Local Fields

Tim Browning
Notes by Florian Bouyer

Contents

1 Foundations

Absolute Values

Let K be a field.

Definition 1.1. An *absolute value* on K is a map $|\cdot| : K \to \mathbb{R}_{>0}$

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x| \cdot |y| \forall x, y \in K$
3. $|x + y| \leq |x| + |y|$ (the $\triangle$ inequality)

Definition. An absolute value on K is called *non-archimedean* if also

1. $|x + y| \leq \max\{|x|, |y|\}$ (the ultrametric inequality)

Otherwise we say the absolute value is *archimedean*

Example.

1. $K = \mathbb{Q}$ and $|\cdot|$ to be the usual absolute value given by inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$. This is an archimedean absolute value.
2. Take $|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$. This is non-archimedean absolute value. "The trivial absolute value"
3. $K = \mathbb{Q}$ and p a prime. For $x \in \mathbb{Q}^*$ the p-adic valuation is $\nu_p(x) = r$ if $x = p^r \frac{u}{v}$ for $u, v \in \mathbb{Z}, r \in \mathbb{Z}$ and $p \nmid uv$. We extend to all of $\mathbb{Q}$ by setting $\nu_p(0) = +\infty$

   Check: $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ and $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$ $(*)$

   Define the p-adic absolute value on $\mathbb{Q}$ to be $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ by $|x|_p = \begin{cases} p^{\nu_p(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$. This satisfies the axioms of being a non-archimedean absolute value (using $(*)$)

   Note. $|p^n|_p = p^{-n}$ so $p^n \to 0$ as $n \to \infty$.
4. Let K be any field. Put $F = K(T) = \left\{ \frac{P(T)}{Q(T)} : P, Q \in K[T], Q \neq 0 \right\}$. Define the valuation

$$\nu_\infty\left(\frac{P(T)}{Q(T)}\right) = \begin{cases} \deg Q - \deg P & \frac{P}{Q} \neq 0 \\ +\infty & \frac{P}{Q} = 0 \end{cases}$$

   Check this satisfies $(*)$. If $c > 1$, then we get a non-archimedean absolute value on F given by $|F(T)|_\infty := c^{-\nu_\infty(f(T))}$.

   Note. If $K = \mathbb{F}_q$ then convenient to take $c = q$.

Lemma 1.2. *Let $|\cdot|$ be an absolute value on a field K. Then*

1. $|1| = 1$
2. *$x \in K$ such that $x^n = 1$, then $|x| = 1$.*

3. $x \in K$, *then* $|-x| = |x|$

4. K *is a finite field then the absolute value has to be the trivial absolute value*

Proof.

1. Note that $x \neq 0 \Rightarrow x > 0$. We have $|1| = |1^2| = |1| \cdot |1|$. So 1. holds.

2. Note that $1 = |1| = |x^n| = |x|^n \Rightarrow |x| = 1$

3. Note that $-x = -1 \cdot x$

4. Follows from 2. since any non-zero element x of a finite field satisfies $x^n = 1$ for some n.

□

The following result gives a criterion for checking whether an absolute value is non-archimedean.

Lemma 1.3. *Let* $|\cdot|$ *be an absolute value on a field* K. *Then* $|\cdot|$ *is non-archimedean if and only if* $|e| \leq 1$ *for all* e *in the additive ring generated by* 1.

Proof. "$\Rightarrow$" Since $|n| = |-n|$ we may as well assume that $n \geq 1$. Then $|n| = |\underbrace{1 + \cdots + 1}_{n\,\text{times}}| \leq |1| = 1$

"$\Leftarrow$" Suppose $|e| \leq 1$ for all elements e in the additive ring generated by 1. Let $x, y \in K$, then

$$\begin{aligned} |x+y|^m &= \left| \sum_{j=0}^{m} \binom{m}{j} x^j y^{m-j} \right| \\ &\leq \sum_{j=0}^{m} \left| \binom{m}{j} \right| |x|^j |y|^{m-j} \\ &\leq \sum_{j=0}^{m} |x|^j |y|^{m-j} \qquad \text{by assumption} \left| \binom{m}{j} \right| \leq 1 \\ &\leq \max(\{|x|, |y|\}^m \end{aligned}$$

Take mth root and let $m \to \infty$ (since $(m+1)^{1/m} \to 1$ as $m \to \infty$) □

Corollary 1.4. *If* $\operatorname{char}(K) \neq 0$ *then all absolute values are non-archimedean*

Proof. The ring in Lemma 1.3 is a finite field. Then apply Lemma 1.2 part 4. □

Corollary 1.5. *Suppose* $F \subset K$ *is a subfield of* K *and* $|\cdot|$ *is an absolute value on* K. *Then* $|\cdot|$ *is non-archimedean on* K *if and only if* $|\cdot|$ *is non-archimedean on* F

Topology

Let K be a field with absolute value $|\cdot|$ on K. Then we get a metric on K induced by $|\cdot|$. Call it $d : K \times K \to R_{\geq 0}$ defined by $d(x, y) \mapsto |x - y|$.

Exercise. Check this is a metric.

The notion of distance on fields with non-archimedean values is weird.

Lemma 1.6. *Let K be a field with non-archimedean absolute value. If $x, y \in K$ with $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$*

Proof. Without loss of generality assume $|x| > |y|$. Then $|x+y| \leq \max\{|x|, |y|\} = |x|$ and $|x| = |x+y-y| \leq \max\{|x+y|, |y|\}$. Hence $|x| \leq |x+y| \leq |x|$. $\square$

Definition 1.7. Let K be a field with absolute value $|\cdot|$. Let $a \in K$ and $r \in \mathbb{R}_{\geq 0}$. The *open ball* of radius r and centre a is $B(a, r) = \{x \in K : |x - a| < r\}$. The *closed ball* of radius r and centre a is $\overline{B}(a, r) = \{x \in K : |x - a| \leq r\}$.

A set $U \subset K$ is *open* if and only if $\forall x \in U$ there exists an open ball around x contained in U. A set is *closed* if and only if its complement in K is open

Lemma 1.8. *Let K be a field with non-archimedean absolute value $|\cdot|$. Then*

1. $b \in B(a, r) \Rightarrow B(a, r) = B(b, r)$
2. $b \in \overline{B}(a, r) \Rightarrow \overline{B}(a, r) = \overline{B}(b, r)$
3. $B(a, r) \cap B(a', r') \neq 0 \iff B(a, r) \subset B(a', r')$ *or* $B(a, r) \supset B(a', r')$
4. $\overline{B}(a, r) \cap \overline{B}(a', r') \neq 0 \iff \overline{B}(a, r) \subset \overline{B}(a', r')$ *or* $\overline{B}(a, r) \supset \overline{B}(a', r')$
5. $B(a, r)$ *is both open and closed*
6. $\overline{B}(a, r)$ *is both open and closed.*

Proof. We prove 1. 3. 5. only.

1. $b \in B(a, r)$ and $c \in B(b, r)$. $|c - a| \leq \max\{|c - b|, |b - a|\} < r$, i.e., $B(b, r) \subset B(a, r)$. Reverse inclusion follows from symmetry since $a \in B(b, r)$.

3. Follows form 1.

5. $b \in B(a, r)$ implies $B(b, r) \subset B(a, r)$, so any open ball is open. To show that it is closed, note that $b \notin B(a, r) \Rightarrow a \notin B(b, r)$. So neither ball is contained in the other and they are disjoint. Hence $B(b, r) \subset K \setminus B(a, r)$ and the complement of $B(a, r)$ in K is open. $\square$

Remark. Recall that a set S is said to be *disconnected* if there exists open sets U, V such that

- $U \cap V = \emptyset$,
- $S \subset U \cup V$
- $S \cap U \neq \emptyset$ and $S \cap V \neq \emptyset$

Otherwise S is *connected.* If $x \in K$ then the *connected component* of x is the union of all connected sets containing it.

Example. $K = \mathbb{R}$ with usual absolute value, then connected component of any $x \in \mathbb{R}$ is $\mathbb{R}$.

Exercise. If $|\cdot|$ is a non-archimedean absolute value on a filed K, then the connected component of any $x \in K$ is $\{x\}$, i.e., K is *totally disconnected* topological space.

Equivalence

Definition 1.9. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field K are *equivalent* if they induce the same topology on K. (i.e., every set which is open with respect to $|\cdot|_1$ is open with respect to $|\cdot|_2$)

Given an absolute value $|\cdot|$ on a field K, a sequence $\{a_n\}_n$ in K *converges* to a in the induced topology if and only if $\forall \epsilon > 0 \exists N \in \mathbb{N}$ such that for $n > N$, $|a_n - a| < \epsilon$. Equivalently, for all open sets U containing a, there exists N such that $a_n \in U$ for $n > N$

Thus the notion of convergence depends on the topology induced by the absolute value.

Lemma 1.10. *Let $|\cdot|_1, |\cdot|_2$ be absolute values on field K, with $|\cdot|_1$ non-trivial. Then the following are equivalent*

1. $|\cdot|_1$, $|\cdot|_2$ *are equivalent*
2. $\forall x \in K$, $|x|_1 < 1 \iff |x|_2 < 1$
3. $\exists \alpha > 0$ *such that* $\forall x \in K$, $|x|_1 = |x|_2^{\alpha}$.

Proof.

3. $\Rightarrow$ 1. Then $|x-a|_2 < r \iff |x-a|_1 < r^{\alpha}$. So any open ball with respect to $|\cdot|_2$ is an open ball with respect to $|\cdot|_1$. Hence the topology must be the same and the absolute value are equivalent.

1. $\Rightarrow$ 2. $|x|_1 < 1 \iff x^n \to 0$ as $n \to \infty$ with respect to $|\cdot|_1 \overset{1.}{\iff} x^n \to 0$ as $n \to \infty$ with respect $|\cdot|_2 \iff |x|_2 < 1$

2. $\Rightarrow$ 3. Now $|x|_1 > 1 \iff |x^{-1}| < 1 \iff |x^{-1}|_2 < 1 \iff |x|_2 > 1$. Also $|x|_1 = 1 \iff |x|_2 = 1$. Now pick (and fix) $a \in K^*$ such that $|a|_1 < 1$ (which is possible since $|\cdot|_1$ is non-trivial). Then also $|a|_2 < 1$. Let $\alpha = \frac{\log|a|_1}{\log|a|_2} > 0$. Choose $b \in k^*$

   1. $|b|_1 = 1$ then $|b|_2 = 1$ and $1 = 1^{\alpha}$
   2. $|b|_1 < 1$ by assumption $|b|_2 < 1$. Define $\beta_i = \frac{\log|a|_i}{\log|b|_i}$ for $o = 1, 2$. We show that $\beta_1 = \beta_2$ which implies $\frac{\log|b|_1}{\log|b|_2} = \frac{\log|a|_1}{\log|a|_2} = \alpha$.
      Suppose that $\beta_1 > \beta_2$, then $\exists \frac{m}{n} \in \mathbb{Q}$ such that $\beta_2 \leq \frac{m}{n} < \beta_1$. Set $x = a^n b^{-m} \in k$, then $\log|x|_i = n\log|a|_i - m\log|b|_i = \underbrace{n\log|b|_i}_{<0} \underbrace{\left(\beta_i - \frac{m}{n}\right)}_{\begin{cases} >0 & i=1 \\ <0 & i=2 \end{cases}}$, hence we have a contradiction with $|x|_1 < 1$ and $|x|_2 > 1$. Similarly if $\beta_2 > \beta_1$. Hence $\beta_1 = \beta_2$
   3. If $|b|_1 > 1$, $|b|_2 > 1$, replace b by b^{-1} and get $\left|b^{-1}\right|_1 < 1$ and $\left|b^{-1}\right|_2 < 1$

$\square$

How independent inequivalent absolute value are

Lemma 1.11. *Let $|\,|_1, \ldots, |\,|_J$ be non trivial inequivalent absolute values on K. Then there exists $x \in K$ such that $|x|_1 > 1$ and $|x|_j < 1$ for $2 \leq j \leq J$.*

Proof. By induction on J.

