then f is irreducible in $\mathcal{O}_K[X]$ if and only if $\|f\| = 1$ and f is irreducible in $K[X]$.*

Proof. ($\Leftarrow$) If $f = gh$ in $\mathcal{O}_K[X]$, then without loss of generality g is a constant $c \in K$. But then $|c| = \|g\| \leq 1$, $\|h\| \leq 1$ and $|c|\,\|h\| = \|f\| = 1$ so $|c| = 1$, which shows that $c \in \mathcal{O}_K^\times$. This proves that f is irreducible in $\mathcal{O}_K$.

($\Rightarrow$)If $f = gh$ in $K[X]$, there is $\gamma, \delta \in K$ such that $\|g\| = |\gamma|$, $\|h\| = |\delta|$. We can then write

$$\frac{f}{\gamma\delta} = \frac{g}{\gamma} \cdot \frac{h}{\delta}$$

with $g/\gamma, h/\delta \in \mathcal{O}_K[X]$ and $|\gamma\delta| = \|g\|\|h\| = \|f\| = 1$ so that $\gamma\delta \in \mathcal{O}_K^\times$. As f is irreducible, so is $f/\gamma\delta$, so either g/γ or h/δ is constant invertible in $\mathcal{O}_K$, which means that g or h is constant non-zero in $K[X]$. □

Corollary 11.4. *Let K be a non-archimedean field with residue field k and let $f \in \mathcal{O}_K$ be a monic polynomial. If $\overline{f}$ is irreducible in k then f is irreducible over K.*

Proof. See exercise sheet 2. □

The following lemma will be crucial in showing the triangle inequality for our candidate absolute value $\left|N_{L/K}(\cdot)\right|_K^{1/[L:K]}$.

Lemma 11.5 (Hensel-Kurschak)**.** *Let K be a complete non-archimedean field. If $f(X) = \sum_{k=0}^{n} a_k X^k$ is irreducible then $\|f\| = \max(|a_0|, |a_n|)$.*

Before going to the proof, we state some corollaries explaining the importance of the lemma:

Corollary 11.6. *Let K be a complete non-archimedean field. If $f \in K[X]$ is irreducible and monic then*

$$f \in \mathcal{O}_K[X] \Leftrightarrow |f(0)| \leq 1.$$

Definition 11.7. *Let L/K be a field extension where K is a non-archimedean field. An element $x \in L$ is called integral over $\mathcal{O}_K$ if $\mu_{K,x} \in \mathcal{O}_K[X]$.*

Corollary 11.8. *Let K be a complete non-archimedean field and let L/K be a finite extension. Then $x \in L$ is integral over $\mathcal{O}_K$ if and only if $N_{L/K}(x) \in \mathcal{O}_K$, if and only if $|N_{L_K}(x)| \leq 1$.*

Proof of the corollary. We have

$$\left|N_{L/K}(x)\right| \leq 1 \Leftrightarrow |\mu_{K,x}(0)|^{[L:K(x)]} \leq 1 \Leftrightarrow |\mu_{K,x}(0)| \leq 1.$$

□

Proof of the lemma. Since $\|f\|$ is a maximum, we can renormalize so that $\|f\| = 1$, in which case we have to show that $\max(|a_n|, |a_0|) = 1$. Suppose, in the aim of obtaining a contradiction, that $|a_0|, |a_n| < 1$. Then, we let

$$r = \min\{k, \quad |a_k| = 1\} \geq 1.$$

For $k < r$ we have $|a_k| < 1$ and thus

$$\begin{aligned} f(X) = \sum_{k=0}^{n} a_k X^k &\equiv a_r X^r + \sum_{k>r} a_k X^k \mod \mathfrak{m} \\ &\equiv X^r (a_r + \sum_{k>r} a_k X^{k-r}) \mod \mathfrak{m} \end{aligned}$$

Since $a_r \not\equiv 0 \mod \mathfrak{m}$, this is a factorization of $(f \mod \mathfrak{m})$ into coprime polynomials, one of them monic of degree r; therefore we can lift this factorization to a factorization $f = gh$ with g monic of degree r, where $\deg f > r > 0$. This is a contradiction to the irreducibility of f. □

Theorem 11.9 (Extension of absolute values)**.** *Let K be a complete non-archimedean field and let L/K be a finite extension. Then*

$$f : x \mapsto \left|N_{L/K}(x)\right|_K^{\frac{1}{[L:K]}}$$

is the unique absolute value on L extending that on K.

