Notes on $p$-adic Field of Norms

Andrew Egbert

November 23, 2011

$Z_p \leftrightarrow [0, 1]^3$

\[ \sum_{i=1}^{\infty} a_i 3^i \leftrightarrow k \sum \frac{e_{a_i}}{2^{i+1}} \]
Projective Limits

This section draws from Wikipedia and various lecture notes from the internet.

Definition 1. \((\zeta_n, \mu_n, \text{primitive } n\text{-th roots of unity, cyclotomic polynomial, cyclotomic extension})\) \(\zeta_n\) denotes a generator of the complex \(n\)-th roots of unity, i.e. the number \(\exp(2\pi i/n)\) and \(\mu_n\) denotes the group of primitive \(n\)-th roots of unity\(^1\).

The \(n\)-th cyclotomic polynomial is the product \(\prod \zeta(X - \zeta)\) over all primitive \(n\)-th roots of unity \(\zeta\). Adjoining the roots to a field \(K\) gives a vector space of degree \(\varphi(n)\) consisting of the numbers \(a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{n-1}\zeta^{n-1}\) called a cyclotomic extension. Usually we denote this \(K(\zeta_n)\) for \(\zeta_n\) a primitive \(n\)-th root or just \(K(\mu_n)\). \(^2\)

---

Definition 2. (valuation, \(\mathcal{O}_R / A, m(A) / \mathcal{M}, U / U, k / R\), discrete) Suppose that in a ring \(R\), every element can be written as \(\pi^n z\) for some fixed \(\pi\) and \(n \in L\).

The \(\pi\)-adic absolute value is the function \(v_x : R \to L\) which returns \(n\). It can also be denoted \(\|\cdot\|_\pi\). \(^3\) If \(L = \mathbb{Z}\), then the valuation is called discrete.

Let \(R\) be a ring with unique maximal ideal \(m\) and a valuation \(v\). The set of \(x \in R\) with \(v(x) \geq 0\) is called alternatively the ring of integers or the valuation ring of \(A\). It is usually be denoted \(\mathcal{O}_R\) or \(A\). In the case the valuation is discrete, \(A\) or \(K\) may be called a DVR- short for discrete valuation ring.

The set of \(x \in A\) with \(v(x) > 0\) (strict inequality) is the maximal ideal denoted \(m(A)\) or \(\mathcal{M}\).

The field of fractions of \(A\) will be denoted \(K\) or with another capital letter.

---

\(^1\)Conrad 5
\(^2\)Wikipedia: Cyclotomic Field
\(^3\)Note that Lang defines the \(p\)-adic valuation as \(1/p^r\) and calls what Serre has defined the "order"
and extensions of $K$ will be given by $L|K$ or $L/K$.

Then we also have the **units** $U$ or $U$ which are $A - \mathfrak{m}(A)$ and the **residue field**, denoted $k$ or $\overline{A}$ which is $A/\mathfrak{m}(A)$.

---

**Definition 3.** (topology from valuation) Given a valuation, we define an absolute value by fixing $0 < a < 1$ and letting $\|x\| = a^{v(x)}, \|0\| = 0$ so that $\|x.y\| = \|x\| \cdot \|y\|, \|x + y\| \leq \sup(\|x\|, \|y\|)$ and $\|\cdot\|$ is positive definite. The metric topology with respect to $\|\cdot\|$ is then constructed.\(^4\)

---

**Definition 4.** (inverse system, projective limit) An **inverse system** is a collection of objects $A_i$, homomorphisms $f_{ij}: A_j \to A_i$ for $i \leq j$ satisfying $f_{ij}f_{jk} = f_{ik}$ and $f_{ii} = id$.

The **projective limit** $\lim\leftarrow$ is then defined as an object $A$ which satisfies\(^5\):

\[
\begin{array}{c}
Y \\
\downarrow \\
A \\
\downarrow \\
A_j \quad \xrightarrow{f_{ij}} \quad A_i
\end{array}
\]

---

**Definition 5.** (\(\hat{K}\)) If $K$ is a field where a discrete valuation is defined, with valuation ring $A$ then $\hat{K}$ denotes the **completion** which is a valued field whose absolute value extends $K$ - i.e. all Cauchy sequences converge.\(^6\). We have that for the uniformizer $\pi$ of $A$

\[
\hat{A} = \lim\leftarrow A/\pi^n A
\]

---

\(^4\)Serre 26

\(^5\)To get a direct limit start let the $f_{ij}$ go in the opposite direct giving a direct system, then flip the diagram upside down and let the arrows flow down and rightwards.

\(^6\)The analytic way of defining the completion is taking $\hat{K}$ to be the set of Cauchy sequences modulo the null sequences(sequences with limit 0.
and $\pi$ is a uniformizer for $\mathbb{A}$ as well.\footnote{Serre, Local Fields, p 27}

**Definition 6.** ($\mathbb{Q}_p$, $\mathbb{F}_p$, perfect field, $\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p}$, $p\mathbb{Z}_p$)

The field $\mathbb{Q}_p$, called the $p$-adic numbers is the completion of the rational numbers $\mathbb{Q}$ for the topology defined by the $p$-adic valuation. $\mathbb{Q}_p$ is locally compact with residue field $\mathbb{F}_p$ (the finite field with $p$ elements).

Note that $\mathbb{F}_p$ has characteristic $p$. Since any polynomial with coefficients in $\mathbb{F}_p$ will be annihilated by $p$, finite extensions of $\mathbb{F}_p$ have characteristic $p$ as well. A field such that every finite extension is separable (minimal polynomials of elements in extension have distinct roots) is called a perfect field. All finite fields such as $\mathbb{F}_p$ and fields of characteristic 0 like $\mathbb{Q}_p$ are perfect.

Define the $p$-adic integers $\mathbb{Z}_p$ by

$$Z_p \cong \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}.$$  

$Z_p$ is the ring of integers of $\mathbb{Q}_p$ and $\mathbb{Q}_p = \frac{\mathbb{Z}}{\mathbb{Z}p}$. 

The unique maximal ideal of a local ring is the set with valuation greater than 0. Thus $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Q}_p$ and $\overline{Q}_p = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. 

\footnote{Serre, Local Fields, p 27}
Ramification of Iwasawa towers

These notes attempt to follow Serre, *Local Fields*, IV.4 as well as Robert, *p-adic Analysis*. The aim is to set up an example to use with Conrad’s *p*-adic hodge theory notes chapter 13.