$J=2$ Since $|\,|_1, |\,|$ are non-trivial and non-equivalent, by the previous lemma there exists $y \in K$ such that $|y|_1 < 1$ and $|y|_2 \geq 1$, and $z \in K$ such that $|z|_1 \geq 1$ and $|z|_2 < 1$. Let $x = zy^{-1}$, then $|x|_1 = |z|_1 |y|_1^{-1} > 1$ and $|x|_2 = |z|_2 |y|_2^{-1} < 1$

$J>2$ By induction, there exists $y, z \in K$ such that $|y|_1 > 1$, $|y|_j < 1$ for $2 \leq j < J$ and $|z|_1 < 1$, $|z|_j > 1$ for $2 \leq j < J$. Consider $|y|_J$ and we have different cases:

1. $|y|_J < 1$ so take $x = y$
2. $|y|_J = 1$ so take $x = y^n z$ for large enough n
3. $|y|_J > 1$, then $\left|\frac{y^n}{1+y^n}\right|_j = \left|\frac{1}{1+y^{-n}}\right|_j \underset{n\to\infty}{\to} \begin{cases} 1 & j = 2, \dots, J \\ 0 & \text{else} \end{cases}$. So Let $x = \left(\frac{y^n}{1+y^n}\right) z$ for large enough n

$\square$

Theorem 1.12 (Weak Approximation). *Let $|\,|_1, \dots, |\,|_J$ be non trivial inequivalent absolute values on K. Let $b_j \in K$ for $j = 1, \dots, J$ and let $\epsilon > 0$. Then there exists $x \in K$ such that $|x - b_j|_j < \epsilon$ for all $j = 1, \dots, J$.*

Proof. By Lemma 1.11, there exists $x_j \in K$ such that $|x_j|_j > 1$ but $|x_j|_i < 1$ for $i \neq j$. Consider $\left|\frac{x_j^n}{1+x_j^n}\right|_j \underset{n\to\infty}{\to} \begin{cases} 1 & i = j \\ 0 & \text{else} \end{cases}$. Take $w_n = \sum_{j=1}^J b_j \left(\frac{x_j^n}{1+x_j^n}\right) \underset{n\to\infty}{\to} b_j$, so take $x = w_n$ for n large enough. $\square$

Remark. This is clearly related to the Chinese Remainder Theorem. Let $p_1, \dots, p_j$ be distinct primes and $m_j \in \mathbb{N}, b_j \in \mathbb{Z}$. Then there exists $x \in \mathbb{Z}$ such that $x \equiv b_j \mod p_j^{m_j}$. Using the Theorem above, $|x - b_j|_j < p_j^{-m_j}$ with p_j-adic absolute value

1.1 Completion

Definition 1.13.

1. A sequence $\{x_n\}$ is a field K is called *Cauchy* if $\forall \epsilon > 0, \exists N > 0$ such that $\forall m, n > N$, $|x_m - x_n| < \epsilon$
2. $(K, |\cdot|)$ is *complete* if every Cauchy sequence is convergent
3. A subset $S \subset K$ is dense if $\forall x \in K$, $\forall \epsilon > 0$, $B(x, \epsilon) \cap S \neq 0$. That is, $\forall x \in K$, there exists a sequence $\{x_n\} \in S$ such that $\{x_n\} \to x$.
4. A field $\left(\widehat{K}, \|\,\|\right)$ is a *completion* of $(K, |\,|)$ if
   (a) There exists an embedding $\iota : K \to \widehat{K}$ which respect absolute values
   (b) $\mathrm{im}(K)$ is dense in $\widehat{K}$
   (c) $\left(\widehat{K}, \|\,\|\right)$ is complete

Theorem 1.14. *Let $(K, |\,|)$ be a field. Then there exists a completion $(\widehat{K}, ||\,||)$ of K and it is unique as any two completions are canonically isomorphic. That is if $(\widehat{K}_j, ||\,||_j)$ for $j = 1, 2$ then there exists a unique isomorphism of $\widehat{K}_1 \cong \widehat{K}_j$ which is the identity of K and preserves $||\,||_1 = ||\,||_2$*

Proof.

Existence of Completion Let $\mathcal{K}$ be the set of all Cauchy Sequences in K. This is a ring as $\{a_n\} + \{b_n\} = \{a_n + b_n\}$, $\{a_n\} \times \{b_n\} = \{a_n b_n\}$ and $\mathrm{id} = \{1\}$. Define $||\,|| : \mathcal{K} \to \mathbb{R}_{>0}$ by $\{a_n\} \to \lim_{n\to\infty} |a_n|$ ($\mathbb{R}$ is complete). Let $\mathcal{N} \subset \mathcal{K}$ be the subset of all null sequences ($||a_n|| = 0$). Then $\mathcal{N}$ is a maximal ideal (Exercise). Hence $\mathcal{K}/\mathcal{N}$ is a field $\widehat{K}$. We have $||\,||$ (not an absolute value since $||a_n|| = 0$ for non zero elements) only depends on $\mathcal{K}/\mathcal{N}$. We get a well defined functions $||\,|| : \widehat{K} \to \mathbb{R}_{>0}$. This is an absolute value. Define $\iota : K \to \widehat{K}$ by $a \mapsto \{a\} \mod \mathcal{N}$. Then $\iota(K)$ is dense and $(\widehat{K}, ||\,||)$ is complete.

Uniqueness Suppose $(\widehat{K'}, ||\,||')$ is complete and is a completion, $\iota' : K \to \widehat{K}'$ satisfy the embedding properties above.

Claim. ι' extends uniquely to an embedding $\lambda : \widehat{K} \to \widehat{K}'$ such that

$$\begin{tikzcd}
K \arrow[r, "\iota'"] \arrow[dr, "\iota"'] & \widehat{K}' \\
 & \widehat{K} \arrow[u, "\lambda"']
\end{tikzcd}$$

Let $x \in \widehat{K}$ and $\{x_n\}$ is a sequence in K such that $\{\iota(x_n)\}$ converges to x (dense). Define $\lambda(x) = \lim_{n\to\infty}\{\iota'(x_n)\}$. Construct $\lambda' : \widehat{K}' \to \widehat{K}$ in the same way

□

Corollary 1.15. *Let K be a field and $|\,|_j$ $(j \leq J)$ be non-trivial and inequivalent absolute values on K. Let $\widehat{K}_j$ be the respective completions, let $\Delta : K \hookrightarrow \prod_j \widehat{K}_j$ defined by $x \mapsto (\iota_j(x))$. Then $\Delta(K)$ is dense, i.e., its closure $\overline{\Delta(K)}$ is $\prod_j K_j$.*

Remark. We have $\mathbb{Q} \hookrightarrow \mathbb{R}$ but $\mathbb{Q} \hookrightarrow \mathbb{R} \times \mathbb{R}$ is not dense.

Proof. Let $\alpha_j \in \widehat{K}_j$, for $1 \leq j \leq J$, then $\forall \epsilon > 0$ there exists $a_j \in K$ such that $|a_j - \alpha_j| < \epsilon$ for $1 \leq j \leq J$. By Theorem 1.12 there exists $b \in K$ such that $|b - a_j|_j < \epsilon$. Then $|b - \alpha_j|_j < 2\epsilon$ so arbitrary closed to α_j, hence dense.

$\square$

2 The p-adic

Theorem 2.1 (Ostrowski). *Every non trivial absolute value on $\mathbb{Q}$ is equivalent to $||_v$ where $v = p$ a prime or $v = \infty$.*

Proof. Let $||$ be an absolute value on $\mathbb{Q}$ and $a > 1$, $b > 0$ be integers. Let $t = \max\{|0|, |1|, \dots, |a-1|\}$, $b = b_m a^m + \cdots + b_1 a + b_0$ with $b_i \in \{0, \dots, a-1\}$, $b_m \neq 0$ and $m \leq \frac{\log b}{\log a}$. Then $|b| \leq \sum_{j=0}^{m} \left|b_j a^j\right| \leq (m+1)t\max\{1, |a|^m\} \leq (\log b/\log a + 1)t\max\{1, |a|^m\}$. Replace b by b^n and take nth root,

$$|b| \leq \underbrace{\left(n\frac{\log b}{\log a} + 1\right)^{1/n} t^{1/n}}_{\underset{n\to\infty}{\to} 1} \max\{1, |a|\}^{\log b/\log a}$$

Take the limit as $n \to \infty$, then $|b| \leq \max\{1, |a|\}^{\log b/\log a}$ $(*)$. We have two cases

1. $||$ is archimedean, then there exists $|b| > 1$ for some b by Lemma 1.3. So apply $(*)$, then $|a| > 1$ for all $a > 1$, so $|b| \leq |a|^{\log b/\log b}$. Reversing a and b we get $|a| \leq |b|^{\log a/\log b}$. Hence $|a|^{1/\log a} = |b|^{\log b}$,so $\frac{\log|a|}{\log a} = \frac{\log|b|}{\log b} = \alpha > 0$, and it is independent of a and b. Hence $|a| = a^\alpha = |a|_\infty^\alpha$ for all $a \in \mathbb{N}$. But $|\pm 1| = 1$, hence $|a| = |a|_\infty^\alpha$ for all $a \in \mathbb{Z}$. Let $q = \frac{a}{b}$, hence true for all $q \in \mathbb{Q}$

2. $||$ is non-archimedean. Then there exists $a \in \mathbb{N}$ such that $|a| < 1$. Let b be the such least integer.

   Claim. $b = p$ a prime number

   We prove this by contradiction. Suppose b is not a prime, $b = uv$. Now $|uv| < 1$, but as b is the least such number, we have $|u| = |v| = 1$, hence $|b| = 1$ a contradiction.

   So b is a prime, let $b = p$.

   Claim. $p|a$ if and only if $|a| < 1$.

   $\Rightarrow$: Let $a = up$, then $|a| = |u||p|$, hence $|u| < 1$ and $|p| < 1$.

   $\Leftarrow$: Suppose that if $p \nmid a$ then $a = up + r$ where $r < p$. By minimality of p, $|r| = 1$, $|up| < 1$, hence $|a| = \max\{|up|, |r|\} = 1$

   So let $\alpha == \frac{\log|p|}{\log p}$, $|p| = |p|_p^\alpha$. For all $a \in \mathbb{Z}$ we have $a = p^r a'$ where $p \nmid a'$, hence $|a'| = |a'|_p = 1$. Therefore, $|a| = |p^r a'| = |p|_p^{r\alpha} = |a|_p^\alpha$. And $|q| = |q|_p^\alpha$ for all $q \in \mathbb{Q}$

$\square$

Definition 2.2.

1. The *field of p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $||_p$. $(\mathbb{Q}_p, ||)$ is a non archimedean complete field.

2. The *ring of p-adic integers* $\mathbb{Z}_p$ is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x|_p \leq 1\} = \overline{B}(0,1)$ (check it is a ring, by using non archimedean properties)

Lemma 2.3. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$*

Proof. $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, $\mathbb{Z}_p$ is open in $\mathbb{Q}_p$ so $\mathbb{Q} \cap \mathbb{Z}_p$ is dense in $\mathbb{Z}_p$. Now $\mathbb{Q} \cap \mathbb{Z}_p = \left\{\frac{a}{b} \in \mathbb{Q} | p \nmid b\right\}$. Let $\frac{a}{b} \in \mathbb{Q}$ be such that $p \nmid b$ for $n \geq 1$ pick $y_n \in \mathbb{Z}$ such that $by_n \equiv 1 \mod p^n$ (b is a unit in $\mathbb{Z}_p$). Then $by_n \to 1$ as $n \to \infty$. Hence $\mathbb{Z}$ is dense in $\mathbb{Q} \cap \mathbb{Z}_p$, hence dense in $\mathbb{Z}_p$ □

What do elements of $\mathbb{Q}_p$ look like?

Let $x \in \mathbb{Z}_p$, let $n \in \mathbb{N}$, then by density there exists $q = \frac{a}{b} \in \mathbb{Q}$ such that $\left|x - \frac{a}{b}\right|_p \leq p^{-n}$. But then $\left|\frac{a}{b}\right|_p \leq \max\{|x|_p, \left|x - \frac{a}{b}\right|_p\}$. Hence $p \nmid b$ and there exists $b' \in \mathbb{Z}$ such that $bb' \equiv 1 \mod p^n$. But then $\left|\frac{a}{b} - ab'\right|_p = \left|\frac{a}{b}(1 - bb')\right|_p \leq p^{-n}$. Hence $|x - ab'|_p \leq \max\left\{\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - ab'\right|_p\right\} \leq p^{-n}$. Now let $\alpha \in \{0, \ldots, p^n - 1\}$ be the unique integer such that $ab' \equiv \alpha \mod p^n$.