Proof. From the previous discussions, it remains only to show the triangle inequality. But we have already shown that f is multiplicative and satisfies $f(x) = 0 \Leftrightarrow x = 0$; therefore it suffices to show that $f(x) \leq 1 \implies f(x+1) \leq 1$. But, we have

$$\begin{aligned} f(x) = \left|N_{L/K}(x)\right|^{[L:K]} \leq 1 &\Leftrightarrow x \text{ is integral over } K \\ &\Leftrightarrow \mu_{K,x}(X) \in \mathcal{O}_K[X] \\ &\Leftrightarrow \mu_{K,x}(X-1) \in \mathcal{O}_K[X] \\ &\Leftrightarrow 1 + x \text{ is integral over } K \\ &\Leftrightarrow f(1+x) \leq 1. \end{aligned}$$

□

Corollary 11.10. *Let K be a complete non-archimedean field and let L/K be an algebraic extension. There is a unique absolute value on L extending that on K.*

Proof. By uniqueness, for $x \in L$ the expression $f(x) = |x|_E$ is independent of any finite subextension $L/E/K$ containing x: if $L/E'/E/K$ are two intermediate finite subextensions then $(|\cdot|_{E'})_{|E} = |\cdot|_E$ since both restrict further to $|\cdot|_K$ on K. To check that f satisfies the axioms of an absolute value, pick any two elements $x, y \in L$ and observe that the corresponding axioms can be checked on the finite extension $K(x,y)/K$, for which they hold since $f_{|K(x,y)} = |\cdot|_{K(x,y)}$. □

In particular, the algebraic closure of K has a unique absolute value extending that on K. We can extract from the two previous proofs the following:

Corollary 11.11. *Let K be a complete non-archimedean field and let L/K be an algebraic extension. The valuation ring of L is the set of elements $x \in L$ integral over K.*

12. Ramfication index and residual degree, part I

Definition–Proposition 12.1. *Let L/K be an extension of non-archimedean fields*[8]*. Write $\kappa(K) = \mathcal{O}_K/\mathfrak{m}_K$ and $\kappa(L) = \mathcal{O}_L/\mathfrak{m}_L$ for their respective residue fields. Then $\kappa(L)$ is a field extension of $\kappa(K)$, of degree $f := [\kappa(L) : \kappa(K)]$ called the residual degree. Moreover, $f \leq [L : K]$.*

Proof. The kernel of the composite map $\mathcal{O}_K \to \mathcal{O}_L \to \kappa(L)$ is exactly $\{x \in \mathcal{O}_K, |x| < 1\} = \mathfrak{m}_K$ so we have an injective morphism of rings $\kappa(K) \to \kappa(L)$. Let $\overline{x_1}, \ldots, \overline{x_f}$ of $\kappa(L)$ over $\kappa(K)$ and choose a family of lifts $(x_i) \in \mathcal{O}_L$.

[8]We've just seen that if K is a complete non-archimedean field, any finite extension L/K is a finite extension of non-archimedean fields, i.e. admits an absolute value extending that on K.

We claim that (x_i) is linearly independent over K, so that $f \leq [L:K]$. Indeed, if not then let

$$\sum \lambda_i x_i = 0$$

be a (finite!) linear relation with $\lambda_i \in K$ not all zero. Let i_0 be an index such that $|\lambda_{i_0}| = \max(|\lambda_i|) > 0$. Then

$$x_{i_0} + \sum_{i \neq i_0} \frac{\lambda_i}{\lambda_{i_0}} x_i = 0$$

is a linear relation with coefficients in $\mathcal{O}_K$, which reduces in $\kappa(L)$ to a non-trivial linear relation between the $\overline{x_i}$. This is a contradiction. □

Definition–Proposition 12.2. *Let K be a complete non-archimedean field with a discrete valuation $v : K^\times \to \mathbb{Z}$. This means that K has a uniformizer π, and $|x|_K = |\pi|^{-v(x)}$ for all $x \in K$, or equivalently $v(x) = -\log(|x|_K)/\log(|\pi|_K)$. Let L/K be a finite extension of degree n. Let $w : L^\times \to \mathbb{R}$ denote the valuation associated to $|\cdot|_L = \left|N_{L/K}(\cdot)\right|_K^{1/n}$ extending v, namely*

$$y \mapsto -\frac{\log(|y|_L)}{\log(|\pi|_K)} = -\frac{1}{n} \cdot \frac{\log(\left|N_{L/K}(y)\right|_K)}{\log(|\pi|_K)} \in \frac{1}{n}\mathbb{Z} \subseteq \mathbb{R}$$

Then $\mathbb{Z} = \mathrm{im}(v) \subseteq \mathrm{im}(w) \subseteq 1/n\mathbb{Z}$ are discrete subgroups of $\mathbb{R}$, so there exists $e \in \mathbb{Z}$ dividing n such that $\mathrm{im}(w) = \frac{1}{e}\mathbb{Z}$ and w is discrete. Equivalently, L has a uniformizer ω with $|\omega|_L = |\pi|_K^{1/e} \geq |\pi|_K$. The number e is called the ramification index of L/K.

Remark. More generally, if L/K is an extension of non-archimedean fields with associated valuations $v : K^\times \to \mathbb{R}$ and $w : L^\times \to \mathbb{R}$, we can define the ramification index

$$e_{w/v} := [w(L^\times) : v(K^\times)] = [\left|L^\times\right|_L : \left|K^\times\right|_K]$$

which is compatible with the previous definition.