**Definition 7.** (ramification index $e$, residue degree $f$, $\pi$)

Consider a finite extension $L$ of $K = \mathbb{Q}_p$ and let $L$ have valuation ring $R$, maximal ideal $P = \pi R$ and residue field $k' = R/P$. We set

$$f = [k' : k] = [R/P : A/m(A)]$$

($f$ is called the **residue degree**) and

$$e = v_\pi(p).$$

($e$ is called the **ramification index**) So $\pi^e = p \cap K$. Note that we have $^8$ for each finite extension $L$ of $Q_p$, $ef = [L : Q_p] = n$. Furthermore, $^9$ ramification index is multiplicative in towers, i.e. $[M : L] = a, [L : K] = b \implies [M : K] = ab.$

**Definition 8.** (unramified, totally ramified, tamely ramified, wildly ramified extensions) A finite extension of $Q_p$ is said to be $^{10}$

- **unramified** when $e = 1$, i.e. when $[K : Q_p] = f = [k : pZ_p],$
- **totally ramified** when $f = 1$, i.e. when $[K : Q_p] = e,$
- **tamely ramified** when $p$ does not divide $e,$
- **wildly ramified** when $e$ is a power of $p,$

$^8$Robert 99
$^9$Ash, Chapter 8
$^{10}$Robert 100
Definition 9. \((\mathbb{Z}/n\mathbb{Z}, (\mathbb{Z}/n\mathbb{Z})^*, (\mathbb{Z}/n\mathbb{Z})^*_v)\)\(^{11}\).

\(\mathbb{Z}/n\mathbb{Z}\) is the set of equivalence classes \([x]\) of integers where \(x \sim y \iff x \equiv y \mod n\). \(\mathbb{Z}/n\mathbb{Z}\) is a ring which is a cyclic group additively, but not always multiplicatively. \((\mathbb{Z}/n\mathbb{Z})^*\) denotes the units in \(\mathbb{Z}/n\mathbb{Z}\), i.e. those elements \(a\) with an inverse \(a'\) such that \(a'a \equiv aa' \equiv 1(\mod n)\). \((\mathbb{Z}/n\mathbb{Z})^*\) is then a multiplicative group with order \(\varphi(n)\) where \(\varphi\) denotes the Euler function. Finally, \((\mathbb{Z}/n\mathbb{Z})^*_v\) will denote the subgroup of \((\mathbb{Z}/n\mathbb{Z})^*\) consisting of those elements \(a\) in \((\mathbb{Z}/n\mathbb{Z})^*\) which satisfy \(a \equiv 1(\mod p^v)\).

- \((\mathbb{Z}/p^k\mathbb{Z})^*\) is cyclic for \(p \neq 2\) since \(^{12}\) there exists a primitive root of unity.

---

Example. \(((\mathbb{Z}/n\mathbb{Z})^v)\)

Suppose that \(p = 3, n = 4\). Then \((\mathbb{Z}/p^n\mathbb{Z})^*\) will have \(\varphi(3^n) = 3^4 - 3^{4-1}\) elements\(^{13}\). Now the groups \((\mathbb{Z}/p^n\mathbb{Z})^v\) are subgroups of \((\mathbb{Z}/p^n\mathbb{Z})^*\) since if \(a \equiv 1, b \equiv 1\) then \(ab \equiv 1\cdot 1\). The subgroups are generated by the elements \([2], [4], [8], [64], [26], [28], [80]\) in \(\mathbb{Z}/3^4\mathbb{Z}\)\(^{14}\). Then we have

|    |   2 | \equiv 2 mod 3 | \ldots |   |
|----|-----|----------------|--------|
| 4  | \equiv 1 mod 3 | \equiv 4 mod 9 | \ldots |
| 8  | \equiv 2 mod 3 | \ldots | |
| 64 | \equiv 1 mod 3 | \equiv 1 mod 3^2 | \equiv 10 mod 3^3 |
| 26 | \equiv 2 mod 3 | \ldots | |
| 28 | \equiv 1 mod 3 | \equiv 1 mod 3^2 | \equiv 1 mod 3^3 |
| 80 | \equiv 2 mod 3 | \ldots | |

\(^{11}\) A good reference on \(\mathbb{Z}/n\mathbb{Z}\) is Stein, *Primes, Congruences, Secrets*

\(^{12}\) Stein, Elementary, 40

\(^{13}\) For information about the function \(\varphi\), see Apostol, Intro to Analytic Number Theory Chapter 2

\(^{14}\) found using Sage
so that \((Z/3^4Z)^1 = \langle [4] \rangle\), \((Z/3^4Z)^2 = \langle [64] \rangle\), and \((Z/3^4Z)^3 = \langle [28] \rangle\). Also \#\langle 4 \rangle = 27, \#\langle 64 \rangle = 9, and \#\langle 28 \rangle = 3.

Figure 1: Cayley graph of the subgroups \((Z/3^4Z)^1\), \((Z/3^4Z)^2\), \((Z/3^4Z)^3\)

**Definition 10.** \((\text{Gal}(L/K), \text{Gal}(K(\mu_n)/K))\) We denote by \(\text{Gal}(L/K)\), the group of automorphisms of \(L\) which fix \(K\). \(\text{Gal}(L/K)\) is the "Galois group" of the
extension $L$ over $K$.”

For a cyclotomic extension, each $\sigma \in \text{Gal}(K(\mu_n)/K)$ performs $\sigma(\zeta) = \zeta^i$ for $i \in (\mathbb{Z}/n\mathbb{Z})^*$. $^{15}$ Thus $\text{Gal}(K(\mu_n)/K)$ is embedded in $(\mathbb{Z}/p^n\mathbb{Z})^*$. Also, for an unramified extension, we have $\text{Gal}(L/K) = \text{Gal}(l/k)$ (the small letters $l, k$ denoting residue fields).

---

**Definition 11.** ($L$ is Galois over $K$, Fundamental theorem of Infinite Galois theory)

- Given an extension of fields $K \subset L$, we say that $L$ is **Galois over $K$** if $^{16}$

\[
L = \bigcup_{M/K, \text{ finite, Galois, } K \subset M \subset L} M
\]

- As a corollary to the **Fundamental theorem of Infinite Galois theory** $^{17}$ we get that

\[
\text{Gal}(L/K) = \varprojlim \text{Gal}(M/K)
\]

indexed over all finite Galois subextensions $M/K$ of $L/K$.

- The lattice of subgroups of $G(K/F)$ is the inverted lattice of intermediate fields of $K$ over $F$.

$^{15}$Milne, Galois, page 49
$^{16}$Lenstra 4
$^{17}$Lenstra 4, Milne 73
A final result tied to the fundamental theorem is that if \( E | F \) is a finite Galois extension and \( K \) is an intermediate field, then \( E | K \) is always Galois.  

**Definition 12.** (Eisenstein polynomials, \( B_f \), Eisenstein’s criterion) A monic polynomial \( f(X) \in \mathbb{Z}_p[X] \) of degree \( n \geq 1 \) satisfying \( f(X) \equiv X^n \mod p \) and \( f(0) \not\equiv 0 \mod p^2 \), is called an **Eisenstein polynomial**. Let \( f \) be an Eisenstein polynomial, \( B_f = A[X]/(f) \) which is the free \( A \)-algebra generated by \( \{1, X, \ldots, X^{n-1}\} \). We have the follow two results known as Eisenstein’s criterion.