Conclusion: $\forall x \in \mathbb{Z}_p, \forall n \in \mathbb{N}, \exists \alpha \in \{0, \ldots, p^n - 1\}$ such that $x \equiv \alpha \mod p^n$

Lemma 2.4. *For all $n \in \mathbb{N}$ there exists an exact sequence of rings* $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\phi_n} \mathbb{Z}/(p^n\mathbb{Z}) \to 0$

Proof. Note that $\ker p^n = \{z \in \mathbb{Z}_p | p^n z = 0\} = \{0\}$ (take absolute value on both side). We have that ϕ_n is surjective since $\{0, \ldots, p^n - 1\} \subset \mathbb{Z}_p$.

We show that $\operatorname{im}(p^n) = \ker(\phi_n)$. Suppose that $x \in \operatorname{im}(p^n)$, then $x = p^n y$ for some $y \in \mathbb{Z}_p$, then $|p^n y - 0|_p \leq p^{-n}$. Thence $\phi_n(x) = 0$ and $x \in \ker \phi_n$.

Conversely, let $x \in \ker(\phi_n)$. Then $|x|_p = |x - 0|_p \leq p^{-n}$, hence $|p^{-n}x| \leq 1$ so $x = p^n \underbrace{p^{-n}x}_{\in \mathbb{Z}_p} \in \operatorname{im}(p^n)$ □

Hence $\mathbb{Z}_p/(p^n\mathbb{Z}_p) \cong \mathbb{Z}/(p^n\mathbb{Z})$. We will see in a more general context that elements of $\mathbb{Q}_p$ can be uniquely written as a Laurent series expansion in p. Later we will consider the extensions of $\mathbb{Q}_p$.

In a Global setting: $[k : \mathbb{Q}] < \infty$, $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in k. In a local setting: $[k : \mathbb{Q}_p] < \infty$, $\mathcal{O}_k$ is the integral closure of $\mathbb{Z}_p$ in k. But in the global setting $\mathcal{O}_k$ is not necessarily a Unique Factorisation Domain while in a local setting it always is.

3 Non-archimedean Local Fields

We will examine a general theory of fields which are complete with respect to a non archimedean absolute value.

Theorem 3.1 (Ostrowski). *Let K be a field complete with respect to a archimedean absolute value. Then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$ and the absolute value are equivalent to the usual absolute value.*

Proof. See Chapter 3 of Cassels *Local Fields* $\square$

Basics Let K be a field with a non-trivial non-archimedean absolute value $|\,|$.

- $\mathcal{O}_K = \{x \in K |\, |x| \leq 1\}$, the *ring of integers* of K
- $\mathcal{P}_K = \{x \in K |\, |x| < 1\}$

Check that $\mathcal{O}_K$ is an integral domain and that $\mathcal{P}_K$ is maximal. (If $J \supsetneq \mathcal{P}_K$ is an ideal of $\mathcal{O}_K$ then there exists $x \in J$ such that $|x| = 1$. Then $|x^{-1}| = 1$ and $|1 = xx^{-1}| \in J$)

- $\mathcal{U}_K = \{x \in K |\, |x| = 1\}$, the *group of units* in K
- $k_K = \mathcal{O}_K / \mathcal{P}_K$, the *residue field* of K

The characteristic of k_K is the residual characteristic.

Note. In general $\mathrm{char} k_K \neq \mathrm{char} K$.

- $\Gamma_K = \{|x| \,| x \in K^*\}$, the *value group* of $|\,|$ on K.

This is a multiplicative subgroup of $\mathbb{R}_{>0}$.

Definition 3.2. A non-archimedean absolute value is *discrete* if Γ_K is discrete. (i.e., $\Gamma_K \cong \mathbb{Z}$)

Lemma 3.3. *A non-archimedean absolute value is discrete if and only if the maximal ideal is principal.*

Proof. By problem A.6 Γ_K is discrete if and only if Γ_K is cyclic.

$\Leftarrow$: Suppose that $\mathcal{P}_K$ is principal, say $\langle \pi \rangle$. Let $\gamma = |\pi| < 1$. Hence for all $x \in \mathcal{P}_K$, we have $|x| \leq \gamma$ (since $x = \pi y$ with $y \in \mathcal{O}_K$). So for all $x \in K$, there exists $n \in \mathbb{Z}$ such that $\gamma^n \leq |x| < \gamma^{n-1}$. Dividing through by γ^{n-1} we get that $\gamma \leq \left|x\pi^{1-n}\right| < 1$, whence $x\pi^{1-n} \in \mathcal{P}_K$. So $\gamma \leq \left|x\pi^{1-n}\right| \leq \gamma$, thus $\left|x\pi^{1-n}\right| = \gamma$. So $|x| = \gamma^n$, hence Γ_K is cyclic generated by γ.

$\Rightarrow$: Suppose that Γ_K is cyclic with generator $\gamma < 1$ say. Let $\pi \in K$ be such that $|\pi| = \gamma$. Clearly $\langle \pi \rangle \subset \mathcal{P}_K$. Conversely, for $x \in \mathcal{P}_K$, then $|x| = \gamma^n$ for some $n \geq 1$ since Γ_K is cyclic. So $|x\pi^{-1}| = \gamma^{n-1} \leq 1$, i.e. $x\pi^{-1} \in \mathcal{O}_K$ and $x \in \langle \pi \rangle$

$\square$

From now on $|\,|$ is a discrete non-archimedean absolute value on a field K. So by the previous lemma $\mathcal{P}_K = \langle \pi \rangle$ .We call π the *uniformiser* for the absolute value. Any $x \in K^*$ can be written as

$$x = \pi^n \epsilon$$

with $n \in \mathbb{Z}$ and $\epsilon \in \mathcal{U}_K$. We write $V_K(x) = n \in \mathbb{Z}$ for the *order* of x. This gives a valuation $V_K : K \to \mathbb{Z} \cup \{\infty\}$ by setting $V_K(0) = \infty$.

Lemma 3.4. *Let $0 \neq I \subset \mathcal{O}_K$ be an integral ideal. Then $I = \mathcal{P}_K^n := \{x_1 \dots x_n | x_i \in \mathcal{P}_K\}$ for some $n \in \mathbb{N}$.*

Proof. The subset $\{|x| \, | x \in I\} \subset \Gamma_K$ is bounded and so it attains its maximal at $x_0 = \pi^n \epsilon$,say (Γ_K is discrete). Then $I = \langle x_0 \rangle = \mathcal{P}_K^n$ $\square$

This implies that $\mathcal{P}_K$ is the unique non-zero prime ideal in $\mathcal{O}_K$. Furthermore, $\mathcal{O}_K$ is a PID and a local ring (with a unique maximal ideal)

Let $\overline{K}$ be the completion of K with respect to the absolute value $|\,|$. Let $\mathcal{O}_{\overline{K}}, \mathcal{P}_{\overline{K}}$ be the ring of integers and the maximal ideal of $\overline{K}$ respectively. then $\mathcal{O}_K = \mathcal{O}_{\overline{K}} \cap K$ and $\mathcal{P}_K = \mathcal{P}_{\overline{K}} \cap K$. There is an inclusion map $\mathcal{O}_K \hookrightarrow \mathcal{O}_{\overline{K}}$ and so a map $\mathcal{O}_K \to k_{\overline{K}} := \mathcal{O}_{\overline{K}} / \mathcal{P}_{\overline{K}}$ defined by $x \mapsto x + \mathcal{P}_{\overline{K}}$. The kernel of this map is $\mathcal{P}_K$, so it induces a natural map $k_K \xrightarrow{\sim} k_{\overline{K}}$.

Claim. This map is an isomorphism. It suffices to show that it is surjective

Proof. Let $\overline{x} \in \mathcal{O}_{\overline{K}}$. By density of K in $\overline{K}$, there exists $x \in K$ such that $|x - \overline{x}| < 1$. Then $x - \overline{x} \in \mathcal{P}_{\overline{K}}$ and $|x| \leq \max \left\{ \underbrace{|x - \overline{x}|}_{<1}, \underbrace{|\overline{x}|}_{\leq 1} \right\} \leq 1$. Thus $x \in K \cap \mathcal{O}_{\overline{K}} = \mathcal{O}_K$ $\square$

Definition 3.5. A *non-archimedean local field* is a field which is complete with respect to a non-trivial discrete non-archimedean absolute value such that the residue class k_K is finite.

Example.

K	$\mathbb{Q}_p$	$\mathbb{F}_q((T))$
Completion of	$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathcal{O}_K$	$\mathbb{Z}_p$	$\mathbb{F}_q[[T]]$
$\mathcal{P}_K$	$p\mathbb{Z}_p$	(T)
k_K	$\cong \mathbb{F}_p$	$\mathbb{F}_q$

From now on, K is a non-archimedean local field.

Say that an infinite sum $\sum_{n=0}^{\infty} x_n$, $x_n \in K$, converges to s if $s = \lim_{N \to \infty} \sum_{n=0}^{N} x_n$

Lemma 3.6. *$\sum_{n=0}^{\infty} x_n$ converges if and only if $x_n \to \infty$ as $n \to \infty$*

Proof. Exercise $\square$

Lemma 3.7. *Let π be a uniformiser of K and let $\mathcal{A} \subset \mathcal{O}_K$ be set of representative of $\mathcal{O}_K / \mathcal{P}_K$. Then $\mathcal{O}_K = \{\sum_{n=0}^{\infty} x_n \pi^n : x_n \in \mathcal{A}\}$*

Proof. By Lemma 3.6 we have $\sum_{n=0}^{\infty}$ converges and lies in $\mathcal{O}_K$. Conversely, if $x \in \mathcal{O}_K$, then there exists a unique $x_0 \in \mathcal{A}$ such that $|x - x_0| < 1$. Hence $x = x_0 + \pi y_1$ for some $y_1 \in \mathcal{O}_K$. Continue inductively with y_1 etc $\square$

Suppose $x \in K^*$, Then $\pi^{-N} x \in \mathcal{O}_K$ for some $N \in \mathbb{Z}$. Apply Lemma 3.7 to get $K^* = \{\sum_{n=N}^{\infty} x_n \pi^n : x_n \in \mathcal{A}, N \in \mathbb{Z},$

Let us return topology. A subset $V \subset K$ is said to be *compact* if whenever we have a family U_λ $(\lambda \in \Lambda)$ of open sets of K such that $V \subset \cup_{\lambda \in \Lambda} U_\lambda$, then there exists a finite subset $\Lambda_0 \subset \Lambda$ such that $V \subset \cup_{\lambda \in \Lambda_0} U_\lambda$. We say that K *locally compact* if every point of K has a compact neighbourhood. (i.e., $\forall x \in K$ there exists $V_x \subset K$ which is compact and contains $B(x, r)$ for some $r > 0$)

Lemma 3.8. *Let K be a non-archimedean local field. Then $\mathcal{O}_K$ is compact, and hence K is locally compact.*

Proof. First we prove that $\mathcal{O}_K$ is compact. Let U_λ $(\lambda \in \Lambda)$ be open sets covering $\mathcal{O}_K$. Suppose that there does not exists a finite subcovering. Now $\mathcal{O}_K = \cup_{x\in\mathcal{A}}(x + \pi\mathcal{O}_K)$ where $\mathcal{A}$ is set of representation for (finite field) $\mathcal{O}_K/\mathcal{P}_K$. Then there exists $x_0 \in \mathcal{A}$ such that $x_0 + \pi\mathcal{O}_K$ is not covered by finitely many U_λ. Similarly there exists $x_1 \in \mathcal{A}$ such that $x_0 + x_1\pi + \pi^2\mathcal{O}_K$ is not finitely covered and so on. Let $\overline{x} = x_0 + x_1\pi + x_2\pi^2 + \cdots \in \mathcal{O}_K$. There exists $\lambda_0 \in \Lambda$ such that $\overline{x} \in U_{\lambda_0}$. Since U_{λ_0} is open it follows that $\overline{x} + \pi^n\mathcal{O}_K \in U_{\lambda_0}$ for some N, which is a contradiction.

Next we prove that K is locally compact. Put $V_x = \overline{B}(x, 1) = x + \mathcal{O}_K$. □

Remark. In fact: F locally compact with respect non-archimedean absolute value $\iff$ F non-archimedean local field.