Remark. Let K be a complete non-archimedean field with a discrete valuation and let L/K be a finite extension of degree n. We will see later that in this case $ef = n$.

Definition 12.3. *Let K be a complete non-archimedean field and let L/K be an algebraic extension. If $e = 1$* and *the residue field extension is separable, we say that the extension is* unramified. *On the other hand, if $f = 1$, we say that the extension is* totally ramified.

Remark. The separability condition is automatic if the residue field of K is of characteristic 0 or a finite field, or more generally of characteristic p such that any element has a p-th root.

Proposition 12.4. *Let K be a complete non-archimedean field with a discrete valuation $v : K^\times \to \mathbb{Z}$. Then K admits totally ramified extensions of all degrees $n = e \geq 1$.*

Proof. We have shown in the exercise sheet that a polynomial satisfying the Eisenstein criterion is irreducible. Fix a uniformizer $\pi \in \mathfrak{m}_K$. Then for $n \geq 1$, the polynomial $X^n - \pi$ satisfies the Eisenstein criterion, so the extension $L = K(\pi^{1/n})$ is of degree n. Moreover, it is of ramification degree $e \leq n$, but $w(\pi^{1/n}) = \frac{1}{n}w(\pi) = \frac{1}{n}v(\pi) = \frac{1}{n}$ so that $e \geq n$ and thus $e = n$. This shows that the extension is totally ramified by the relation $ef = n$ (the proof of which we postponed). □

Corollary 12.5. *Let K be a complete non-archimedean field with a discrete valuation $v : K^\times \to \mathbb{Z}$. Then its algebraic closure $\overline{K}$ is not finite over K, and the valuation $w : \overline{K}^\times \to \mathbb{R}$ satisfies $\mathrm{im}(w) = \mathbb{Q}$; equivalently, if $\pi \in \mathfrak{m}_K$ is a uniformizer of K, then $\mathrm{im}(|\cdot|_{\overline{K}}) = |\pi|_K^{\mathbb{Q}} \cup \{0\}$.*

Proof. It suffices to prove the last statement; taking over notations from the previous proof, we find that $w((\pi^{1/b})^a) = a/b$ so the image contains $\mathbb{Q}$. On the other hand, for any $x \in \overline{K}^\times$, $w(x)$ can be computed in the finite extension $K(x)$, and thus belongs to $\frac{1}{[K(x):K]}\mathbb{Z} \subseteq \mathbb{Q}$. □

Proposition 12.6. *Let K be a complete non-archimedean field with residue field k. If k admits an extension k' of degree n, then K admits an unramified extension L of degree n with residue field $\kappa(L) = k'$. In particular if k is not algebraically closed, or if the algebraic closure of k is not finite over k, then K has the same property.*

Proof. We can write $k' = k(\alpha_1, \cdots, \alpha_l)$. By induction it thus suffices to treat the case $l = 1$. Suppose $k' = k(\alpha)$. Choose a monic lift $P \in \mathcal{O}_K[X]$ of the minimal polynomial $\mu_{k,\alpha} \in k[X]$. We have shown in the previous section that P is necessarily irreducible in $K[X]$, and has degree n. Consider the extension $L = K[X]/(P)$ and let β denote the class of X in L, so that $L = K[\beta]$. Then L is an extension of degree n of K. Moreover, the minimal polynomial of β is monic with coefficients in $\mathcal{O}_K$, so that $\beta \in \mathcal{O}_L$ as we saw in the previous section. Denote by f the residual degree. Since $\kappa(L)$ contains the element $\overline{\beta}$ which is a root of $\overline{P} = \mu_{k,\alpha}$, we find a field embedding $k[\alpha] \simeq k[X]/(\mu_{k,\alpha}) \to \kappa(L)$ sending α to β. This shows that $f \geq n$, and thus $f = n$ and this embedding is an isomorphism. □

Remark. The above proposition applies even when the valuation is not discrete, at the expense of needing to describe the finite extensions of the residue field.

13. Onto $\mathbb{C}_p$

Definition 13.1. *Let K be a field, let L/K be an extension, and let $\alpha, \alpha' \in L$ be algebraic. We say that α and α' are* conjugate *over K if $\mu_{K,\alpha} = \mu_{K,\alpha'}$, i.e. if α and α' are roots of the same monic irreducible polynomial.*

Remark. If K is a complete non-archimedean field and L/K an algebraic extension, then any two elements in L conjugated over K have the same absolute value, by our explicit formula for the absolute value.