- Eisenstein polynomials are irreducible in \( \mathbb{Z}_p[X] \) and \( \mathbb{Q}_p[X] \).
- The homomorphism of \( A[X] \) into an integral closure \( B \) (of \( A \) in a finite extension \( L | K \)) which maps \( X \) onto a uniformizing element \( \pi \) is an isomorphism of \( B_f \) to \( B \).

**Definition 13.** \((K_n)\) Define \( K_n = \mathbb{Q}_p(\zeta_{p^n}) \) for \( p \) an odd prime. This forms what is called the **cyclotomic tower** or **Iwasawa tower**. We could also use the **Kummer tower**: \( K_n = K(p^{1/p^n}) \), however, I will stick to the cyclotomic case.

**Result 1.** (We have that) \( \text{(i)} \) \( [K_n : K] = \varphi(p^n) = (p - 1)p^{n - 1} \),

\( \text{(ii)} \) The Galois group \( \text{Gal}(K_n/K) \) can be identified with the group \((\mathbb{Z}/p^n\mathbb{Z})^*\),

---

18 Ash 6.2.1  
19 Robert 101-102, Serre 17-18  
20 These results are taken from Robert 101-104, Serre 78
(iii) $K_n$ is a totally ramified extension of $K$. The element $\pi = \zeta - 1$ is a uniformizer of $K_n$, and $A_{K_n} = A_K[\zeta]$.

- We know $\text{Gal}(K_n/K) \cong H \leq (\mathbb{Z}/p^n\mathbb{Z})^*$ 21. (We use $\leq$ to denote subgroup here). The order of $(\mathbb{Z}/p^n\mathbb{Z})^*$ is $\varphi(p^n)$. But then the degree of a cyclotomic field extension is the order of the Galois group, and $\varphi(p^n) = p^n - p^{n-1}$ 22
  = $(p - 1)p^{n-1}$. Thus (i) and (ii) are equivalent.

- Let $\zeta = \zeta_p^n = \exp\left(\frac{2\pi i}{p^n}\right)$. Let $u = \zeta^{p^{n-1}}$. Since $\exp\left(\frac{2\pi i}{p^n} \cdot p^{n-1}\right) = \zeta_p$, then $u$ is a primitive $p$-th root of unity.

- Using geometric series, we have $\sum_{i=0}^{p-1} u^i = \frac{1-u^p}{1-u} = 0$. This equality holds if $u$ were to be any other primitive $p$-th root of unity, or indeed for any power of $\zeta_p$ between 1 and $p^n - 1$ which is relatively prime to $p$.

- Let $F(X) = X^{(p-1)p^{n-1}} + X^{(p-2)p^{n-2}} + \cdots + 1$ so that $F$ factors (by the previous step) as $\prod_{1 \leq j \leq p^n - 1, (j,p) = 1} (X - \zeta^j)$ and let $G(X) = F(X + 1)$.

- Thus we get $\pi = \zeta - 1$ has $G(\pi) = 0$. $G(0) = p$ which is the constant term of $G(X)$, and every non-initial coefficient of $G$ contains a factor of $p$. By Eisenstein’s criterion, $G$ is irreducible.

- We have 23 that
  $$\sum_{j=1}^{p^n} 1 = \varphi(p^n) = (p - 1)p^{n-1}$$
  so that $G$ is an irreducible polynomial which factors linearly over $K_n$ and whose coefficients generate $K_n$. i.e. $K_n$ is a splitting field $G$. Thus $[K_n : K] = \varphi(n)$. We have now shown (i) and (ii).

21 Also see Evens 14, Milne: Galois 50
22 Apostol 28
23 Apostol 25, 28
• By induction, since $\zeta \equiv 1 \mod \pi$ then

$$\frac{(1 - \zeta^j)}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{j-1} \equiv j \mod \pi.$$ 

For $(j, p) = 1$ therefore, $\pi \nmid \frac{(1-\zeta^j)}{1-\zeta}$ so that $v_\pi(\frac{1-\zeta^j}{1-\zeta}) = 0$ and thus $v_\pi(1-\zeta) = v_\pi(1 - \zeta^j)$ for $(j, p) = 1$.

• Since $p = \prod_{1 \leq j \leq p^{n-1}, (j, p) = 1} (1 - \zeta_p)^j$, then $v_\pi(p) = \varphi(p^n) \cdot (v_\pi(1 - \zeta))$ so that $K_n$ is totally ramified over $Q_p$. Note that using the second Eisenstein proposition, we have both of these much easier and in addition, we get straight away that $A_{K_n} = A_K[\zeta]$.

Something we will use later is that the quotient $[K_n : K_{n_0}]$, for $n_0 > 1$, is totally ramified since ramification is multiplicative in towers. \(\square\)

---

**Definition 14.** $(G_i, i_G, G_u)$ Let $L$ a finite extension of $K$ and $B$ the integral closure of $A$ in $L$. For instance in the cases we have been looking at we have $L = Q_p(\zeta_p^m)$ and $K = Q_p$, $A = \mathbb{Z}_p$, $B = A[\zeta_p^m]$.

We have \(^{24}\) if $B$ (then also $A$) is a DVR, and the extension of residue fields separable, then $B$ has a basis over $A$ consisting of a single element.

Let $G_i$, the $i$-th lower ramification group, be the set of all $s \in Gal(L/K)$ satisfying the following equivalent conditions:

- $s$ operates trivially on the quotient ring $A_L/p_L^{i+1}$
- $v_L(s(a) - a) \geq i + 1$ for all $a \in A_L$
- $v_L(s(x) - x) \geq i + 1$ where $x$ generates $A_L$ as an $A_K$ algebra.

With $x$ an $A_K$-generator of $A_L$, (i.e. $\zeta_p^m$) we define $i_G : G \to Z$ by $i_G(s) = v_L(s(x) - x)$ so that $\text{Serre 57}$
\begin{itemize}
  \item $i_G(s) \geq i + 1 \iff s \in G_i$
  \item $i_G(tst^{-1}) = i_G(s)$
  \item $i_G(st) \geq \text{Inf}(i_G(s), i_G(t))$
\end{itemize}

Finally, if $u$ is a real number, $\geq -1$, $G_u$ denotes the ramification group $G_i$, where $i$ is the smallest integer $\geq u$.