3.1 Hensel's Lemma

Theorem 3.9. *Let K be a non-archimedean local field and $f \in \mathcal{O}_K[X]$. Suppose $x_0 \in \mathcal{O}_K$ satisfies $|f(x_0)| < |f'(x_0)|^2$. Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$, $|x - x_0| \leq \frac{|f(x_0)|}{|f'(x_0)|}$.*

Proof. Define $f_j \in \mathcal{O}_K[X]$ via

$$f(X+Y) = f(X) + f_1(X)Y + f_2(X)Y^2 + \dots \tag{3.1}$$

In particular $f_1(X) + f'(X)$. Defined $y_0 \in \mathcal{O}_K$ by $f(x_0) + y_0 f'(x_0) = 0$. Then

$$\begin{aligned}
|f(x_0 + y_0)| &\leq \max_{j\geq 2}\left|f_j(x_0)y_0^j\right| \quad \text{By (3.1)}\\
&\leq \max_{j\geq 2}\left|y_0^j\right|\\
&\leq |y_0|^2\\
&= \left|\frac{f(x_0)}{f'(x_0)}\right|^2\\
&< |f(x_0)|
\end{aligned}$$

Similarly $|f_1(x_0 + y_0) - f_1(x_0)| \leq |y_0| < |f_1(x_0)|$. Then $|f_1(x_0 + y_0)| = |f_1(x_0)|$. Put $x_1 = x_0 + y_0$. Then $|f(x_1)| \leq \frac{|f(x_0)|^2}{|f_1(x_0)|^2}$, $|f_1(x_1)| = |f_1(x_0)|$ and $|x_1 - x_0| = \frac{|f(x_0)|}{|f'(x_0)|}$. So repeat the process and obtain a sequence of $x_{n+1} = x_n + y_n$ such that $|f_1(x_n)| = |f_1(x_0)|$ and $|f(x_{n+1})| \leq \frac{|f(x_n)|^2}{|f_1(x_n)|^2} = \frac{|f(x_n)|^2}{|f_1(x_0)|^2}$. So $f(x_n) \to 0$ as $n \to \infty$. Finally $|x_{n+1} - x_n| = |y_n| = \frac{|f(x_n)|}{|f_1(x_n)|} \to 0$ as $n \to \infty$. So $\{x_n\}$ is Cauchy and it has a limit as required.

Now suppose that we have another solution $x + z$ with $z \neq 0$ and $|z| \leq \frac{|f(x_0)|}{|f_1(x_0)|} < |f_1(x_0)| = |f_1(x)|$. Then, putting $X = x$ and $Y = z$ in equation (3.1), we get $0 = f(x+z) - f(x) = xf_1(x) + z^2 f_2(x) + \dots$. But $|zf_1(x)| > \left|z^j\right| \geq \left|z^j f_j(x)\right|$ for all $j \geq 2$. Which gives a contradiction. □

Example.

1. Squares in $\mathbb{Q}_p$.

   - $p \neq 2$. Suppose that $y \in \mathbb{Z}_p^*$. If there exists $x_0 \in \mathbb{Z}_p$ such that $\left|x_0^2 - y\right| < 1$ then there exists $x \in \mathbb{Z}_p$ such that $x^2 = y$. (Take $f(X) = X^2 - y$, so $|f(x_0)| < 1$ but $|f'(x_0)| = |2x_0| = 1$).

Theorem. *Any $z \in \mathbb{Z}$ with $p \nmid z$, is a square in $\mathbb{Z}_p$* $\iff \left(\frac{z}{p}\right) = +1$

Claim. $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ has 4 elements represented by $1, c, p, cp$ where $c \in \{1, \dots, p-1\}$ is a quadratic non-residue.

Corollary. *It follows that $\mathbb{Q}_p$ has exactly 3 quadratic extensions.*

Proof of the claim. Suppose $x \in \mathbb{Q}_p^*$. We may assume $x = u$ or pu for $u \in \mathbb{Z}_p$ (on multiplying x by a power of $p^2 \in \mathbb{Q}^{*2}$). Let $\alpha \in \{1, \dots, p-1\}$ be such that $u \equiv \alpha \mod p\mathbb{Z}_p$ (i.e. $u = \alpha + v$ for some $v \in p\mathbb{Z}_p$). Then $u = \alpha(1 + \alpha^{-1}v)$ and $1 + \alpha^{-1}v \equiv 1 \mod p\mathbb{Z}_p$ which is a square. Thus we may assume $u = \alpha$. But $\left(\frac{u}{p}\right) = 1 \Rightarrow u \in \mathbb{Q}_p^{*2}$, otherwise uc is in $\mathbb{Q}_p^{*2}$. □

- $p = 2$. See exercise B.1

2. Since residue field $k_K$is finite, it follows that k_K^* is cyclic group of order $q - 1$ where $q = p^r$ for some prime p. Now show there exists an alternative set of representative for $k_K = \mathcal{O}_K/\mathcal{P}_K$, besides $\{0, \dots, q-1\}$.

   Note $p \cdot 1 \in \mathcal{O}_K$ and so $q - 1 \in \mathcal{O}_K^*$. For each $\alpha \in k_K^*$, let $x_0 \in \mathcal{O}_K^*$ such that $x_0 \equiv \alpha \mod p$ and consider $f(x) = x^{q-1} - 1$. Then $|f(x_0)| < 1$, $|f'(x_0)| = |q-1| \cdot |x_0|^{q-2} = 1$. Hence by Theorem (3.9), there exists a unique *Teichmuller representative* $\widehat{\alpha} \in \mathcal{O}_K^*$ of α such that $f(\widehat{\alpha}) = 0$ and $\widehat{\alpha} \equiv \alpha \mod p$. We can take $\{0\} \cup \{\widehat{\alpha} : \alpha \in k_K^*\}$ as a set of representative for k_K.

   Define *principal congruence subgroup* $\mathcal{U}_K^n = \{u \in \mathcal{U}_K = \mathcal{O}_K^* : u - 1 \in \mathcal{P}_K^n\} = 1 + \mathcal{P}_K^n$. Then $\mathcal{U}_K$ and $\mathcal{U}_K^n$ are open and closed and compact in K^* (with induced topology).

   We have isomorphism of topological groups:

   - $K^*/\mathcal{U}_K \to \mathbb{Z}$ defined by $x\mathcal{U}_K \mapsto V_K(x)$.
   - $\mathcal{U}_K/\mathcal{U}_K^1 \to k_K^*$ defined by $\xi^v \mathcal{U}_K^1 \mapsto g^v$ where ξ is a primitive $(q-1)$th root of unity in K and g is a generator for k_K^*.

   Hence any $x \in K^*$ can be uniquely written as $\pi^u \xi^v \epsilon$ for $\epsilon \in \mathcal{U}_K^1$, i.e., $K^* \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathcal{U}_K^1$.

4 Extensions of local fields

We consider field extensions of non-archimedean local fields. We would like to show that these extension are non-archimedean local fields.

4.1 Normed vector spaces

Let K be a non-archimedean local field

Definition 4.1. Let V be a vector space over K. A function $\| \ \| : V \to \mathbb{R}_{\geq 0}$ is a *norm* if

1. $\|x\| = 0$ if and only if $x = 0$
2. $\|x + y\| \leq \|x\| + \|y\|$
3. $\|\lambda x\| = |\lambda| \cdot \|x\|$ for all $\lambda \in K$

Note. The norm induces a metric $d(x, y) = \|x - y\|$ on V, which gives a topology.

Definition 4.2. Two norms $\| \ \|_1$ and $\| \ \|_2$ one a vector V are *equivalent* if $\exists c_1, c_2 > 0$ such that $c_1\|x\|_2 \leq \|x\|_1 \leq c_2\|x\|_2 \ \forall x \in V$

Exercise. Show that $\| \ \|_1, \| \ \|_2$ are equivalent if and only if they induce the same topology on V.

Lemma 4.3. *Let V be a finite dimensional vector space over K. Then any 2 norms on V are equivalent. Moreover, V is complete with respect to the induced metric.*

Proof. We proof by induction on $n = \dim_K V$

$n = 1$ Trivial

$n > 1$ Let $e_1, \ldots, e_n$ be a basis for V over K. Put $a = a_1e_1 + \cdots + a_ne_n$ $(a_j \in K)$ and define $\|a\|_0 := \max_j |a_j|$. Check that $\| \ \|_0$ is a norm and that V is complete with respect to it. It will suffice to show any norm $\| \ \|$ on V is equivalent to $\| \ \|_0$. Firstly $\|a\| \leq \sum_j |a_j| \cdot \|e_j\| \leq c_2\|a\|_0$ with $c_2 = \sum \|e_j\|$.

We now need to show $\exists c > 0$ such that $\|a\|_0 \leq c\|a\|$ for all $a \in V$ $\quad (*)$. If not, $\forall \epsilon > 0$, there exists $b = b_\epsilon \in V$ such that $\|b\| \leq \epsilon\|b\|_0$. Assume without loss of generality that $\|b\|_0 = |b_n|$. Replacing b by $b_n^{-1}b$ we have $b = c + e_n$ where $c \in \langle e_1, \ldots, e_{n-1}\rangle_K$.

Summary: $(*)$ false, implies we can find a sequence $c^{(m)} \in W = \langle e_1, \ldots, e_{n-1}\rangle_K$ such that $\|c^{(m)} + e_n\| \to 0$ as $m \to \infty$. But then $\|c^{(m)} - c^{(l)}\| \to 0$. So now use induction hypothesis. Since $\dim W = n-1$, it is complete under $\| \ \|$. Thus there exists $c^* \in W$ such that $\|c^{(m)} - c\| = 0$. Hence $\|c^* + e_n\| = \lim_{m\to\infty} \|c^{(m)} + e_n\| = 0$. Therefore $c^* + e_n = 0$, which is impossible. Hence $(*)$ hold and so $\| \ \|$ and $\| \ \|_0$ are equivalent.

$\square$

Corollary 4.4. *V finite dimensional normed vector space over K. Then V is locally compact. (i.e., $v \in V$ has a compact neighbourhood)*

Proof. By Lemma 4.3 we can assume $\| \ \|$ is $\| \ \|_0$, with respect to some fixed basis $e_1, \ldots, e_n$. Now imitate the proof of Lemma 3.8 to show that $\{v \in V : \|v\|_0 \leq 1\}$ is compact. $\square$

4.2 Extension of Absolute Values

Let K be a non-archimedean local field and $L \supset K$ an extension. We say that an absolute value $\| \ \|$ L *extends to the absolute value* $| \ |$ on K if $\|\lambda\| = |\lambda|$ for all $\lambda \in K$

Theorem 4.5. *Let $L \supset K$ be a finite extension. Then there exists a unique extension $\| \ \|$ of $| \ |$ to L. Moreover, L, $\| \ \|$ is a non-archimedean local field.*

Proof.

Uniqueness: Suppose $\| \ \|_1, \| \ \|_2$ extend $| \ |$ to L. Then, regarding L as a finite dimensional vector space over K, Lemma 4.3implies $\| \ \|_1$ and $\| \ \|_2$ are equivalent and some define the same topology on L. But then they are equivalent as absolute values and so by Lemma 1.10, there exists α such that $\|x\|_1 = \|x\|_2^\alpha \forall x \in L$. But the two absolute values are equal on K, so that $\alpha = 1$.

Second_part Apply 4.4 and converse of Lemma 3.8

Existence We will show that the extension of $\| \ \|$ of $| \ |$ to L is given by $\|x\| = |N_{L/K}(x)|^{1/n}$ for $x \in L$, where $n = [L : K]$. Here $N_{L/K} : L \to K$ is the norm map. (Recall: Thinking of L as a vector space over K, multiplication by $\alpha \in L$ gives a linear map $m_\alpha : K \to L$, with matrix $A_\alpha \in M_n(K)$. Put $N_{L/K}(\alpha) := \det A_\alpha$). For $x \in K$, $\|x\| = |x^n|^{1/n} = |x|$. So $\| \ \|$ does extend $| \ |$.

For $x \in L^*$, the linear map $m_x : L \to L$ is invertible with inverse $m_{x^{-1}}$. Thus the matrix A_x is invertible, and $\det A_x \neq 0$. Hence $\|x\| \neq 0$. Multiplicativity follows from the multiplicativity of the norm map.