Lemma 13.2. *Let K be a complete non-archimedean field and let $f \in K[X]$ be a monic polynomial of degree n. For any root α of f in $\overline{K}$ we have $|\alpha| \leq \|f\|$.*

Proof. Write $f(X) = \sum_{k=0}^{n} a_k X^k$. Since f is monic we have $\|f\| \geq 1$. For all k we have either $|a_k| \leq 1$ in which case $|a_k|^{1/(n-k)} \leq 1 \leq \|f\|$ or $|a_k| > 1$ in which case $|a_k|^{1/(n-k)} \leq |a_k| \leq \|f\|$. Now if $|\alpha| > \|f\|$, then in particular $|\alpha| > |a_k|^{1/(n-k)}$ for all $k < n$, which we can rewrite as $|a_k| < |\alpha|^{n-k}$. This implies that

$$|\alpha|^n = |\alpha^n| = \left| -\sum_{k=0}^{n-1} a_k \alpha^k \right| < \max(|a_k|\,|\alpha|^k) \leq \max(|\alpha|^{n-k}\,|\alpha|^k) = |\alpha|^n\,,$$

a contradiction. □

Lemma 13.3. *Let K be a complete non-archimedean field and let $f, g \in K[X]$ be monic polynomials of the same degree. Let $\alpha \in \overline{K}$ be a root of f. Then*

$$|g(\alpha)| \leq \|f - g\| \|f\|^{n-1}$$

Proof. Write $f = \sum a_k X^k$, $g = \sum b_k X^k$. Then

$$g(\alpha) = g(\alpha) - f(\alpha) = \sum_{k=0}^{n-1} (b_k - a_k)\alpha^k,$$

so that

$$|g(\alpha)| \leq \|f - g\| \max_{k=0,\ldots,n-1} (|\alpha|^k).$$

But since f is monic we have $|\alpha| \leq \|f\|$, and thus $|\alpha|^k \leq \|f\|^k$, while $\|f\| \geq 1$ implies that $\|f\|^k \leq \|f\|^{n-1}$ for all $k = 0, \ldots, n-1$. This gives the claimed inequality. □

Proposition 13.4 (Continuity of roots)**.** *Let K be a complete non-archimedean field and let $f, g \in K[X]$ be monic polynomials of the same degree. Then for each root $\alpha \in \overline{K}$ of f there exists a roots $\beta \in \overline{K}$ of f such that*

$$|\alpha - \beta| \leq \|f - g\|^{1/n} \|f\|$$

Proof. Write $g(X) = \prod_{i=1}^{n} X - \beta_i$ over $\overline{K}$. Suppose by contradiction that $|\alpha - \beta_i| > \|f - g\|^{1/n} \|f\|$ for all i. Then we get

$$|g(\alpha)| = \prod |\alpha - \beta_i| > \|f - g\| \|f\|^n,$$

which contradicts the lemma since $\|f\| \geq 1$, which implies $\|f\|^n \geq \|f\|^{n-1}$. □

Corollary 13.5. *Let K be a complete non-archimedean field and let $(f_i)_{i \geq 1} \in K[X]^{\mathbb{N}}$ be a sequence of monic polynomials of the same degree n which converges (with respect to the Gauss norm) to a polynomial $g \in K[X]$. Let α_i be a root of f_i in $\overline{K}$ for each i. Then the sequence $(\alpha_i)_{i \geq 1}$ contains a subsequence which converges to a root of g.*

Proof. The polynomial g must be monic of degree n. We apply the proposition: for each i, there exists a root β_i of the (fixed!) polynomial g in $\overline{K}$ such that

$$|\alpha_i - \beta_i| \leq \|g - f_i\|^{1/n} \|f_i\|.$$

Since g has at most n distinct roots, there must exists a root β of g and a strictly increasing map $\varphi : \mathbb{N} \to \mathbb{N}$ such that $\beta_{\varphi(i)} = \beta$ and thus

$$\left|\alpha_{\varphi(i)} - \beta\right| \leq \|g - f_{\varphi(i)}\|^{1/n} \|f_{\varphi(i)}\|.$$

By the strong triangle inequality, since f_i converges to g we have $\|f_{\varphi(i)}\| = \|g\|$ for i big enough. Thus, for i big enough we find

$$\left|\alpha_{\varphi(i)} - \beta\right| \leq \|g - f_{\varphi(i)}\|^{1/n} \|g\|$$

which tends to 0 when i goes to ∞, as claimed. □

Definition 13.6. *We denote by $\mathbb{C}_p$ the completion of the algebraic closure of $\mathbb{Q}_p$ for the extendend p-adic absolute value. More generally, if K is a complete non-archimedean field, we will denote by $\mathbb{C}_K$ the completion of $\overline{K}$ for the extended absolute value.*

We observed that for a non-archimedean field, the absolute value of the limit of a sequence is equal to the absolute value of all its terms after a certain point. Therefore, going from a non-archimedean field to its completion does not change the value group of the absolute value. As a consequence the value group of the p-adic absolute value on $\mathbb{C}_p$ is $p^{\mathbb{Q}}$.