---

**Result 2.** The ramification groups $G_u$ of $\text{Gal}(K_n/K)$ are:

\begin{align*}
  G_0 &= (\mathbb{Z}/p^n\mathbb{Z})^* \\
  1 \leq u \leq p - 1 & \quad G_u = (\mathbb{Z}/p^n\mathbb{Z})^1 \\
  p \leq u \leq p^2 - 1 & \quad G_u = (\mathbb{Z}/p^n\mathbb{Z})^2 \\
  \vdots & \quad \vdots \\
  p^{n-1} \leq u & \quad G_u = (\mathbb{Z}/p^n\mathbb{Z})^n = \{1\}
\end{align*}

Figure 2: Cayley graphs of the subgroups $(\mathbb{Z}/3^4\mathbb{Z})^1, (\mathbb{Z}/3^4\mathbb{Z})^2, (\mathbb{Z}/3^4\mathbb{Z})^3$. Each ring represents a coset

\begin{itemize}
  \item Let $a \neq 1$ be an element of $(\mathbb{Z}/p^n\mathbb{Z})^*$, and let $s_a$ be the corresponding element of $\text{Gal}(K_n/K)$.
  \item Let $v$ be the largest integer such that $a \equiv 1 \mod p^v$. Clearly $a \in (\mathbb{Z}/p^n\mathbb{Z})^v$ and $a \notin (\mathbb{Z}/p^n\mathbb{Z})^{v+1}$ by maximality of $v$.
\end{itemize}
• We have $i_G(s_a) = v_{K_n}(s_a(\zeta) - \zeta) = v_{K_n}(\zeta^a - \zeta) = v_{K_n}(\zeta^{a-1} - 1)$ for some $q$. (The last from $v_{K_n}(\zeta) = 0$ since it’s a unit and $v_{K_n}(ab) = v_{K_n}(a) + v_{K_n}(b)$.) Then from the proof of the previous result, $\zeta - 1 = \pi, \zeta \equiv 1 \mod \pi, v(1) = 0$.)

• Notice that $s_a$ is an isomorphism so preserves primitive roots. Then

$$(Z/p^mZ)^*/(Z/p^nZ)^* \simeq (Z/p^{m-n}Z)^*$$

(we are just doing $\exp(2\pi k/p^n)$. In the quotient, $a \equiv 1 (\mod p^i) \iff a - 1 \equiv 0 (\mod p^i)$ for any $i$ so that $a$ is a generator of the quotient $(Z/p^{m-n}Z)^*$. Thus $\zeta^{a-1}$ is a primitive $n - v$-th root of unity.

• Using the above result, $\zeta^{a-1} - 1$ is a uniformizer for the field $K_{p^{n-v}} \cong K_n/K_{n-v}$. Thus $i_G(s_a) = v_{K_n}(\zeta^{a-1} - 1) = [K_n : K_{n-v}]$. The cardinality here is $\varphi(p^n)/\varphi(p^{n-v})$ which comes out to $p^v$. You can also say this is the cardinality of $(Z/p^nZ)^{n-v}$ since $\zeta^{a-1}$ is primitive in both extensions. In particular, a cyclic group of size $p^v$ is the additive group $Z/p^vZ$.

• We defined the ramification groups by $s \in G_u \iff i_G(s) \geq u + 1$. Hence if $p^{k-1} \leq u \leq p^k - 1$ then $s_a \in G_u \iff i_G(s_a) = p^v \geq u + 1$ or $v \geq k$ so $G_u = (Z/p^nZ)^v$. 25

---

**Definition 15.** ($G^i$, Herbrand Function) Recall that $s \in G_u \iff i_G(s) > u + 1$. Put

$$\phi_{L/K} = \int_0^u \frac{dt}{(G_0 : G_t)}.$$  

Then, 26

25Note that if we adjoin then $p^n$th roots for all $n$, then the upper ramification groups indices are unbounded. This is the same as saying that the upper ramification group $\text{Gal}(L/F)(x)$ is open (i.e. finite index) in the union

26Serre 73, Conrad 200
• $Gal(L/K)_x = Gal(L/K)^{\phi_{L/K}(x)}$. The $G^u$ are the upper ramification groups of the extension.

• This function is continuous, piecewise-linear self-map of $[-1, +\infty)$ whose slope on the interval $(i - 1, i)$ is $\#Gal(L/K)_i / \#Gal(L/K)_0$ for all $i \geq 0$ and $\phi_{L/K}(x) = x$ for $x \in [-1, 0]$. The graph is increasing and also it is linear except for a countable set of “jumps”.

\[
\begin{array}{c}
\phi_{L/K}(u) \\
\end{array}
\]

An explicit representation of $\phi_{L/K}$ is

\[
\phi_{L/K}(u) = \frac{1}{g_0}(g_1 + \cdots + g_m + (u - m)g_{m+1})
\]

where $g_i = \#G_i$. The function $\phi_{L/K}(u)$ is called the herbrand function.

**Result 3.** (The jumps in the filtration $(G^v)$ are integers. Moreover, $G^v = (Z/p^n Z)^v$ for $0 \leq v \leq n$ and $G^v = \{1\}$ for $v \geq n$. )

• We saw in the last result that the jumps in the filtration $(G_u)$ occur when $u = p^k - 1$, with $0 \leq k \leq n - 1$ whenever $0 \leq k \leq n - 1$. We must show that $\phi_{L/K}(p^k - 1) = k$ for $0, 1, \ldots, n - 1$.

• For integers $m$ we have $\phi_{L/K}(m) = \frac{1}{g_0} \sum_{i=0}^{m} g_i$ where $g_i = \#G_i$. 

14
• We have \( \#G_i = \varphi(p^{n-i}) = p^{n-i} - p^{n-i-1} \) and we know that on the interval \( p^i \leq u \leq p^{i+1} \) there are \( p^{i+1} - p^i \) terms. Decompose each of these into \( (p-1) \), giving \( p^{n-i}(p-1) \) and \( p^{i+1}(p-1) \) we see that they cancel out to make 1 so we add one each increase.

\[ \square \]

**Definition 16.** \((Q_p(\zeta_{p^\infty}), K_\infty, \Gamma)\)

Let \( K_\infty = K_{p^\infty} = Q_p(\zeta_{p^\infty}) \) be the direct limit with respect to inclusions of the extensions \( K_n \). Recall the fundamental theorem of infinite Galois theory:

\[ \text{Gal}(L/K) = \lim_{\leftarrow} \text{Gal}(M/K) \]

Thus we have that the Galois group \( \Gamma = \text{Gal}(K_{p^\infty}/K) \) is equal to the projective limit of the groups \((Z/p^mZ)^*\). An element \( s_\alpha \in \text{Gal}(K_\infty/K) \) associated to \( \alpha \) transforms a \( p^m \)-th root of unity \( z \) into \( z^{\alpha^{27}} \).

As the\(^{28}\) projective limit of the rings \( Z/p^mZ \) is the ring \( Z_p \) of \( p \)-adic integers, the limit of \((Z/p^mZ)\) can naturally be identified with the group \( U_p = Z_p^* \) of invertible elements of \( Z_p \). Note that \(^{29}\) gives us

\[ Z_p^* \cong \begin{cases} 
Z/(p-1)Z \times Z_p & p > 2 \\
Z/2Z \times Z_2 & p = 2
\end{cases} \]

---

\(^{27}\)Serre 79

\(^{28}\)Serre 79

\(^{29}\)Lenstra 1
Field of Norms and $\pi$

Here I attempt to follow Conrad’s $p$-adic Hodge theory notes using examples constructed in the previous section to illustrate how to build a norm-compatible sequence of maps for construction of the “field of norms.” The purpose is to build necessary scaffolding for expository on Fontaine and Wintenberger’s equivalence of categories between norm fields and absolute galois groups.

I will say a little about the slightly more general case.