Remains to prove the ultrametric inequality. Suffices to show $\|x\| \leq 1$, then $\|1+x\| \leq 1$. (Then, assuming $\|x\| \leq \|y\|$ then $\|x+y\| = \|y\| \cdot \|\frac{x}{y} + 1\| \leq \|y\|$). Suppose $\|x\| \leq 1$. Let $\chi(x)$ be the characteristic polynomial of the linear map $m_x : L \to L$. Let $f(X) = X^r + f_{r-1}X^{r-1} + \cdots + f_0$ be the minimal polynomial of x. Here r is the degree of x over K. Then $\chi(X) = f(X)^{n/r}$ (where n/r is the degree of L over $K(x)$, a proof of this can be found in Cassels book Lemma B.3). Then $|f_0^{\text{power}}| = |N_{L/K}(x)| \leq 1$, hence $|f_0| \leq 1$. Since f is irreducible and monic it follows from consideration of Newton polygon associated to it that $|f_i| \leq 1$ (See Cassels chapter 4). Hence $f \in \mathcal{O}_K[X]$ and also $\chi \in \mathcal{O}_K[X]$. Now $N_{L/K}(1+x) = \det(I_n + A_x) = (-1)^n \chi(-1)$. So $\|1+x\| = |\chi(-1)|^{1/n} \leq 1$. This completes the proof

□

Since the absolute value on L is unique, we will usually write it as $| \ |$ instead of $\| \ \|$.

Corollary 4.6. *$| \ |_p$ on $\mathbb{Q}_p$ extends uniquely to an absolute value on algebraic closure $\overline{\mathbb{Q}_p}$.*

Proof. $x \in \overline{\mathbb{Q}_p}$ then $x \in K$ for some finite extension $K/\mathbb{Q}_p$. Let $| \ | = | \ |_K$ where $| \ |$ is the unique absolute value on K extending $| \ |_p$. This is independent of choice of K by Theorem 4.5 □

4.3 Ramification

Suppose L/K is a finite extension of non-archimedean local fields of degree $n = [L : K]$.

Lemma 4.7. *There exists a natural injection $k_K \to k_L$ such that k_L is an extension of k_K of degree $f = f(L/K) := [k_L : k_K] \leq n$.*

Proof. There is certainly an inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$. But $\mathcal{P}_K = \mathcal{O}_K \cap \mathcal{P}_L$, this induces the injection $k_K \to k_L$.

Let $\alpha_1, \ldots, \alpha_{n+1} \in k_L$. Show that there are linearly dependent over k_K. Then we will have shown that $f = \dim_{k_K} k_L \leq n$. Let $\widehat{\alpha_1}, \ldots, \widehat{\alpha_{n+1}} \in \mathcal{O}_L$ such that $\alpha_i = \widehat{\alpha}_i + \mathcal{P}_L$ for $1 \leq i \leq n+1$. Since $\dim_K L = n$, there are linearly dependent over K, i.e., there exists $\lambda_i \in K$ not all zeroes such that $\sum_{i=1}^{n+1} \lambda_i \widehat{\alpha_i} = 0$. Without loss of generality, we assume that $\lambda_{n+1} \neq 0$. Let $\mu_i \in k_K$ be the reduction of $\lambda_i \lambda_{n+1}^{-1}$ modulo $\mathcal{P}_L$. Then $\sum_{i=1}^{n} \mu_i \alpha_i + \alpha_{n+1} = 0$, as required. $\square$

Definition 4.8. If $f = f(L/K) = n$, we say L/K is *unramified.*

If $f = f(L/K) = 1$, we say L/K is *totally ramified.*

If $f = f(L/K) < n$, we say L/K is *ramified.*

Remark. If $K \subset L \subset E$ is a tower of extensions then $f(E/K) = f(E/L) \cdot f(L/K)$.

We shall see that unramified extensions are easy to characterise.

Theorem 4.9. *Let $\alpha \in k_L = \mathcal{O}_L/\mathcal{P}_L$. Then there exists $\widehat{\alpha} \in \mathcal{O}_L$ such that $\widehat{\alpha} + \mathcal{P}_L = \alpha$ and $[K(\widehat{\alpha}) : K] = [k_K(\alpha) : k_K]$.*

Furthermore, the field $K(\widehat{\alpha})$ depends on α.

Remark. The extension $K(\widehat{\alpha})/K$ is unramified.

Proof. Let $\phi \in k_x[x]$ be the minimal polynomial of α. Let $\Phi \in K[X]$ be any *lift* of ϕ (i.e., $\deg \phi = \deg \Phi$ and $\phi = \overline{\Phi}$, meaning coefficients of Φ are reduced modulo $\mathcal{P}_K$). Let $\widehat{\alpha_0} \in \mathcal{O}_L$ be an element of the residue class of α. Then $\overline{\Phi}(\widehat{\alpha_0}) = \phi(\alpha) = 0$ and $\overline{\Phi}'(\widehat{\alpha}_0) = \phi'(\alpha) \neq 0$ (since k_K is a finite field so it is perfect). Thus $|\Phi(\widehat{\alpha_0})| < 1$ and $|\Phi'(\widehat{\alpha_0})| = 1$. Hence by Hensel's lemma, with $K(\widehat{\alpha}_0)$ as the ground field, implies there exists $\widehat{\alpha} \in K(\widehat{\alpha}_0) \subset L$ such that $\Phi(\widehat{\alpha}) = 0$, $|\widehat{\alpha} - \widehat{\alpha_0}| < 1$. Hence $\widehat{\alpha}$ in residue class of α and $[K(\widehat{\alpha}) : K] = [k_K(\alpha) : k_K]$ since Φ is irreducible.

Now suppose that $\widehat{\alpha}'$ is also in the residue class of α and satisfies $[K(\widehat{\alpha}') : K] = [k_K(\alpha) : k_K]$. Then the above argument implies $\widehat{\alpha} \in K(\widehat{\alpha}')$ and so $K(\widehat{\alpha}) = K(\widehat{\alpha}')$. But we must have equality since the degrees are the same. $\square$

Corollary 4.10. *There exists a bijection between intermediate fields E (with $K \subset E \subset L$) which are unramified and the fields k with $k_K \subset k \subset k_L$, given by $E \to k_E = E \cap \mathcal{O}_L / E \cap \mathcal{P}_L$*

Proof. The previous theorem gives one direction.

Let k be an intermediate field $k_K \subset k \subset k_L$. Let $q = \#k$. Then $k = k_K(\alpha)$ for some $(q-1)$th root of unity α. Then apply Theorem 4.9 $\square$

Corollary 4.11. *Let K be a non-archimedean local field. For all $n \in \mathbb{N}$ there exists a unique (up to isomorphism) unramified extension of degree n. It is the splitting field over K of $X^q - X$ where $q = q_K^n$, with $q_K = \#k_K$*

Proof. Let L/K be unramified extension of degree n. Then k_L has $q = q_K^n$ elements. Then L contains a full set of $(q-1)$th roots of unity (By example 2 after Hensel's lemma). In particular $X^q - X$ splits in L and so L contains its splitting field, say F. However $q_L = q_F = q$ and so by Corollary 4.10 we must have $F = L$ $\square$

Corollary 4.12. *Let $f \in \mathcal{O}_K[X]$ be monic of degree n and reduction $\overline{f} \mod \mathcal{P}_K$ is irreducible. Then*

1. *if $L = K(\alpha)$ and α has minimal polynomial f, then L/K is unramified*

2. The splitting field of f over K is unramified and has degree n.

Proof.

1. Note that $k_L \supset k_K(\overline{\alpha})$, where $\overline{\alpha}$ is the reduction of $\alpha \mod \mathcal{P}_L$. Moreover, $k_K(\overline{\alpha})$ has degree n over k_K. Hence $f(L/K) \geq n$. But we also have $f(L/K) \leq n = [L : K]$ by Lemma 4.7.

2. Let L be the splitting field of f over K and let α, β be roots of f in L. Then part 1. implies that $K(\alpha)$ and $K(\beta)$ are both unramified extensions of degree n. Then Corollary 4.10 implies they are equal, therefore $L = K(\alpha)$.

□

Summary. Unramified extensions of K are obtained by adjoining a root of unity of order coprime to residual characteristic of K.

Now let us look at ramified extensions.

Suppose L/K is a finite extension of non-archimedean local fields. Consider the relationship between value groups $\Gamma_L = \{|x| : x \in L^*\}$ is a discrete (cyclic) subgroup of $\mathbb{R}_{>0}$.

Definition 4.13. The *ramification index* of L/K is $e = e(L/K) = [\Gamma_L : \Gamma_K]$.

If π_L, π_K are uniformisers for L and K respectively. Recall $|\pi_K| < 1$ is a generator for Γ_K and similarly π_L for Γ_L. Then $|\pi_K| = |\pi_L|^e$. This implies $e(E/K) = e(E/L)e(L/K)$ for any tower $K \subset L \subset E$.

Theorem 4.14. *L/K be a finite extensions of non-archimedean local fields of degree n. Then $n = ef$.*

It follows from this that L/K is unramified if and only if $e(L/K) = 1$
L/K is totally ramified if and only if $e(L/K) = n$
It is ramified if and only if $e(L/K) > 1$

Proof. Let π_L be a uniformiser of L and let $\widehat{\alpha}_1, \ldots, \widehat{\alpha}_f$ be any lift to $\mathcal{O}_L$ of a basis for k_L/k_K. (As in Theorem 4.9) We will prove that $\mathcal{B} = \left\{\widehat{\alpha}_i \pi_L^j : 1 \leq i \leq f, 0 \leq j \leq e-1\right\}$ is a basis for L/K. (In fact we will prove that it is an $\mathcal{O}_K$ basis for $\mathcal{O}_L$.)

Firs suppose that $\mathcal{B}$ is not linearly independent over K. Then there exists $a_{ij} \in K$, not all zeroes, such that

$$\sum_{i,j} a_{ij} \widehat{\alpha}_i \pi_L^j = 0 \ \ (*)$$

Without loss of generality, assume that $\max_{i,j} |a_{ij}| = 1$. Hence, there exists integers, I, J such that $|a_{ij}| \leq |\pi_K|$ for $1 \leq i \leq f, j < J$, $|a_{IJ}| = 1$. If we reduce $\sum_i a_{iJ} \widehat{\alpha}_i$ module $\mathcal{P}_L$, then we get a non-zero coefficient $\overline{a}_{IJ}$. Since $\widehat{\alpha}_i \mod \mathcal{P}_L$ are linearly independent over k_K, this reduction is non-zero. Thus $|\sum_i a_{iJ} \widehat{\alpha}_i| = 1$. We now get

$$\left|\sum_i a_{ij} \widehat{\alpha}_i \pi_L^j\right| \begin{cases} \leq |\pi_K| = |\pi_L|^e & j < J \\ = |\pi_L|^J & j = J \\ \leq |\pi_L|^{J+1} & j > J \end{cases}$$

Recalling $J \leq e-1$, one term in $(*)$ has to be bigger than all the others. Contradiction

Now let $x \in L$. We claim that x is in the K-span of $\mathcal{B}$. Multiplying by a suitable power of π_K, we reduce to the case $x \in \mathcal{O}_L$. (If $\pi_K^n x = \sum_{ij} a_{ij} \widehat{\alpha}_i \pi_L^j$ with $a_{ij} \in K$, then putting $b_{ij} = \pi_k^{-n} a_{ij}$ gives $x = \sum b_{ij} \widehat{\alpha}_i \pi_L^j$).