Theorem 13.7. *Let K be a complete non-archimedean normed field. Then $\mathbb{C}_K = \widehat{\overline{K}}$ is complete and algebraically closed, and it is the smallest complete and algebraically closed non-archimedean field containing K isometrically.*

Proof. Let $f \in \mathbb{C}_K[X]$ be a monic polynomial of degree $n \geq 1$. We must find a root of $f \in \mathbb{C}_K$. Since $\overline{K}$ is dense in $\mathbb{C}_K$ by definition, we can find a sequence $(f_i)_{i \geq 1} \in \overline{K}[X]^{\mathbb{N}}$ of monic polynomials of degree n converging to f. But then each f_i has all its roots already in $\overline{K}$. Applying the above corollary, we find a sequence $(\alpha_{\varphi(i)})$ where each $\alpha_{\varphi(i)} \in \overline{K}$ is a root of $f_{\varphi(i)}$, converging to a root of f in $\overline{\mathbb{C}_K}$. But $\overline{K} \subset \mathbb{C}_K$ and $\mathbb{C}_K$ is complete, hence closed in $\overline{\mathbb{C}_K}$, so the root belongs to $\mathbb{C}_K$, as we needed.

The second statement is left to the reader. □

Proposition 13.8. *Let K be a complete non-archimedean field with residue field $\kappa(K)$. Then $\kappa(\overline{K})$ is an algebraic closure of $\kappa(K)$.*

Proof. We first show that $\kappa(\overline{K})$ is algebraically closed. Let $\overline{p} \in \kappa(\overline{K})[X]$ be a monic irreducible polynomial. We can lift $\overline{p}$ to a monic polynomial $p \in \mathcal{O}_{\overline{K}}$, which must also be irreducible in $\mathcal{O}_{\overline{K}}$ and thus also in K since $\|p\| = 1$. This implies that $\deg \overline{p} = \deg p = 1$.

We now show that $\kappa(\overline{K})$ is algebraic over $\kappa(K)$. Let $\overline{x} \in \kappa(\overline{K})$ and lift it to $x \in \mathcal{O}_{\overline{K}}$. Then x is integral over $\mathcal{O}_K$ so $\mu_{K,x} \in \mathcal{O}_K[X]$. Reducing back

we find that $\overline{\mu_{K,x}}$ is a monic polynomial over $\kappa(K)$ such that $\overline{\mu_{K,x}}(\overline{x}) = 0$, so we are done. □

Lemma 13.9. *Let L/K be an extension of non-archimedean fields such that K is dense in L. Then K and L have the same residue fields. In particular, if K is any non-archimedean field, then K and its completion have the same residue field.*

Proof. The map between residue fields is a map of fields hence injective. It suffices to show that it is surjective. Let $\overline{x} \in \kappa(L)$ with lift $x \in \mathcal{O}_L$. Then by density there exists $y \in K$ such that $|y - x| < |x| \leq 1$. By the strong triangle inequality, we get that $|y| = |x| \leq 1$, and thus $y \in \mathcal{O}_K$. Moreover we can write $x = y + (y - x)$ where $y \in \mathfrak{m}_L$ by construction, which gives in $\kappa(L)$ that $\overline{x} = \overline{y}$ is in the image of $\kappa(K) \to \kappa(L)$. □

Corollary 13.10. *Let K be a complete non-archimedean field with residue field $\kappa(K)$. Then $\kappa(\mathbb{C}_K)$ is an algebraic closure of $\kappa(K)$. In particular, the residue field of $\mathbb{C}_p$ is $\overline{F_p}$.*

We finish this section with two things: first we introduce Krasner's lemma and its consequences; the lemma is useful in a lot of situations. Then we examine whether it was actually needed to complete the algebraic closure, i.e. whether the algebraic closure can be complete; we show that the algebraic closure of a complete non-archimedean field is never complete.

Definition 13.11. *Let K be a field. A polynomial $P \in K[X]$ is said to be separable if it has no multiple root in any algebraically closed field containing K, which is equivalent to the condition* $\gcd(P, P') = 0$.

Let L/K be an extension. An algebraic element $x \in L$ is said to be separable if its minimal polynomial is separable, or equivalently if there is a separable polynomial $P \in K[X] \setminus \{0\}$ such that $P(x) = 0$.

Remark. If P is irreducible over K, then $\det P' < \deg P$ so $\gcd(P, P') = 1 \Leftrightarrow P' \neq 0$. If K is of characteristic 0, this is always true, i.e. an irreducible polynomial is separable. However, in characteristic p there are counter-examples: consider the field extensions $\mathbb{F}_p \subseteq \mathbb{F}_p(T^p) \subseteq \mathbb{F}_p(T)$. Then one can show that the polynomial $P(X) = X^p - T^p \in \mathbb{F}_p(T^p)[X]$ is irreducible, but it is not separable since over $\mathbb{F}_p(T)$ it obtains the factorization $X^p - T^p = (X - T)^p$ showing that T is a multiple root of order p.