**Definition 17.** $(K, M, L, L_n, L_\infty, n_0)$ Since I have already used $\overline{K}$ to denote the residue field, let $K$ be the closure of $K$. Fix a finite extension $M/K_\infty$ inside of $K$. Choose a finite extension $L/K$ such that $M = LK_\infty$, and define $L_n = LK_n$ for all $n \geq 0$ and $L_\infty = LK_\infty = M$. Then there is an $n_0(L)$ such that $L_\infty/L_{n_0(L)}$ is a totally ramified $\mathbb{Z}_p$-extension with each $L_n/L_{n_0(L)}$ of degree $p^{n-n_0(L)}$ for $n \geq n_0(L)$. $n_0$ is fixed.

$$M = \lim \rightarrow \begin{array}{c}
L = L_0 \\
\square
\end{array} \begin{array}{c}
L_1 \\
\triangle
\end{array} \begin{array}{c}
L_2 \\
\diamond
\end{array} \begin{array}{c}
L_3 \\
\circ
\end{array} \ldots $$

Here are some facts we will need:

**Result 4.** *(Some notes on the ramification and valuations of $K_n$)*

- Before, we showed that for $K_n$ there is $m_0 \geq 0$ such that $y_{m+1} = y_m + e$, where $e$ is the ramification index (1 in totally ramified) and $y_n$ denotes the upper ramification indexes. This comes straight from the definition of the herbrand function as $\phi_{L/K}(m) + 1 = \frac{1}{g_0} \sum_{i=0}^{i=m} g_i$ where $g_i = \text{Card}(G_i)$. We note that $G_i = \{1\}$ for $i > m$.

- In fact this holds for the extends $L_n$ as well. \(^{31}\)

\(^{30}\)Conrad 13.1.4, 199

\(^{31}\)Conrad 13.1.6, page 201
• Using the above, there exists \( m_K \geq m_0 \) such that

\[
v((g - id)(t)) \geq \frac{1}{2(p - 1)}
\]

for all \( m \geq m_K \), all \( g \in \text{Gal}(K_{m+1}/K_m) \), and all \( t \in \mathcal{O}_{K_{m+1}} \).

• In the case of \( K_n \), we use the fact that \( \text{Gal}(K_{p^n}/K_{p^{n-1}}) = G_1 \) \(^{33}\) which satisfies \( v(g(x) - x) \geq i + 1 \) for all \( x \in \mathcal{O}_{K_{m+1}} \). The more general case is not much more involved. \(^{34}\)

\[\square\]

Definition 18. (APF, Hasse-Herbrand function) For \( L \) a separable extension of \( K \) with finite residue field extension, we view \( L \) as the union of an increasing directed family of subfields \( L_i \) which are finite extensions of \( K, i \geq 0 \). The extension \( L/K \) is said to be arithmetically profinite (APF) if one of the following is satisfied \(^{35}\):

• The composite of Herbrand functions \( h_{L/F} = \cdots \circ h_{L_i/L_{i-1}} \circ \cdots \circ h_{L_0/K}(a) \) is a real number for every real \( a > 0 \).

• The upper ramification jumps form a discrete unbounded set.

• For every \( x \) the upper ramification group \( \text{Gal}(L/F)(x) \) is open (i.e. of finite index) in \( \text{Gal}(L/F) \). That it is open means that \( y_m \to \infty \). \(^{36}\)

The function \( h_{L/F} \) described above is called the Hasse-Herbrand function of \( L/F \). \( h_{L/F} \) is piecewise linear, continuous, and increasing \(^{37}\).

\(^{32}\)Conrad 13.1.7, page 202

\(^{33}\)Serre 78

\(^{34}\)Conrad, page 202

\(^{35}\)Fesenko 96-97

\(^{36}\)Conrad 201

\(^{37}\)Fesenko, 96
Result 5. ($K_\infty$ is APF)

- Since $K_\infty/K$ is totally ramified, the residue degree is finite.
- Let $a > 0$ and choose $m$ such that $p^m > a$.
- We have in general\(^{38}\) $\phi_{L/K} = \phi_{K'/K} \circ \phi_{L/K'}$.
- For $p^m, p^n > u$ we have $\phi_{K_n/K}(u) = \phi_{K_m/K}(u)$. This is because for $p^{n-1} \leq u$, $G_u = (\mathbb{Z}/p^n\mathbb{Z})^n = 1$.
- Therefore, $\phi_{K_{n+1}/K_n}$ for $p^n > u$ is constant so that $h_{K_\infty/K}$ is a real number.
- Note that this basically means the Herbrand function completely flattens out:

\[
\begin{array}{c}
\text{Slopes of } \phi_{K_n/K} \\

\begin{array}{c}
\text{1} \\
\text{1/p} \\
\ldots \\
\text{1/p^{m-1}} \\
\text{0}
\end{array}
\end{array}
\]

\[\square\]

Definition 19. ($R, v_R, N(L|K)$)

In general, the perfection $R(A)$ (also denoted $R_A$ or just $R$ if context is clear)\(^{38}\) Serre, 74
of a ring $A$ which has characteristic $p$ is the projective limit of $\cdots \to A \to A \to A \to \cdots$ where transition maps are given by Frobenius. Thus an element of $R_M$ might look like $(t, t^{1/p}, t^{1/p^2}, \ldots)$ for some $t \in \hat{O}_M$.

![Diagram](image1)

Figure 3: Perfection: In the infinitely ramified case, the transition maps map a circle with a bunch of vectors on it to another circle with a bunch of vectors on it.

![Diagram](image2)

Figure 4: Perfection: In the finitely ramified case, the transition maps map a circle with a bunch of vectors on it to another circle with a bunch of vectors on it.

The perfection comes equipped with a map sending $(x_n)_n \mapsto x_0$. We define the valuation $v_R$ to be the limit of valuations of elements in a sequence in $R$.

Let $L$ be an infinite APF extension of $K$, and let $L_i, i \geq 0$, be an increasing directed family of subfields, which are finite extensions of $K$, $L = \bigcup L_i$. Let

$$N(L|F)^* = \lim_{\leftarrow} L_i^*$$

be the projective limit of the multiplicative groups with respect to the norm homomorphisms$^{39}$ $N_{L_i/L_j}, i \geq j$. Put $N(L|F) = N(L|F)^* \cup \{0\}$. $N(L|F)$ will be

---

$^{39}$The importance of using the norm is that it is valuation preserving at each joint $L_i/L_j$
shown to be a field, called the **field of norms**\(^{40}\). Fontaine-Wintenberger classically \(^{41}\) proved a result which is partly motivation for Scholze’s Perfectoid tilting equivalence, \(^{42}\) that the absolute Galois group of \(L\) is naturally isomorphic to the absolute Galois group of \(N(L|F)\).

