Local Fields
Part III Michaelmas 2016-2017

Alexandre Daoud

May 27, 2017

Contents

1 Basic Theory

1.1 Fields

Definition 1.1.1. Let K be a field. An **absolute value** on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that

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

In this case, we refer to K as a **valued** field.

Example 1.1.2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $|z| = \sqrt{z\bar{z}}$.

Remark. An absolute value defines a metric $d(x, y) = |x - y|$ and thus induces a topology on K.

Definition 1.1.3. Let K be a field and $|\cdot|, |\cdot|'$ absoute values on K. We say that $|\cdot|$ and $|\cdot|'$ are **equivalent** if they induce the same topology on K.

Proposition 1.1.4. *Let K be a field and $|\cdot|_1, |\cdot|_2$ absolute valeis on K. Then the following are equivalent*

1. *$|\cdot|_1$ and $\cdot|_2$ are equivalent.*
2. *$|x|_1 \leq 1 \iff |x|_2 \leq 1$ for all $x \in K$.*
3. *There exists $s > 0$ such that $|x|_1 = |x|_2^s$ for all $xinK$.*

Proof.

(1) $\implies$ (2): Suppose that $|\cdot|_1$ and $|\cdot|_2$ are equivalent. Then these absolute values generate the same topology on K so that any sequence that converges to a limit with respect to $|\cdot|_1$ must also converge to the same limit with respect to $|\cdot|_2$. Let $x \in K$ be such that $|x|_1 \leq 1$. Then $|x^n|_1 = |x|_1^n$ and so $\lim_{n\to\infty} |x^n|_1 = 0$. But then we must also have that $\lim_{n\to\infty} |x^n|_2 = 0$. Hence $|x^n|_2 = |x|_2^n < 1$ for all $n \geq 1$ and, in particular, $|x|_2 < 1$.

(2) $\implies$ (3): We first observe that the hypothesis $|x|_1 \leq 1 \iff |x|_2 \leq 1$ implies that $|x|_1 > 1 \iff |x|_2 > 1$.

Now, since $|\cdot|_1$ and $|\cdot|_2$ induce the same topology on K, given $0, 1 \neq a \in K$ there exists an $s > 0$ such that $|a|_1 = |a|_2^s$. We claim that, in fact, for all $x \in K$ we have $|x|_1 = |x|_2^s$. To this end, let $0, 1 \neq x \in K$. Then there exists $t \in \mathbb{R}$ such that $|x|_1 = |a|_1^t$. Now fix $a/b \in \mathbb{Q}$ such that $a/b < t$. Then

$$\begin{aligned} |a|_1^{m/n} < |x|_1 &\implies |a^m|_1 < |x^n|_1 \\ &\implies \left|\frac{a^m}{x^n}\right|_1 < 1 \\ &\implies \left|\frac{a^m}{x^n}\right|_2 < 1 \\ &\implies |a|_2^{m/n} < |x|_2 \end{aligned}$$

Similarly, if $m/n > t$, we can show that $|a|_2^{m/n} > |x|_2$. We thus have

$$|a|_2^{m/n} < |x|_2 < |a|_2^{m/n}$$

Since $|x|_2$ is continuous, the Sandwich Theorem then implies that $|x|_2 = |a|_2^t$. But then

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

<u>(3) $\implies$ (1):</u> Now suppose that there exists $s > 0$ such that for all $x \in K$ we have $|x|_1 = |x|_2^s$. Let $B_1(x, r)$ be the open ball of radius r, centered at x with respect to $|\cdot|_1$ and similarly for $B_2(x, r)$. Then

$$\begin{aligned} B_2(x, r) &= \{ y \in K \mid |x-y|_2 < r \} \\ &= \{ y \in K \mid |x-y|_1^{1/s} < r \} \\ &= \{ y \in K \mid |x-y|_1 < r^s \} \\ &= B_1(x, r^s) \end{aligned}$$

Now let U be an open set of the metric topology on K with respect to $|\cdot|_1$. Fix $u \in U$. We claim that we can excise an open $|\cdot|_2$-ball around u. Indeed, we can always find an $r > 0$ such that $x \in B_1(x, r) \subseteq U$. But by the above calculation, $x \in B_2(x, r^{1/s}) \subseteq U$ and hence U is also open in the metric topology on K with respect to $|\cdot|_2$. By symmetry, we can always excise an open $|\cdot|_1$-ball around any point in an $|\cdot|_2$-open set so that the two metric topologies coincide.

□

Definition 1.1.5. Let $(K, |\cdot|)$ be a valued field. We say that $|\cdot|$ is **non-archimedean** if it satisfies the **strong** triangle inequality $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$. The induced metric is also referred to as non-archimedean and the corresponding **ultrametric** inequality $d(x, z) \leq \max\{d(x, y), d(y, z)\}$. If this is not the case then $|\cdot|$ is said to be **archimedean**.