Definition 13.12. *Let K be a complete non-archimedean field and let $\alpha \in \overline{K}$ be a* separable *element of degree > 1. We put*

$$r(\alpha) := \inf_{\substack{\alpha' \text{ conjugate to } \alpha \\ \alpha' \neq \alpha}} |\alpha' - \alpha|$$

which we call the "Krasner radius" of α.[9]

[9]This is non-standard terminology.

Lemma 13.13 (Krasner's lemma)**.** *In the above situation, if $\beta \in \overline{K}$ is such that $\beta \in B(\alpha, r(\alpha))$ then $K(\alpha) \subseteq K(\beta)$, or in other words α can be written as a polynomial in β with coefficients in K.*

Proof. Put $L = K(\beta)$ and suppose by contradiction that $\alpha \neq L$. Consider the extension $L(\alpha)/L$, which by hypothesis is of degree $m > 1$. Then $\mu_{L,\alpha}$ is of degree m and divides $\mu_{K,\alpha}$, so it also has only simple roots, and has at least two of them. Thus, we can pick $\alpha' \in \overline{K}$, $\alpha' \neq \alpha$ a conjugate of α over L. But then $\mu_{L,\alpha}(X + \beta)$ is monic irreducible with coefficients in L, and has the two distinct roots $\alpha - \beta$ and $\alpha' - \beta$; this shows that $\alpha - \beta$ is conjugated to $\alpha' - \beta$ over L. The remark above then implies that

$$\left|\alpha' - \beta\right| = |\alpha - \beta|$$

so by the strong triangle inequality

$$\left|\alpha - \alpha'\right| \leq \max(|\alpha - \beta|, \left|\alpha' - \beta\right|) < r(\alpha),$$

a contradiction. □

Corollary 13.14. *Let K be a complete non-archimedean field, let $f \in K[X]$ be a separable monic irreducible polynomial of degree $n > 1$ with a root $\alpha \in \overline{K}$. There exists $\varepsilon > 0$ such that for every monic polynomial $g \in K[X]$ of degree n satisfying $\|f - g\| < \varepsilon$, g is irreducible over K and has a root in $\beta \in \overline{K}$ such that $\beta \in B(\alpha, r(\alpha))$ and $K(\beta) = K(\alpha)$.*

More precisely, we can take $\varepsilon = \|f\|^{-n} r(\alpha)^n$.

Proof. The proposition on continuity of roots gives the existence of a root β of any monic polynomial g of degree n such that

$$|\alpha - \beta| \leq \|f - g\|^{1/n} \|f\|.$$

Thus if $\|f - g\| < \varepsilon := \|f\|^{-n} r(\alpha)^n$ we find

$$|\alpha - \beta| < r(\alpha),$$

and Krasner's lemma then gives that $K(\alpha) \subseteq K(\beta)$. From there we get

$$n = \deg g \geq [K(\beta) : K] \geq [K(\alpha) : K] = \deg f = n$$

so we have equality everywhere, which shows that g is irreducible (it is monic and has the same degree as the minimal polynomial of its root β) and $K(\beta) = K(\alpha)$. □

Remark. It can be shown that α is a separable algebraic element if and only if $K(\alpha)$ is a separable extension. In particular, in the conclusion above, we find $\beta \in K(\alpha)$ must be separable, so that g is separable as well.

Theorem 13.15. *Let K be a complete non-archimedean field of characteristic 0 with a non-trivial absolute value. If $[\overline{K} : K] = \infty$ then $\overline{K}$ is not complete.*

Proof. Since K is of characteristic 0, any element $x \in \overline{K}$ is separable. Choose a sequence $(x_n)_{n\geq 0}$ of elements in $\overline{K}$, with $x_0 = 1$, that forms a linearly independent family over K. We then define inductively $c_1 = 1, c_2, \ldots, c_n, \ldots$ non-zero elements of K such that

$$|c_{n+1}|\,|x_{n+1}| < \max\left(\frac{1}{2^{n+1}}, |c_n x_n|, r\left(\sum_{k=1}^{n} c_k x_k\right)\right)$$

where r denotes the Krasner radius. Note that $\sum_{k=1}^{n} c_k x_k \in \overline{K}$ is of degree > 1, i.e. does not belong to K. Indeed, as $x_0 = 1 \in K$, if the sum was in K, there would exist $b \in K$ with $b = \sum_{k=1}^{n} c_k x_k$ or equivalently

$$-bx_0 + \sum_{k=1}^{n} c_k x_k = 0.$$

Since the x_i are linearly independent and $c_k \neq 0$ for all k by construction, this is a contradiction. Thus the Krasner radius above is well-defined.