The ring structure of \(N(L|F)\) is given by \((xy)^{(n)} = x^{(n)}y^{(n)}\) and \((x + y)^{(n)} = \lim_{m \to \infty} N_{K_{n+m}/K_n}(x^{(n+m)} + y^{(n+m)})\).\(^{43}\)

---

**Result 6.** *(The group \(N(L|K)^\ast\) does not depend on the choice of \(L_i)\)*

- Let \(L'_i\) another increasing directed family of finite extensions of \(K\) and \(L = \bigcup L'_i\)
- Then we can find \(L'_i \subset L_j\) for any \(i\).
- But \(N_{L_j/K} = N_{L_j/L'_i} \circ N_{L'_i/K}\).

---

**Definition 20.** *(Teichmuller Coefficients)* Any \(\pi\)-adic integer can be written as a power series \(a_0 + a_1p^1 + a_2p^2 + \ldots\) where the \(a_i\)'s are usually taken from the set

---

\(^{40}\) Actually, we will give it another equivalent definition
\(^{41}\) Fontaine-Wintenberger, Corps Locaux
\(^{42}\) MathOverflow Scholze
\(^{43}\) Berger 23
\{0,1,\ldots,p-1\}. Really the important thing is that \(a_i \in F_p\) (the finite field of order \(p\)) - using an isomorphism. Thus another set of possible coefficients is the \(p-1\)st roots of unity together with 0, i.e. roots of \(x^p - x = x(x^{p-1} - 1) = 0\). \(^{44}\)

---

**Result 7.** (*Why we use the terminology “norm fields”*)

- We have the uniformizer \((1 - \zeta)\) for \(K_n/K\). Then \(N_{K_n/K_{n-1}}(1 - \zeta) = \prod_{g \in \text{Gal}(K_n/K_{n-1})} g((1 - \zeta))\).

- \(g\) is just sending \(\zeta \mapsto \zeta^a\). Also the numbers \(\frac{(1-\zeta^i)}{(1-\zeta)}\) are units for \(i < p\).

- Thus, up to unit, \(N_{K_n/K_{n-1}}(1 - \zeta) = (1 - \zeta)^p\). \(^{45}\)

- Thus, up to unit, \(N_{K_n/K_{n-1}}\) is just a \(p\)-power map on \(O_{K_n}\) since every element of \(O_{K_n}\) can be written \(u\pi^n\) for a unit \(u\).

- Now consider \(pA_K[\zeta_p^n]\) if we mod out by this then we get

\[(\zeta_p^n - 1)^p \equiv \zeta_p^{n-1} - 1 \mod pA_K[\zeta_p^n]\]

- Thus

\[N_{L_{n+1}/L_n}(x) \equiv x^p \mod pA_K[\zeta_p^{n+1}]\]

up to units. In general, by definition of the lower ramification groups, the automorphism \(g\) operates trivially on the quotient ring \(A/pA_K[\zeta_p^{n+1}]\) so that the norms of units are in the same residue class giving the congruence.

- In the more general case, \(^{46}\) There exists an integer \(n_L \geq 0\) and a proper ideal \(a_L\) in \(O_{L^{(n_L)}}\) containing \(p\) and such that \(a^N \subseteq pO_{L^{(n_L)}}\) for some \(N \geq 1\)

\(^{44}\)In these cases, we call the set of \(\pi\)-adic integers an \(F_p\)-algebra?

\(^{45}\)Here we can also use Serre 2.2.3, which states that conjugate elements have the same valuation

\(^{46}\)Conrad 13.3.1, page 210
such that
\[ N_{L_{n+1}/L_n}(x) \equiv x^p \mod a_LO_{L_{n+1}} \]
for all \( x \in O_{L_{n+1}} \) and all \( n \geq n_L \).

- The argument goes something like:
  
  - Since we know the slopes of the Herbrand function, we can find \( n_L \geq n_0(L) \) such that
    \[ v((g - id)(x)) \geq \frac{1}{2(p-1)} \]
  for all \( x \in O_{L_{n+1}} \) and all \( g \in Gal(L_{n+1}/L_n) \).

  - Now choose an ideal to replace \( p \) which is \( gO_{L_{n_L}} \) for some \( y \) with \( 0 \leq v(y) \leq \frac{1}{2(p-1)} \).

  - Then all \( g \in Gal(L_{n+1}/L_n) \) are in the ramification group cut out by
    \( i = \frac{1}{2(p-1)} \) and so all automorphisms act trivially on the residue field, thus on the units. Thus use the multiplicativity of the norm and the fact that the uniformizer divided by a power of itself is a unit.

\[ \square \]

---

**Example.** (An element of \( N(K_{\infty}/K) \)) Note that we can compute

\[ (1 - \exp(\frac{2\pi i}{p^n}))p \equiv 1 - \exp(\frac{2\pi i}{p^{n-1}}) \mod pO_K \]

This element \((1 - \zeta_p^n)_n = \epsilon\) is a uniformizer for \( N(K_{\infty}/K) \).

---

**Result 8.** (For any \( n \geq n_L \) and uniformizer \( \pi_{L_n} \) of \( L_n \), there exists a uniformizer \( \pi_{L_{n+1}} \) of \( L_{n+1} \) such that \( \pi_{L_{n+1}}^p \equiv \pi_{L_n} \mod a_LO_{L_{n+1}} \).)

\[ ^{47} \text{Conrad 13.3.6, page 212} \]
• Choose a uniformizer $\pi$ of $L_{n+1}$. $N_{L_{n+1}/L_n}(\pi)$ is a uniformizer of $L_n$ since it is not a unit (norm and powers of units are units) and we are in indices where galois group acts trivially on units.

• Using Teichmuller $\pi$-adic expansion we write $N_{L_{n+1}/L_n}(\pi) = \sum_{i=1}^{\infty} [a_i] \pi^{i}$ where the constant term is zero so the two uniformizers $N_{L_{n+1}/L_n}(\pi)$ and $\pi_{L_n}$ are congruent and also $[a_1]$ is nonzero.

• The uniformizer we want, $\pi_{L_{n+1}}$ must be $\pi_{L_{n+1}} = \sum_{j=1}^{\infty} [b_j] \pi^j$. Then, using the fact that $p \in a_L$, and working mod $a_L$,

$$\pi_{L_{n+1}}^p \equiv \sum_{j=1}^{\infty} [b_j]^p \pi^{pj} \equiv$$

(by the previous result)

$$\sum_{j=1}^{\infty} [b_j]^p \left( \sum_{i=1}^{\infty} [a_i] \pi^{i} \right)^j \equiv$$

$$\sum_{m=1}^{\infty} (b_m)^p [a_1]^m + \sum_{j=1}^{m-1} [b_j]^p P_{m,j}([a_1],\ldots,[a_m]) \equiv \pi_{L_{n+1}}^m \mod a_L \mathcal{O}_{L_{n+1}}$$

for some $P_{m,j} \in Z[X_1,\ldots,X_m]$.