Since $\alpha_i \equiv \widehat{\alpha}_i \mod \mathcal{P}_L$ form a basis for k_L/k_K, there exists $c_{i0} \in k_K$ such that $\overline{x} = \sum_i c_{i0}\alpha_i$. Choose any lifts $\widehat{c_{i0}} \in \mathcal{O}_K$, we have $x - \sum_i \widehat{c}_{i0}\widehat{\alpha}_i = \pi_L x_1 \in \mathcal{P}_L$ for some $x_1 \in \mathcal{O}_L$. Now repeat process on x_1, and so on, until we have obtained $\widehat{c}_{ij} \in \mathcal{O}_K$ such that

$$x - \sum_{j=0}^{e-1}\sum_i \widehat{c}_{ij}\widehat{\alpha}_i\pi_L^j = \pi_L^e x_e$$

for some $x_e \in \mathcal{O}_L$. Now $|\pi_L|^e = |\pi_K|$ and so $\pi_L^e x_e = \pi_K x^{(1)}$ for some $x^{(1)} \in \mathcal{O}_L$. Now we start again with $x^{(1)}$ instead of x. Carrying on in this way, we find a succession of linear combinations

$$c_r = \sum_{j=0}^{e-1}\sum_i \widehat{c}_{ij}^{(r)}\widehat{\alpha}_i\pi_L^j$$

of elements of $\mathcal{B}$ with coefficients in $\mathcal{O}_K$ such that $x - c_0 - c_1\pi_K - \cdots - c_s\pi_K^s \in \pi_K^{s+1}\mathcal{O}_L$, $\forall s \geq 0$. Now let $s \to \infty$ and, using completeness, put

$$a_{ij} = \sum_{r=0}^{\infty} \widehat{c}_{ij}^{(r)}\pi_K^r$$

Then $x = \sum_{i,j} a_{ij}\widehat{\alpha}_i\pi_L^j$ as required. $\square$

A polynomial $f(X) = f_nX^n + f_{n-1}X^{n-1} + \cdots + f_0 \in \mathcal{O}_K[X]$ is said to be *Eisenstein* if

$$|f_n| = 1, |f_j| < 1\,\forall 0 \leq j < n, |f_0| = |\pi_K| \quad (\dagger)$$

Aside on irreducibility: Let $f = f_0 + f_1X + \cdots + f_nX^n \in K[X]$ with $f_0 \neq 0, f_n \neq 0$. The *Newton polygon* of f is the convex hull in $\mathbb{R}^2$ of the points $p(j) = (j, \log|f_j|)$ for $f_j \neq 0$. It consist of line segments σ_s for $1 \leq s \leq r$, where σ_s joins $P(m_{s-1})$ to $P(m_s)$ and $0 = m_0 < m_1 < \cdots < m_r = n$. The slope of σ_s is $\gamma_s = \left(\log|f_{m_s}| - \log\left|f_{m_{s-1}}\right|\right)/(m_s - m_{s-1})$. We say f is of type $(l_1, \gamma_1, \ldots, l_r, \gamma_r)$ where $l_s = m_s - m_{s-1}$. If $r = 1$ then f is said to be pure.

Fact. (Cassels Local Field pg 100): *f of type $(l_1, \gamma_1, \ldots, l_r, \gamma_r)$ then $f(X) = g_1(X)\ldots g_r(X)$ where g_s is pure of type (l_s, γ_s).*

Totally ramified extensions are quite easy to classify.

Theorem 4.15. *Let L/K be a finite extension of non-archimedean local fields. Then L/K is totally ramified if and only if $L = K(\beta)$, where β is the root of an Eisenstein polynomial.*

Proof.

$\Rightarrow$ L/K totally ramified of degree n, let $\beta = \pi_L$ be a uniformiser for L. Then $1, \pi_L, \ldots, \pi_L^{n-1}$ are linearly independent over K (as in the proof of Theorem 4.14). Hence there exists an equation $\beta^n + f_{n-1}\beta^{n-1} + \cdots + f_0 = 0$ with $f_j \in K$. Two of the summands must have the same absolute value and this must be the first and the last. (Suppose $|f_k\beta^k| = |f_l\beta^l|$ for some $n \geq k > l \geq 0$, then there exists $a_k, a_l \in \mathbb{Z}$ such that $\left|\pi_L^{k-l}\right| = |\beta|^{k-l} = |\pi_K|^{a_k - a_l} = |\pi_L|^{n(a_k - a_l)}$, hence $l = 0$ and $k = n$). Therefore $|f_0| = |\pi_L|^n = |\pi_K|$ and $|f_j| < 1$ for all j. Hence a polynomial in the equation is Eisenstein.

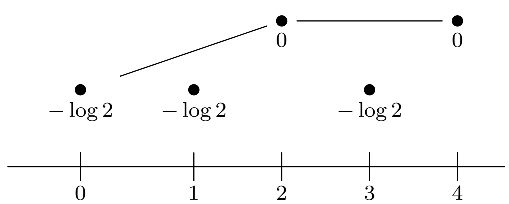
$\Leftarrow$ Suppose $f_n\beta^n + \cdots + f_0 = 0$, where $f_j \in K$ such that $|f_n| = 1$, $|f_j| < 1$ and $|f_0| = |\pi_K|$.Then $|\beta^n| < 1$ and so $|\beta| < 1$. Hence the last term in the sum is bigger than all the others. except possibly for the first. Since the sum is zero, they must be equal (in absolute value) and so $|\beta|^n = |f_0| = |\pi_K|$. Hence $\beta = \pi_L^g y$ for some unit y, then $|\pi_L|^{gn} = |\pi_K|$, whence $e(L/K) = gn \geq n$. But we must have equality by Theorem 4.14, since $n = [L : K]$. Hence L/K is totally ramified.

$\square$

Example. Let $f(X) = X^4 - 2X^3 + 17X^2 + 22X + 66$. We are going to look at the splitting field E over $\mathbb{Q}_p$ for various prime p. In each case, we want to calculate:

- The degree $[E : \mathbb{Q}_p]$?
- Residue class degree $f(E/\mathbb{Q}_p)$?
- Ramification index $e(E/\mathbb{Q}_p)$?
- (If possible) maximal unramified subextension L? i.e., $E \supset L \supset \mathbb{Q}_p$ with $L/\mathbb{Q}_p$ unramified and hence E/L totally ramified.

$p = 2$ Newton polygon. Note $\log |2^a b|_2 = \log 2^{-1}$



$l_1 = 2 - 0 = 2$, $\gamma_1 = \log 2/2$, $l_2 = 4 - 2 = 2$, $\gamma_2 = 0$. So the type is $(2, \frac{1}{2}\log 2, 2, 0)$ and factorises as a product of 2 quadratic. Trial an error over $\mathbb{Z}$ gives $f(X) = \underbrace{(X^2 - 2X + 6)}_{:=g(X)} \cdot \underbrace{(X^2 - 11)}_{:=h(X)}$ and g, h irreducible over $\mathbb{Q}_2$ (Eisenstein criterion for g and $11 \not\equiv 1 \mod 8$ so apply Exercise B.1). Let αbe a root of g and β a root of h in E. Then by Theorem 4.15, we have that $\mathbb{Q}_2(\alpha)/\mathbb{Q}_2$ is totally ramified. Since $\beta - 1$ satisfies $0 = h(X + 1) = X^2 + 2X - 10$ which is Eisenstein, we also have $\mathbb{Q}_2(\beta)/\mathbb{Q}_2$ is totally ramified. Note that $[\mathbb{Q}_2(\alpha) : \mathbb{Q}_2] = [\mathbb{Q}_2(\beta) : \mathbb{Q}_2] = 2$.

Next $\gamma = \alpha - 1$ satisfies $0 = g(X + 1) = X^2 - 7$, so $\gamma^2 = 7$. Let $\delta = \beta\gamma$, then $\delta^2 = 7 \cdot 11$. We claim that $\mathbb{Q}_2(\delta)/\mathbb{Q}_2$ is unramified of degree 2. Then $[E : \mathbb{Q}_2] = 4$, $e(E/\mathbb{Q}_2) = f(E/\mathbb{Q}_2) = 2$ and $L = \mathbb{Q}_2(\delta)$. To show that $\mathbb{Q}_2(\delta)/\mathbb{Q}_2$ is unramified, we need to show (by Corollary 4.11) that $\mathbb{Q}_2(\delta)$ is obtained from $\mathbb{Q}_2$ by adjoining a root of $X^2 + X + 1$ (i.e., a primitive $(2^2 - 1)$th root of unity). Do this by applying Hensel to $(\delta - 1)/2$.

p odd Use the fact that $E = \mathbb{Q}_p(\gamma, \beta)$ where γ and β are as above ($\gamma^2 = 7$, $\beta^2 = 11$)

$p = 3$ Since $\left(\frac{7}{3}\right) = 1$, then $\gamma \in \mathbb{Q}_3$, while $\left(\frac{11}{3}\right) = -1$, so $X^2 - 11$ is irreducible in $\mathbb{F}_3[X]$. Hence it follows that $E = \mathbb{Q}_3(\beta)$ and it is unramified of degree 2 over $\mathbb{Q}_3$ (by Corollary 4.12)

$p = 19$ Since $\left(\frac{7}{19}\right) = \left(\frac{11}{19}\right) = 1$ so $E = \mathbb{Q}_{19}$

(all primes behave like $3, 5, 11, 13$ or 19)

5 Algebraic Closure

Recall that a field K is called *algebraically closed* if every polynomial with coefficients in K has a root in K.

Definition 5.1. An extension $\overline{K} \supset K$ is the *algebraic closure* of K if

1. $\overline{K}$ is algebraically closes
2. Any $\alpha \in \overline{K}$ is algebraic over K.

For example, $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, $[\mathbb{C} : \mathbb{R}] = 2$. If $\overline{\mathbb{Q}_p}$ is the closure of $\mathbb{Q}_p$ then $[\overline{\mathbb{Q}_p} : \mathbb{Q}_p] = \infty$. (Note $\overline{\mathbb{Q}_p}$ must contain roots of $X^n - p$ for all $n \in \mathbb{N}$)

Theorem 5.2. *Let K be a field. Then there exists an algebraic closure $\overline{K}$ of K and it is unique up to isomorphism.*

Proof. (Sketch) Let Λ be the set of all irreducible polynomials over K of degree ≥ 2. Let $\Xi = \{X_f : f \in \Lambda\}$ be a family of indeterminate indexed by Λ. Put $R = K[\Xi]$. Consider the ideal $I = \{f(X_f) : f \in \Lambda\}$. This is a proper ideal: if not we would have an equation $1 = u_1 f_1(X_{f_1}) + \cdots + u_n f_n(X_{f_n})$ for some $u_j \in R$. Let E/K formed by adjoining roots $\alpha_1, \ldots, \alpha_n$ of $f_1, \ldots, f_n$ respectively. Then we deduce that $1 = 0$ a contradiction.

Since I is proper, it is contained in a maximal ideal m of R. Then $\overline{K} = R/m$ is a field and the homomorphism $K \to K[\Xi] \twoheadrightarrow \overline{K}$ is an embedding of $K \to \overline{K}$. We claim $\overline{K}$ is an algebraic closure of K. If f is an irreducible polynomial in $K[X]$, then $\alpha = X_f + m$ is an root of f in $\overline{K}$ (since $f(X_f) \in I \subset m$). Moreover, each $X_f + m$ is algebraic over $\overline{K}$ and $\overline{K}$ is generated by them.

Uniqueness: Essentially follows form uniqueness of splitting fields of polynomials over K. ☐

From now on K is a non-archimedean local field with algebraic closure $\overline{K}$. Recall that the absolute value on K extends uniquely to $\overline{K}$. ($\forall \alpha \in \overline{K}$,there exists $K \subset L \subset \overline{K}$ such that $L = K(\alpha)$, then $|\alpha| = \left|N_{L/K}(\alpha)\right|^{1/[L:K]}$).

We want to know if it is possible for $\overline{K}$ to be a non-archimedean local field:

$\Gamma_{\overline{K}}$ Let us ask is the value group $\Gamma_{\overline{K}}$ is discrete? Suppose $\Gamma_K = \{|x| : x \in K\}$ is generated by $g < 1$. Suppose $r \in \Gamma_{\overline{K}}$. Then $r = |\alpha|$ for some $\alpha \in \overline{K}$. Let L/K of degree n such that $\alpha \in L$. Then $|\alpha| = g^{m/n}$ for some $m \in \mathbb{Z}$. Hence $\Gamma_{\overline{K}} \subset \left\{g^{m/n} : \frac{m}{n} \in \mathbb{Q}\right\}$. In fact we have equality. Let $L \subset \overline{K}$ be an extension obtained by adjoining a root α of the Eisenstein polynomial $X^n - \pi_K X - \pi_K$. Then α is the uniformiser for L and L/K is totally ramified of degree n. Hence $|\alpha| = g^{1/n}$ and so $|\alpha^m| = g^{m/n}$. This shows that $\Gamma_{\overline{K}}$ is <u>not</u> discrete.