We want to show that the series $\sum_{k\geq 1} c_k x_k$ does not converge in $\overline{K}$. If it did, then letting $x \in \overline{K}$ denote its limit, we would have for all $n \geq 1$:

$$\left|x - \sum_{k=1}^{n} c_k x_k\right| = \left|\sum_{k>n} c_k x_k\right| \leq |c_{n+1} x_{n+1}| < r\left(\sum_{k=1}^{n} c_k x_k\right)$$

so by Krasner's lemma $\sum_{k=1}^{n} c_k x_k \in K(x)$. Since every c_n is non-zero, we obtain first that $c_1 x_1 \in K(x)$ so $x_1 \in K(x)$, and then by induction $x_n \in K(x)$ for all $n \geq 1$. But this is impossible as $[K(x) : K] < \infty$, while (x_i) is an infinite linearly independent family. □

Remark. With some modifications and more knowledge about separable extensions, one can remove the hypothesis on the characteristic in the above theorem. See [BGR84, §3.4.3, Lemma 1].

Remark. On the other hand, if K has the trivial absolute value, then K is automatically complete, and its algebraic closure must have the trivial absolute value hence also be complete, independently of its degree over K.

Corollary 13.16. *The field $\overline{\mathbb{Q}_p}$ is not complete.*

Proof. We have shown with the theory of ramification index that $\mathbb{Q}_p$ has totally ramified extensions of arbitrary degree, which implies that $[\overline{\mathbb{Q}_p} : \mathbb{Q}_p] = \infty$. □

14. Finite fields

15. Taxonomy of the finite extensions of $\mathbb{Q}_p$

Proposition 15.1. *Let K be a complete non-archimedean field with a discrete valuation and let L/K be an algebraic extension. Then $ef = [L : K]$.*

Remark. The above says that if L/K is the completion of an algebraic extension with finite residue degree and ramification index, it is actually a finite extension.

Proof. We have shown that if $[L:K]$ is finite then f and e are finite. Thus if e or f is infinite then $[L:K]$ is infinite and the relation is trivially true. Suppose now that e and f are finite. Keeping notations as above, we fix $\pi \in \mathcal{O}_K$ with $v(\pi) = 1$ and $\omega \in \mathcal{O}_L$ with $w(\omega) = 1/e$. Note that by definition, $\mathfrak{m}_L$ is the ideal generated by ω. Since $w(\omega^e/\pi) = e \cdot 1/e - 1 = 0$, we have $\omega^e/\pi \in \mathcal{O}_L^\times$ so that $\omega^e \mathcal{O}_L = \pi \mathcal{O}_L$.

Observe that $\mathcal{O}_L/(\omega^e) = \mathcal{O}_L/(\pi)$ is naturally a $\kappa(K) := \mathcal{O}_K/(\pi)$-vector space. We will show that $\mathcal{O}_L/(\pi) = \mathcal{O}_L/(\omega^e)$ is of dimension $ef < infty$ over $\kappa(K)$. We have a descending chain of sub-vector spaces

$$\mathcal{O}_L/\omega^e\mathcal{O}_L \supset \omega\mathcal{O}_L/\omega^e\mathcal{O}_L \supset \cdots \supset \omega^{e-1}\mathcal{O}_L/\omega^e\mathcal{O}_L \supset \{0\}\,.$$

The quotient of two successive steps is

$$\frac{\omega^k\mathcal{O}_L/\omega^e\mathcal{O}_L}{\omega^{k+1}\mathcal{O}_L/\omega^e\mathcal{O}_L} \simeq \omega^k\mathcal{O}_L/\omega^{k+1}\mathcal{O}_L$$

Moreover, the morphism

$$\begin{array}{ccc} \mathcal{O}_L & \to & \mathcal{O}_L \\ x & \mapsto & \omega^k x \end{array}$$

induces a well-defined (non-zero hence injective) morphism $\kappa(L) \to \mathcal{O}_L/\omega^{k+1}\mathcal{O}_L$ sending $\overline{x}$ to $\omega^k x$. Its image is thus $\omega^k\mathcal{O}_L/\omega^{k+1}\mathcal{O}_L$, so we have an isomorphism of $\kappa(K)$-vector spaces $\kappa(L) \xrightarrow{\simeq} \omega^k\mathcal{O}_L/\omega^{k+1}\mathcal{O}_L$. Finally, we get

$$\begin{aligned} \dim(\mathcal{O}_L/\omega^e\mathcal{O}_L) &= \sum_{k=0}^{e-1} \dim(\omega^k\mathcal{O}_L/\omega^e\mathcal{O}_L) - \dim(\omega^{k+1}\mathcal{O}_L/\omega^e\mathcal{O}_L) \\ &= \sum_{k=0}^{e-1} \dim(\omega^k\mathcal{O}_L/\omega^{k+1}\mathcal{O}_L) \\ &= e\dim(\kappa(L)) \\ &= ef. \end{aligned}$$