• Solve $b_m a_1^m + \sum_{j=1}^{m-1} b_j^p P_{m,j}(a_1,\ldots,a_m) = \delta_{m,1}$ in order to get a single coefficient for the $\pi_{L_n}$-adic expansion. This gives a set of coefficients which makes the desired uniformizer.

\[\square\]

**Definition 21.** (Absolute Galois group, Field of Norms (second definition), $\mathcal{P}$)

Let the separable closure of a field $F$ (or maybe an extension $L$) be

$$L^{sep} = \{ \alpha \in \overline{L} : \alpha \text{ separable over } L \}$$
remembering that \textit{separable} means the minimal polynomials are separable - \( \gcd(f, f') = 1 \). The \textbf{Absolute Galois group} of of \( F \) is \( \text{Gal}(F^{\text{sep}}/F) \). This absolute galois group is denoted \( G_F \).

Let \( E_L^+ \subset R_{L_{\infty}} \) be the subring of \( p \)-power compatible sequences \((x_n)_n\) such that \( x_n \in \mathcal{O}_{L_n} = \mathcal{O}_{LK_n}\). For a finite extension \( M/K_{\infty} \), choose a finite extension \( L/K \) inside of \( M \) such that \( M = LK_{\infty} = L_{\infty} \). We define \( E_M^+ \) as \( E_L^+ \) inside of \( R_{L_{\infty}} = R_M \). The fraction field \( E_M = \text{Frac}(E_M^+) \) is called the \textbf{field of norms} of \( M \) relative to \( K_{\infty}/K \) (it is also denoted \( E_L \)). We will use this second definition from now on for the \textbf{field of norms}.

\begin{example} \textbf{(Induced Galois action)} \ Assume that \( p = 5 \) let \( M = L_{\infty} \) be the extension of \( K_{\infty} \) given by adjoining \( \exp\left(\frac{2\pi i}{3}\right) \). Then \( \sigma \in \text{Gal}(L_{\infty}/K_{\infty}) \) is a ring isomorphism which is the identity on \( K_{\infty} \) and so \( \sigma : \zeta_3 \mapsto \zeta_3^\sigma \). The extension \( L_{\infty} \) is equivalent to extending \( K \) by \( \zeta_3 \) to get an extension \( L \) and then taking the direct limit of \( L_i = K_iL \). \( E_M = E_{L_{\infty}} \) is the fraction field of \( p \)-power compatible sequences and if \( (x_n)_{n \geq 0} \in E_M \) and \( \sigma : \zeta_3 \mapsto \zeta_3^\sigma \), then

\begin{align*}
\sigma(x_n)^p &= \sigma(l_n \cdot k_n)^p = \\
\sigma(l_n)^p \cdot (k_{n-1}) &= \sigma(p_n)^p \cdot (k_{n-1}) = \\
\sigma(l_{n-1}) \sigma(k_{n-1}) &= \sigma(x_{n-1})
\end{align*}

so that there is a natural galois action of the galois group of \( M \) on the field of norms \( E_M \). This describes a homomorphism from \( \text{Gal}(M/K_{\infty}) \) to \( \text{Gal}(E_M/E_{K_{\infty}}) \)
Functor of the Field of Norms

We want to associate the Galois behavior of $E_{K\infty}$ and $K\infty$. In order to do this, wts that the correspondence $M \mapsto E_M$ sets up a fully faithful bijection between finite extensions of $K\infty$ inside of $\overline{K}$ and the finite extensions of $E_{K\infty} = E_K$. This will give us the equivalence of absolute Galois groups.

We have the following topological results:

- The topology on $E_K$ is given by the the valuation with respect to $\pi_K$.
- For an extension $M/K\infty$, the subring $\varphi^{-\infty}(E_M^+)$ of all $p$-power roots is contained in $R_M$ and is dense for the $\pi_L$ induced topology.
- For an extension $M/K\infty$, if $g \in \text{Gal}(M/K\infty)$ acts trivially on $R_M$ then $g = 1$.

Result 9. (Idea of the Galois equivalence)

- We want to show that all finite separable extensions of the norm field $E_{K\infty}$ have the form $E_M$.
- In this case, the absolute galois group is $G_K = \text{Gal}(K^{\text{sep}}/K)$, where $K^{\text{sep}}$ is the direct limit of all finite extensions of $K$.
- Thus we can write $G_K = \lim \rightarrow \text{Gal}(M/K)$ where $M$ is separable over $K$ and similarly, $G_{E_K} = \lim \rightarrow \text{Gal}(E_M/E_K)$ where $M$ is finite over $K$.
- If $\text{Gal}(M/K\infty) \cong \text{Gal}(E_M/E_{K\infty})$ the theorem is proved.
- In the slightly more general case, you prove it for $M'/M/K\infty$ giving the result for $M$ and the proof is not much worse.

Result 10. (For $M'/M/K\infty$ inside of $\overline{K}$, the extension $E_{M'}/E_{M}$ has finite degree equal to $[M' : M]$. )
• We examine the case $M = K_\infty$ and just write $M$ for $M'$. By transitivity of field degrees, if the result is true for finite galois extensions, it works for all finite separable extensions. To see this, choose $E|M|K_\infty$ finite, Galois. Then by the fundamental theorem of Galois, $E|M$ is galois so $[E : K_\infty] = [E : M][M : K_\infty]$. Since the norm fields also have transitivity of degree, the result will hold.

• We know that $k = k_\infty$ since the $K_n|K$ are totally ramified. (totally ramified means residue degree is 1)

• Choose $L$ such that $M = L_\infty$. Thus $K_n = KK_n$ and $L_n = LK_n$ and

$$\text{Gal}(L/K) = \text{Gal}(LK_n/KK_n) = \text{Gal}(L_n/K_n) = \text{Gal}(M/K_\infty)$$

• Since $L/K$ and $M/K_\infty$ have equivalent Galois groups, there is a bijection between their lattices of intermediate fields by the fundamental theory of Galois.

• First assume that $L|K$ is unramified. Since $K_\infty|K$ is totally ramified, then $L_n|K_n$ is unramified for all $n$.

• Unramified, means the ramification index is 1, so a uniformizer doesn’t split. Thus we can use $\pi_K$ as $\pi_L$, so the extension $E_L/E_K$ has ramification index 1.

• The residue field extension for $E_L/K$ is $k_{L_\infty}/k_{K_\infty}$. Since it is an unramified extension then $[E_L : E_K] = [k_{L_\infty} : k_{K_\infty}]$ and $K'|K$ is unramified so

$$[L : K] = [k_{K'} : k_K].$$
• We know that \( k_{K_\infty} = k_K \) since totally ramified residue field degree is 1. Pass to the limit and get the result since \( k_{L_n} = k_L \).

• Next assume \( L/K \) is totally ramified so that all \( L_n, K_n, L_\infty, K_\infty \) have a common residue field \( k \). Each \( L_n/K_n \) is thus totally ramified of degree \( e = [L_\infty : K_\infty] \).