$k_{\overline{K}}$ Consider the residue field $k_{\overline{K}}$. Let $\alpha \in k_{\overline{K}} = \mathcal{O}_{\overline{K}}/\mathcal{P}_{\overline{K}}$ and let $\widehat{\alpha}$ be a lift of α to $\mathcal{O}_{\overline{K}}$. Then $\widehat{\alpha} \in \overline{K}$ and so there exists a minimal polynomial $\Phi \in \mathcal{O}_K[X]$ of $\widehat{\alpha}$ over K. Let $\phi \in k_K[X]$ denote the reduction modulo $\mathcal{P}_K$ of Φ. Then it follows $\phi(\alpha) = 0$ and so α is algebraic over k_K. Thus $k_{\overline{k}} \subset \overline{k_K}$. In fact we have equality here. Suppose $\phi \in k_K[X]$ is irreducible and let Φ be a lift of ϕ. Then Φ has a root $\alpha \in \mathcal{O}_{\overline{K}}$ (since $\overline{K}$ is algebraic closed). Then $\overline{\alpha} = \alpha + \mathcal{P}_{\overline{K}}$ is a root of ϕ in $k_{\overline{K}}$. Hence $k_{\overline{K}} = \overline{k_K}$.

Suppose L/K is Galois.

Exercise. If $|\ |$ is an absolute value on L which extends the absolute value on K, then so $\|x\| = |\sigma(x)|$ for all $\sigma \in \mathrm{Gal}(L/K)$. By uniqueness, we have $|x| = |\sigma(x)|$ for all $x \in L \forall \sigma \in \mathrm{Gal}(L/K)$.

Theorem 5.3 (Krasner's Lemma). *K field of characteristic 0, which is complete with respect to a non-archimedean absolute value $|\ |$. Let $a, b \in \overline{K}$ and suppose that $|b-a| < |a-a_i|$for all $2 \leq i \leq n$ where $a_1 = a, a_2, \ldots, a_n$ are roots of the minimal polynomial of a in $K[X]$. Then $K(a) \subset K(b)$.*

Proof. Put $L = K(b)$. Suppose for contradiction that $a \notin L$. Let $f \in L[X]$ be minimal polynomial of a over L. Let E be the splitting field f over L. Then E/L is Galois and since $a \notin L$, there exists $\sigma \in \mathrm{Gal}(E/L)$ which does not fix a. Then $\sigma(a) = a_i$ for some $i > 1$. $|a - a_i| \leq \max\{|a-b|, \underbrace{|b-a_i|}_{=|\sigma(b-a)|=|b-a|}\} = |a-b|$, which is a contradiction. ☐

Incompleteness

$K = \mathbb{Q}_p$

Theorem 5.4. *$\overline{\mathbb{Q}}_p$ is not complete with respect to $|\ |_p$*

Proof. We need to find a Cauchy sequence $\{\alpha_n\}$ in $\overline{\mathbb{Q}}_p$ which does not converge. For $i \geq 0$, let ζ_i be a root of unity of order $p^{(i+1)!} - 1$. Put $F_i = \mathbb{Q}_p(\zeta_i)$, then

- F_i is the splitting field of $X^{p^{(1+i)!}} - X$ over $\mathbb{Q}_p$. Thus it is an unramified extension of $\mathbb{Q}_p$ of degree $(i+1)!$ and it is Galois (Corollary 4.11)
- $\zeta_{i-1} \subset F_i$ since $[F_i : F_{i-1}] = i+1$ and moreover $p^{i!} - 1 | p^{(i+1)!} - 1$.

Consider the sequence $\alpha_n = \sum_{i=1}^{n} \zeta_i p^i$. Since $|\alpha_m - \alpha_n|_p = \left(\frac{1}{p}\right)^{\min\{m,n\}}$, so this is certainly Cauchy. We claim it does not have a limit in $\overline{\mathbb{Q}}_p$. Suppose that it does have a limit, $\alpha = \sum_{n=0}^{\infty} \zeta_i p^i \in \overline{\mathbb{Q}}_p$. Let d be the degree of the minimal polynomial m_α of α over $\mathbb{Q}_p$. Now F_d/F_{d-1} is Galois of degree $d+1$. Hence there exists $\sigma_1, \ldots, \sigma_{d+1} \in \mathrm{Gal}(F_d/F_{d-1})$ such that the images of ζ_d are all distinct. Note that $|\sigma_i(\alpha - \alpha_d)|_p = |\alpha - \alpha_d|_p \leq p^{-(d+1)}$. Also for $i \neq j$, we have

$$\begin{aligned} \sigma_i(\alpha_d) - \sigma_j(\alpha_d) &= \sum_{k=0}^{d-1} \zeta_k p^k + \sigma_i(\zeta_d) p^d - \left(\sum_{k=0}^{d-1} \zeta_k p^k + \sigma_j(\zeta_d) p^d \right) \\ &= p^d(\sigma_i(\zeta_d) - \sigma_j(\zeta_d)). \end{aligned}$$

Hence for $i \neq j$, we have $|\sigma_i(\alpha_d) - \sigma_j(\alpha_d)|_p = p^{-d}$ (since $\sigma_i(\zeta_d)$ and $\sigma_j(\zeta_d)$ are distinct and $(p^{(d+1)!} - 1)$th root of unity). We conclude that

$$\begin{aligned} |\sigma_i(\alpha) - \sigma_j(\alpha)|_p &= |\sigma_i(\alpha - \alpha_d) + \sigma_i(\alpha_d) - \sigma_j(\alpha_d) - \sigma_j(\alpha - \alpha_d)|_p \\ &= p^{-d} \end{aligned}$$

This implies that $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for all $i \neq j$. But then $\sigma_1(\alpha), \ldots, \sigma_{d+1}(\alpha)$ are distinct conjugates of α. This is a contradiction to the fact that the degree of m_α is d. ☐

Note. Our sequence $\{\alpha_n\}$ was actually in $\mathbb{Q}_p^{\mathrm{un}} := \mathbb{Q}_p\left(\cup_{(n,p)=1} \mu_n\right)$, which we've shown is not complete.

We let $\mathbb{C}_p$ denote the completion of $\overline{\mathbb{Q}}_p$ (as in Theorem 1.14)

Theorem 5.5. *$\mathbb{C}_p$ is algebraic closed.*

Proof. The proof is based on the

Lemma. *Let char$(K) = 0$ and K complete with respect to a non-archimedean value. Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$. Assume f is irreducible over K. Then there exists $\delta > 0$ such that for all $g = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in K[X]$ with $|a_i - b_i| < \delta$ $(0 \leq i \leq n-1)$, g is irreducible.*

Proof. Let $\lambda_1, \ldots, \lambda_n$ be the roots of f in $\overline{K}$ and similarly let $\mu_1, \ldots, \mu_n$ be the roots of g in $\overline{K}$. Put $C = \max\{1, |a_i|\}$. Define $r = \min_{i \neq j} |\lambda_i - \lambda_j|$, $R(f,g) = \prod_{i,,j}(\lambda_i - \mu_j) = \prod_i g(\lambda_i) = \prod_j f(\mu_j) \cdot (-1)^n$ (the resultant).

Step 1 If $0 < \delta < C$ then for all g with $|a_i - b_i| < \delta$, every root μ_j over g has $|\mu_j| \leq C$.

Suppose for contradiction, we have $|\mu| > C$. Then for $0 \leq i \leq n-1$, $\left|b_i \mu^i\right| \leq C\left|\mu\right|^i < |\mu|^{i+1} \leq |\mu|^n$. This is a contradiction.

Step 2 For all $\epsilon > 0$, there exists $\delta > 0$ such that if $|a_i - b_i| < \delta$ for all i then $|R(f,g)| < \epsilon$

If $|a_i - b_i| < \delta < C$ for all i then

$$
\begin{aligned}
|f(\mu_j)| &= |f(\mu_j) - g(\mu_j)| \\
&= \left|\sum_{i=0}^{n-1}(a_i - b_i)\mu_j^i\right| \\
&\leq \max_i |a_i - b_i| \cdot \max\{1, |\mu_j|^n\} \\
&< \delta C^n
\end{aligned}
$$

by step 1. Thus for all $\delta < \min\{C, \epsilon^{1/n}C^{-n}\}$, we have $|R(f,g)| = \prod_j |f(\mu_j)| < \delta^n C^{n^2} < \epsilon$.

Step 3 If $|R(f,g)| < r^{n^2}$ then g is irreducible over K.

The condition means at least one of the factors $|\lambda_I - \mu_J| < r = \min_{i \neq j} |\lambda_i - \lambda_j|$. Then by Krasner's lemma (Theorem 5.3) , we have $K(\lambda_I) \subset K(\mu_J)$, hence $K(\mu_J)$ has degree n and so g is irreducible.

□

We apply the sublemma with $K = \mathbb{C}_p$. Let $f \in \mathbb{C}_p[X]$ be irreducible, which is monic. Let $\delta > 0$ be as in the sublemma. Since $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$, there exists a monic polynomial $g \in \overline{\mathbb{Q}}_p[X]$ satisfying the hypothesis of the sublemma. Thus g is irreducible of degree n in $\mathbb{C}_p[X]$, so also in $\overline{\mathbb{Q}}_p[X]$. But since $\overline{\mathbb{Q}}_p$ is algebraic closed, so $\deg g = 1$ □

6 Algebraic Number Fields

Let $K/\mathbb{Q}$ be a number field. A *place* is an equivalence class of non-trivial absolute values on k, denote the completion of k at $\mathcal{P}$ by $k_\mathfrak{p}$. If $\mathcal{P}$ is non-archimedean, then absolute values in $\mathbb{Q} \subset K$ are equivalent to p-adic absolute value $|\ |_p$, we write $\mathfrak{p}|p$. Then $k_\mathfrak{p}$is an extension of $\mathbb{Q}_p$ (and so is a non-archimedean local field). Let $q_\mathfrak{p}$ be the cardinality of residue field of $k_\mathfrak{p}$

Definition 6.1. The *renormalised absolute value* $|\ |_\mathfrak{p}$ on $k_\mathfrak{p}$ is determined by $|\pi_\mathfrak{p}|_\mathfrak{p} = q_\mathfrak{p}^{-1}$ where $\pi_\mathfrak{p}$ is a uniformiser. By problem C.1, we have $|\alpha|_\mathfrak{p} = |\alpha|_p^{[k_\mathfrak{p}:\mathbb{Q}_p]}$ for all $\alpha \in k_\mathfrak{p}$

If $\mathfrak{r}$ is an archimedean place, the relevant completion $k_{\mathfrak{r}}$ is either $\mathbb{R}$ ($\mathfrak{r}$ is a real place) or $\mathbb{C}$ ($\mathfrak{r}$ is a complex place) The renormalised absolute value is

$$| \ |_{\mathfrak{r}} = \begin{cases} | \ |_{\infty} & \mathfrak{r} \, \text{real} \\ | \ |_{\infty}^{2} & \mathfrak{r} \, \text{complex} \end{cases}$$

An archimedean place $\mathfrak{r}$ is an extension of an archimedean place ∞ on $\mathbb{Q}$, write $\mathfrak{r}|\infty$

Lemma 6.2. *Let $\alpha \in k^*$. Then $|\alpha|_{\mathfrak{p}} = 1$ for all but finitely many places $\mathfrak{p}$*

Proof. Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}[X]$ be a minimal polynomial of α over $\mathbb{Q}$. Then $a_j \in \mathbb{Z}_p$ $(0 \le j \le n-1)$ for almost all primes p. Hence $|\alpha|_{\mathfrak{p}} \le 1$ for almost all $\mathfrak{p}$ (not $a_j \in \mathbb{Z}_p$ implies $|\alpha|_{\mathfrak{p}} \le 1 \forall \mathfrak{p}|p$)

Similarly $\left|\alpha^{-1}\right|_{\mathfrak{p}} \le 1$ for almost all $\mathfrak{p}$ □

Theorem 6.3 (Product Formula)**.** *Let $\alpha \in k^*$. Then*

$$\prod_{\mathfrak{p} \, \text{archimedean} \, \& \, \text{non-archimedean}} |\alpha|_{\mathfrak{p}} = 1$$

Proof. By standard field theory we have $k \otimes_{\mathbb{Q}} \mathbb{Q}_p = \oplus_{\mathfrak{p}|p} k_{\mathfrak{p}}$ and $\sum_{\mathfrak{p}|p} [k_{\mathfrak{p}} : \mathbb{Q}_p] = [k : \mathbb{Q}]$

Similarly $k \otimes_{\mathbb{Q}} \mathbb{R} = \oplus_{\mathfrak{r}|\infty} k_{\mathfrak{r}}$ and $\sum_{\mathfrak{r}|\infty} [k_{\mathfrak{r}} : \mathbb{R}] = [k : \mathbb{Q}]$

Hence for all $w \in \{p, \infty\}$ (with $\mathbb{Q}_\infty := \mathbb{R}$)

$$\begin{aligned} \prod_{\mathfrak{p}|w} |\alpha|_{\mathfrak{p}} &= \prod_{\mathfrak{p}|w} |\alpha|_w^{[k_{\mathfrak{p}}:\mathbb{Q}_w]} \\ &= \left|N_{k/\mathbb{Q}}(\alpha)\right|_w \end{aligned}$$

since $N_{k/\mathbb{Q}} = \prod_{\mathfrak{p}|w} N_{k_{\mathfrak{p}}/\mathbb{Q}_w}$ (c.f. Theorem 4.5). This reduces the statement to of the theorem to the case $k = \mathbb{Q}$. Apply Problem A.2 □

Theorem 6.4 (Strong Approximation)**.** *Let S be a finite set of non-archimedean places of a number field k. Let $\epsilon > 0$. Let $\alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}$ for $\mathfrak{p} \in S$. Then there exists $\alpha \in k$ such that*

1. $|\alpha - \alpha_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon$ *for all* $\mathfrak{p} \in S$
2. $|\alpha|_{\mathfrak{p}} \le 1$, $\mathfrak{p} \notin S$, $\mathfrak{p}$ *non-archimedean*

Note: If $\alpha_{\mathcal{P}} \in \mathcal{O}_{\mathcal{P}}$ (for $\mathfrak{p} \in S$), then 2. can be replaces by $\alpha \in \mathcal{O}$.