We now relate the dimension of $\mathcal{O}_L/(\pi)$, which is finite equal to ef, to $[L:K]$. Pick a basis $\overline{x_1}, \ldots, \overline{x_{ef}}$ of $\mathcal{O}_L/(\pi)$ over $\kappa(K)$ and choose a family of lifts $(x_i) \in \mathcal{O}_L$. We claim that (x_i) is linearly independent over K. Indeed, if

$$\sum \lambda_i x_i = 0$$

is a linear relation with $\lambda_i \in K$ not all zero, put $k = \min(v(\lambda_i))$. Then for every i, $v(\pi^{-k}\lambda_i) \geq 0$ so that $\pi^{-k}\lambda_i \in \mathcal{O}_K$, and there exists an index i_0 such that $v(\pi^{-k}\lambda_{i_0}) = 0$, so that $\pi^{-k}\lambda_{i_0} \not\equiv 0 \mod \pi$. Thus

$$\sum \pi^{-k}\lambda_i x_i$$

is a linear relation with coefficients in $\mathcal{O}_K$, which reduces modulo π to a linear relation $\sum \overline{\pi^k \lambda_i} \overline{x_i}$ over $\kappa(K)$ with at least one non-zero coefficient, namely its coefficient on $\overline{x_{i_0}}$. This is a contradiction.

Consider the sub-K-vector space V of L generated by the (x_i), which is of dimension ef by the previous paragraph. We will show that it is equal to L, concluding that $ef = [L : K] < \infty$. It suffices to show that any $x \in \mathcal{O}_L$ belongs to V. For $x \in \mathcal{O}_L$, we can lift an expression of $\overline{x}$ in the basis $\overline{x_i}$ to an expression

$$x = \sum a_i x_i + y$$

where $y \in \pi\mathcal{O}_L$ and $a_i \in \mathcal{O}_L$. This means that $\mathcal{O}_L \subseteq V + \pi\mathcal{O}_L$. Since V is stable by scalar multiplication, iterating we find

$$\mathcal{O}_L \subseteq V + \pi\mathcal{O}_L \subseteq V + \pi V + \ldots + \pi^{k-1}V + \pi^k\mathcal{O}_L = V + \pi^k\mathcal{O}_L$$

for all $k \geq 1$. We reformulate this as saying that for any $x \in \mathcal{O}_L$ and $k \geq 0$, there exist $v_k \in V$, $y_k \in \pi^k\mathcal{O}_L$ such that $x - v_k = y_k$. Since $w(y_k) \geq k \xrightarrow[k\to\infty]{} \infty$, this means that $v_k \xrightarrow[k\to\infty]{} x$ so that $x \in \overline{V}$. But V is finite-dimensional so it is closed, and thus $x \in V$. □

16. Monsky's theorem

Reference: [AZ18, Chapter 22: one square and an odd number of triangles].

We need the extension of the 2-adic valuation on $\mathbb{Q}$ to a valuation $v : \mathbb{R} \to \Gamma \cup \{\infty\}$. Alternatively, in any figure constructed, the extension of $\mathbb{Q}$ generated by the coordinates of the vertices of the figure is an extension of finite type of $\mathbb{Q}$, so the tools we have developed show that $|\cdot|_2$ has an extension to that field, which suffices for the proof.

17. p-adic methods applied to Diophantine equations

References:

(1) Keith Conrad's note "Selmer's exampe" `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf` (this one necessitates some algebraic number theory for the second part)
(2) Keith Conrad's note "Integral solutions to $x^3 - 2y^3 = 1$" `https://kconrad.math.uconn.edu/blurbs/gradnumthy/x3-2y3=1.pdf`
(3) [Coh07, Prop. 4.5.17]. Everything from 4.5 to the end of chapter 6 might be relevant; it is a matter of picking something accessible with p-adic methods and not too much (or none) algebraic number theory. Prop 4.5.17 is expanded upon in chapter 3 of Josha Box's unpublished bachelor thesis "An introduction to Skolem's p-adic method for solving Diophantine equations" at the University of Amsterdam; this might give some ideas and references for generalizations.

18. Tate algebras

References:

(1) Piotr Achinger's notes [Ach21, Chapter 1-3]
(2) Their source [Bos14, Sections 1 and 2]
(3) [BGR84] (warning, this one has way too much material, and is more a reference text to be cited than a textbook to be read).

References

[Ach21] Piotr Achinger. *Introduction to non-Archimedean Geometry*. 2021. URL: https://achinger.impan.pl/rigid/notes.pdf.

[AZ18] Martin Aigner and Günter M. Ziegler. *Proof from THE BOOK*. 6th ed. Springer Berlin, Heidelberg, 2018. ISBN: 978-3-662-57264-1.

[BGR84] S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedean Analysis. A Systematic Approach to Rigid Analytic Geometry*. 1st ed. Grundlehren der mathematischen Wissenschaften. Springer Berlin, Heidelberg, 1984. ISBN: 978-3-540-12546-4.

[Bos14] Siegfried Bosch. *Lectures on Formal and Rigid Geometry*. 1st ed. Lecture Notes in Mathematics. Springer Cham, 2014. ISBN: 978-3-319-04417-0.

[Coh07] Henri Cohen. *Number Theory. Volume 1: Tools and Diophantine equations*. Vol. 239. Graduate Texts in Mathematics. Springer Science + Business media, LLC, 2007. ISBN: 978-0-387-49922-20.