• Thus for any choice of uniformizers \( \pi_{K_n} \) of \( K_n \) and \( \pi_{L_n} \) of \( K'_n \) we get \( \mathcal{O}_{L_n} = \mathcal{O}_{K_n}[\pi_{L_n}] \). (We proved this a few sections ago.) Also because the extension is totally ramified, \( \pi_{K_n} = \pi_{L_n}^e u_n \) for some unit \( u_n \). WLOG assume that \( (e, p) = 1 \) so that \( L \)

• Choose uniformizers so that for \( n \geq \max(n_K, n_L) \) we have

\[
\pi_{K_{n+1}}^p \equiv \pi_{K_n} \pmod{a_K \mathcal{O}_{K_{n+1}}}, \pi_{L_{n+1}}^p \equiv \pi_{L_n} \pmod{a_K \mathcal{O}_{L_{n+1}}}
\]

If \( (e, p) = 1 \), the result now follows by a theorem of Lang\(^{48}\) about tamely ramified extensions.

\[\square\]

**Result 11.** (Construct a natural isomorphism from \( \text{Gal}(M'/M) \cong \text{Gal}(E_{M'}/E_M) \)).

• Using transitivity like in the last result, we assume that \( M'/M \) is Galois. We view \( \text{Gal} \) as a functor from field extensions to groups.

• Again, we examine the base case. Since \( [E_M : E_{K_\infty}] = [M : K_\infty] \) and since we noted in the last result that \( \text{Gal}(L/K) = \text{Gal}(M/K_\infty) \) we have the identification

\[
\text{Gal}(L/K) \rightarrow \text{Aut}(E_L/E_K) = \text{Aut}(E_M/E_{K_\infty})
\]

\(^{48}\)Lang, Algebraic Number Theory page 53

27
where the target and source have the same size.

- Suppose that $g \in \text{Gal}(L/K)$ acts trivially on $E_L$. (The action here is the natural action preserving $p$-power compatible sequences.) Then the induced action $\text{Gal}(L/K) \ni g : x^{1/p^n} \mapsto g(x)^{1/p^n}$ on $\varphi^{-\infty}(E_M^+)$ is trivial. From stated topological facts, we know that $\varphi^{-\infty}(E_M^+)$ is dense in $R_M$. For $\beta \in R_M$, define $g\beta$ to be $g\alpha$ for $\alpha \in \varphi^{-\infty}(E_M^+)$ such that $\alpha$ is arbitrarily close to $\beta$. Then $g\beta = g\alpha = \alpha \approx \beta$ so that $g$ is trivial on $R_M$. From stated topological facts, we know that if $g$ acts trivially on $R_M$, then $g = 1$. 

\[ \square \]

\[ {\text{Conrad p207, 208}} \]
Epilogue

Proceeding from here in the Fontaine-Wintenberger case we have the following theorem without too much more work:

**Result 12.** (The functor finite extensions of $K_{\infty}$ in $\overline{K} \rightarrow$ finite separable extensions of $E_{K_{\infty}}$ in Frac($R$)

\[ M \rightsquigarrow E_M \]

is an equivalence of Galois categories. □

In Scholze case, we have (2.7 Scholze)

**Result 13.** Let $K$ a perfectoid field. Let $K^{\flat}$ be the tilt of $K$. Then the tilting functor induces an equivalence of categories between the category of finite extensions of $K$ and the category of finite extensions of $K^{\flat}$. □

**Definition 22.** (rank of a valuation, isolated subgroups, nonarchimedean field, Perfectoid field, powerbounded elements)

- The rank of a valuation is the number of isolated subgroups of the image of the valuation.

- A subgroup $H$ of an ordered group $G$ is isolated if $h \in H$, $g \in G$ and $h \leq g \leq 1$ implies $g \in H$.

- A field is **nonarchimedean** if it is a topological field whose topology is induced by a nontrivial valuation of rank 1.

- A **perfectoid field** is a complete nonarchimedean field $K$ of residue characteristic $p > 0$ whose associated rank-1 valuation is nondiscrete, such that the Frobenius is surjective on $K^\circ/p$. 29
- $K^o$ is the set of power bounded elements, i.e. $x$ is power-bounded if $\{x^n|n \geq 0\}$ is bounded by the valuation.

In Kedlaya’s *Relative p-adic Hodge theory, Foundations*, he states that the theorem of Scholze is a generalization of Fontaine-Wintenberger, but that the proofs are very different (page 47).

**Definition 23.** (Tilt) For a better description see (Scholze 2.4, page 10). Let $\omega \in K^\times$ such that $|p| \leq |\omega| < 1$. We denote by $K^b = (\lim_{\leftarrow, \Theta} K^o/\omega)[(\omega^b)^{-1}]$ where $\omega^b$ is an element in $\lim_{\leftarrow, \Theta} K^o/\omega$ with $|(\omega^b)^2| = |\omega|$. Here $^2$ denotes the image under a certain map $\lim_{\leftarrow, \Theta} K^o/\omega \rightarrow K^o$.

**Definition 24.** (Galois category) From (Lenstra - Group Schemes, page 37) Let $C$ be a category and $F$ a covariant functor for $C$ to the category of finite sets. We say that $C$ is a *Galois Category* with *fundamental functor* $F$ if the following six conditions are satisfied

- There is a *terminal object* in $C$, and the *fibred product* of any two objects over a third one exists in $C$.

- *Finite sums* exist in $C$, in particular, an *initial object*, and for any object in $C$ the quotient by a finite group of automorphisms exists.

- Any morphism $u$ in $C$ can be written as $u = u'u''$ where $u''$ is an *epimorphism* and $u'$ a monomorphism, and any monomorphism $u : X \rightarrow Y$ in $C$ is an isomorphism of $X$ with a direct summand of $Y$.

- The functor $F$ transforms terminal objects in terminal objects and commutes with fibred products.
• The functor $F$ commutes with finite sums, transforms epimorphisms in epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms.

• If $u$ is a morphism in $C$, such that $F(u)$ is an isomorphism, then $u$ is an isomorphism.
<table>
<thead>
<tr>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apostol, T.</td>
</tr>
<tr>
<td>Ash, R.</td>
</tr>
<tr>
<td>Berger, L.</td>
</tr>
<tr>
<td>Corry, S.</td>
</tr>
<tr>
<td>Eisenbud, D.</td>
</tr>
<tr>
<td>Evens, L.</td>
</tr>
<tr>
<td>Fesenko, I.</td>
</tr>
<tr>
<td>J.Fontaine, J. Wintenberger</td>
</tr>
<tr>
<td>Lang, S.</td>
</tr>
<tr>
<td>Lang, S.</td>
</tr>
<tr>
<td>Lenstra, E.</td>
</tr>
<tr>
<td>Lenstra, E.</td>
</tr>
<tr>
<td>Milne, J.S.</td>
</tr>
<tr>
<td>Owino,</td>
</tr>
<tr>
<td>Robert, A.</td>
</tr>
<tr>
<td>Scholze, P.</td>
</tr>
<tr>
<td>Serre, J.P.</td>
</tr>
<tr>
<td>Stein, W.</td>
</tr>
<tr>
<td>Stein, W.</td>
</tr>
</tbody>
</table>