Proof. Let S_0 be the set of rational primes p such that $\mathfrak{p}|p$ for some $\mathfrak{p} \in S$. Without loss of generality we assume S contains all $\mathfrak{p}$ extending $p \in S_0$ (put $\alpha_{\mathfrak{p}} = 0$ for $\mathfrak{p}$ not in original S). By the Weak Approximation Theorem (Theorem 1.12) there exists $\beta \in k$ such that $|\beta - \alpha_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon$ (for $\mathfrak{p} \in S$) . Lemma 6.2 implies the set R of non-archimedean places $\mathfrak{p} \notin S$ for $|\beta|_{\mathfrak{p}} > 1$ is finite. Let R_0 be the set of rational primes p such that $\mathfrak{p}|p$ for some $\mathfrak{p} \in R$. Then $R_0 \cap S_0 = \emptyset$.

Let $\eta > 0$. By the Chinese Remainder Theorem we can find $l \in \mathbb{Z}$ such that $|l - 1|_p < \eta$ for $p \in S_0$ and $|l|_p < \eta$ for $p \in R_0$. Check that $\alpha = l\beta$ satisfies the conclusion of the theorem. □

7 Diaphantine Equations

7.1 Quadratic forms

Let K be a field of characteristic not 2, $Q = \sum a_{ij}x_ix_j \in K[x_1, \ldots, x_n]$ is a *quadratic form* of rank n, We say Q is *soluble* if there exists $x \in K^n \setminus \{0\}$ such that $Q(x) = 0$

Lemma 7.1. *Suppose $[K : \mathbb{Q}_p] < \infty$, $p \neq 2$. Assume without loss of generality that $Q = \sum a_i x_i^2$, then Q is soluble if either*

1. *$n \geq 3$ and $a_i \in \mathcal{O}_K^*$ for all i*
2. *$n \geq 5$*

Proof.

1. Without loss of generality, assume $Q = ax^2 + by^2 - z^2$ for $a, b \in \mathcal{O}_K^*$. Let $k = k_K$ and assume $q = \#k$. The maps $x \to \bar{a}x^2$ and $y \to 1 - \bar{b}y^2$ have images of size $\frac{q+1}{2}$ in k. Thus the images overlap and there exists $x, y \in \mathcal{O}_K$ such that $ax^2 + by^2 \equiv 1 \mod \pi_K$. By Hensel's lemma, Q is soluble
2. On multiplying by the square of the uniformiser we may assume $v_K(a_i) \in \{0, 1\}$. As $n \geq 5$, without loss of generality, $v_K(a_1) = v_K(a_2) = v_K(a_3)$. If $v_K(a_1) = v_K(a_2) = v_K(a_3) = 0$, then apply part 1. .Otherwise if $v_K(a_1) = v_K(a_2) = v_K(a_3) = 1$, then divide through by uniformiser and apply part 1.

$\square$

Note. Part 2. is still true when $p = 2$: quinary quadratic forms are isotropic over any p-adic field.

On the arXiv, there is a recent paper by Bhargava, Cremona, Fisher which looks at the density of isotropic quadratic forms in 4 variables (roughly 97%).

Theorem 7.2 (Hasse-Minkowski Theorem)**.** *Q is a quadratic form over a number field k. Then Q is soluble over k if and only if Q is soluble over k_p for every place p.*

Proof. Omitted $\square$

Remark.

1. Lemma 7.1 implies if $n \geq 3$, then local solubility is automatic for all but finitely many primes.
2. When $n = 2$ and $k = \mathbb{Q}$ this is very easy: $a \in \mathbb{Q}_p^{*2}$, if and only if $v_p(a)$ is even. $a \in \mathbb{R}^{*2}$, if and only if $a > 0$. Both of these implies $a \in \mathbb{Q}^{*2}$.
3. Using Rimenan-Roch one can show that any smooth and projective curve of genus 0 is over a number field k is k-birationally equivalent to a conic over k. Thus Theorem 7.2 implies that the "Hasse principle" holds for smooth and projective curves of genus 0.

7.2 Cubic forms

Natural question: Is there an analogue of Lemma 7.1 for a cubic forms?

Theorem 7.3 (Demyanov ($p \neq 3$), Lewis, 1950's)**.** *Suppose $[K : \mathbb{Q}_p] < \infty$. Assume $F = \sum_{i \leq j \leq k} x_i x_j x_k \in K[x_1, \ldots, x_n]$. Then F is soluble if $n \geq 10$.*

Proof. Treat case $k = \mathbb{Q}_p$. Let $\Delta = \Delta(F)$ be the discriminant of F (this is the resultant of $\frac{\partial F}{\partial x_1}, \dots \frac{\partial F}{\partial x_n}$). Then Δ is a non-zero form of degree $n2^{n-1}$ in the coefficients of F. Moreover if $M \in \mathrm{GL}_n(\mathbb{Q}_p)$ such that $x = My$, $(F(x) = F(My) = F^*(y))$ then $F^*(y) = aF(y)$, then $\Delta(F^*) = a^{n2^{n-1}}(\det M)^{3 \cdot 2^{n-1}}\Delta$.

Since Δ is a non-zero form it can not vanish on any neighbourhood of a point. Hence if $\Delta(F) = 0$ then $\forall N \in \mathbb{N}$ there exists $c_{ijk}^{(N)} \in \mathbb{Q}_p$ such that $\Delta(F^{(N)}) \neq 0$ and $\left| c_{ijk} - c_{ijk}^{(N)} \right|_p < 1/N$. Suppose $a^{(N)}$ is zero at $F^{(N)}$ in $\mathbb{Z}_p^n$. By compactness, these points have an accumulation point in $\mathbb{Z}_p$ and since F is continuous, this point is a zero of F. Hence without loss of generality $\Delta(F) \neq 0$.

Note if F and F^* are equivalent over $\mathbb{Q}_p$, then $\Delta(F) = 0 \iff \Delta(F^*) = 0$. F is equivalent over $\mathbb{Q}_p$ to a form with coefficients in $\mathbb{Z}_p$. Then $\delta(F) = v_p(\Delta(F)) \geq 0$. We say that F is *reduced* if it has coefficients in $\mathbb{Z}_p$ and $\Delta(F) \neq 0$ and $\delta(F) \leq \delta(F^*)$ for all F^* over $\mathbb{Z}_p$ equivalent to F over $\mathbb{Z}_p$.

It suffices to work with reduced F. Let $r \in \mathbb{N}$ minimal such that $F(x) \equiv F_1(L_!, \dots, L_r) \mod p$ where $F_1 \in \mathbb{Z}_p[y_1, \dots, y_r]$ and the L_i are linear forms with coefficients in $\mathbb{Z}_p$, and are linearly independent. Clearly $r \leq n$ and make unimodular transformation $y_i = L_i$ for $1 \leq i \leq r$, to obtain an equivalent form F^*, where $F^*(y_1, \dots, y_n) \equiv F_1(y_1, \dots, y_r)$. If F is reduced then so is F^*. Let $F'(z_1, \dots, z_n) = p^{-1}F^*(pz_1, \dots, pz_r, z_{r+1}, \dots, z_n)$. Then F' has coefficients in $\mathbb{Z}_p$ and $\delta(F') = \delta(F^*) + 2^{n-1}(3r - n)$. Hence $r \geq n/3$ since F is reduced. Now $n \geq 10$ implies $r \geq 4$, hence there exists $(b_1, \dots, b_r) \in \mathbb{F}_p^4 \setminus \{0\}$ such that $F_1(b) = 0$ (by Chevaley-Warning: "Over $\mathbb{F}_p$ any form of n variables of degree d is soluble if $n > d$"). Assume without loss of generality $b_1 = 1$. Then $F^*(z_1, b_2z_1 + z_2, \dots, b_rz_1 + z_r, z_{r+1}, \dots, z_n) \equiv z_1^2L + z_1Q + C \mod p$ where L, Q, C are forms in $z_2, \dots, z_n$. Since r is minimal, L and Q are not both identically zero modulo p.

Case 1. L not identically zero modulo p: Then $(1, 0, \dots, 0)$ is a solution of $F^* \equiv 0 \mod p$ and some partial derivative of F^* does not vanish modulo p at $(1, 0, \dots, 0)$

Case 2. L is identically zero modulo p: There exists $d = (d_2, \dots, d_n) \in \mathbb{Z}^{n-1}$ such that $p \nmid (d_2, \dots, d_n)$ and such that $Q(d_2, \dots, d_n) \not\equiv 0 \mod p$. Then $(-C(d), d_2Q(d), \dots, d_nQ(d))$ is a solution of $F^* \equiv 0 \mod p$ with $\frac{\partial F^*}{\partial x_1} \neq 0 \mod p$.

In either case Hensel's lemma yields the result □

Remark.

1. $n \geq 10$ is best possible in Theorem 7.3. See problem C.3
2. Artin's conjecture: $\mathbb{Q}_p$ is a C_2 field, i.e, any form over $\mathbb{Q}_p$ in n variables and degree d is soluble over $\mathbb{Q}_p$ if $n > d^2$. This is FALSE.
3. What about an analogue of Theorem 7.2? Let k be a number field and F a cubic form over k. Then F is soluble over k if

n	Conditions	Notes
$n \geq 16$	None	Pleasants (1975)
$n \geq 10$	F non-singular	Brawning and Vishe (2013)

However the Hasse principle can fail for cubic forms in fewer variables.

For $n = 4$, the first example was produced by Swinnerton-Dyer in 1962: Let $K = \mathbb{Q}(\theta)$ where $\theta^3 - 7\theta^2 + 14\theta - 7 = 0$. Abelian cubic field of discriminant 49 and $\mathcal{O}_K = \mathbb{Z}[\theta]$. Here $(7) = P^3$ and $v_P(\theta) = 1$. Consider

$$F(x_1, \dots, x_4) = N_{K/\mathbb{Q}}(x_1 + \theta x_2 + \theta^3 x_3) + x_4(x_4 + x_1)(2x_4 + x_1)$$

Check: non-singular, soluble over $\mathbb{Q}_p$ for all p. But it is not soluble over $\mathbb{Q}$!

Proof. Note that if $N(\,) = 0$ then $x_1 = x_2 = x_3 = 0$, hence $x_4 = 0$. Contradiction as we want a non-zero solution. May assume that x_1, x_4 are coprime integers and $x_2, x_3 \in \mathbb{Q}$. Now $7|N(\,)$ implies P divides $N(\,)$, hence $7|x_1$ and $7 \nmid x_4$. Hence $7 \nmid x_4(x_1 + x_4)(2x_4 + x_1)$ which is a contradiction. Hence $7 \nmid N(\,)$.

Since $x_4, x_4 + x_1$ and $2x_4 + x_1$ are all coprime, and their product is a norm in K, each of them must separately be a norm of an ideal. Now $p \neq 7$ splits in K if and only $p = \pm 1 \mod 7$. Hence each of the factors above is congruent to ± 1 modulo 7. This contradicts $x_4 + (x_4 + x_1) = 2x_4 + x_1$. $\square$

c.f. Elsenhans-Jahnel. (Recent paper on the arXiv, they show there is a Zariski dense set of counter examples).