Proposition 1.1.6. *Let K be a non-archimedean valued field, $x \in K$ and $r \in \mathbb{R}_{>0}$. Then any point in the closed ball around x of radius r, $B[x, r]$ is a centre.*

Proof. Fix a $z \in B[x, r]$ and let $y \in B[z, r]$. Then

$$|x-y| = |x-z+z-y| \leq \max\{|x-z|, |z-y|\} \leq \max\{r, r\} = r$$

and so $y \in B[x, r]$ whence $B[z, r] \subseteq B[x, r]$. By symmetry we then have that $B[x, r] = B[z, r]$. □

Proposition 1.1.7. *Let K be a non-archimedean valued field. Then*

$$\mathcal{O} = \{ x \mid |x| \leq 1 \}$$

is an open subring of K called the ***valuation ring*** *of K with unit group given by $\mathcal{O}^\times = \{ x \mid |x| = 1 \}$. Furthermore, given any $r \in (0,1]$ the sets $\{ x \mid |x| < r \}$ and $\{ x \mid |x| \leq r \}$ are open ideals of $\mathcal{O}$.*

Proof. It follows immediately from Proposition 1.1.6 that we can can always excise an open ball around any point of $\mathcal{O}$ whence $\mathcal{O}$ and the other sets are open. We now show that $\mathcal{O}$ is a subring of K. It is clear that $|1| = |-1| = 1$ whence $1, -1 \in \mathcal{O}$. Now suppose that $x, y \in \mathcal{O}$. Then $|x+y| \leq \max\{|x|, |y|\} \leq 1$ which implies that $x, y \in \mathcal{O}$. Similarly, $|xy| = |x||y| \leq 1$ and so also $xy \in \mathcal{O}$. Hence $\mathcal{O}$ is a subring of K.

Now suppose that $x \neq 0$. Then

$$x \in \mathcal{O}^\times \iff |x|, |x|^{-1} \leq 1 \iff |x| = 1$$

and so $\mathcal{O}^\times = \{ x \mid |x| = 1 \}$. The fact that the other sets are ideals are checked by a similar process. □

Proposition 1.1.8. *Let K be a non-archimedean valued field and $(x_n) \subseteq K$ a sequence. If $x_n - x_{n-1} \to 0$ then (x_n) is Cauchy. Furthermore, if K is complete then*

1. *(x_n) converges.*
2. *if $x_n \to 0$ then $\sum_{n=0}^{\infty} x_n$ converges.*

Proof. Fix $\varepsilon > 0$ and suppose there exists $N \in \mathbb{N}$ such that $|x_n - x_n - x_{n-1}| < \varepsilon$ for all $n \geq N$. Choose $m \geq n$. Then

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

whence (x_n) is Cauchy. The rest follows immediately. □

1.2 Rings

Definition 1.2.1. Let $R \subseteq S$ be rings. We say that $s \in S$ is **integral** over R if there exists a monic $f(X) \in R[X]$ such that $f(s) = 0$.

Remark. Recall the following from linear algebra. Let $A = (a_{ij}) \in M_{n \times n}(R)$. The adjoint matrix $A^* = (a^*_{ij})$ of A is defined by $a^*_{ij} = (-1)^{ij} \det(A_{ij})$ where A_{ij} is the $(n-1) \times (n-1)$ matrix obtained from A by deleting the i^{th} column and j^{th} row. Then $A^*A = AA^* = \det(A)\mathbb{1}_n$.

Proposition 1.2.2. *Let $R \subseteq S$ be rings. Then $s_1, \ldots, s_n \in S$ are integral over R if and only if $R[s_1, \ldots, s_n] \subseteq S$ is a finitely generated R-module.*

Proof. First suppose that $s_1, \ldots, s_n$ are all integral over R. Note that

$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \ldots, s_n] \subseteq S$$

with s_i integral over $R[s_1, \ldots, s_{i-1}]$. By induction, it thus suffices to prove the case where $n = 1$. Let $s = s_1$ and fix some monic $f(X) \in R[X]$ such that $f(s) = 0$. Given $g(X) \in R[X]$ the division algorithim for polynomials implies that there exists $q, r \in R[X]$ such that $g(X) = f(X)q(X) + r(X)$ where $\deg r < \deg f$. Observe that $g(s) = f(s)q(s) + r(s) = r(s)$ whence $1, s, \ldots, s^{\deg(f)-1}$ generate $R[s]$ as an R-module.

Now assume that $R[s_1, \ldots, s_n]$ is a finitely generated R-module and fix some generators $t_1, \ldots, t_d \in R[s_1, \ldots, s_n]$. Let $b \in R[s_1, \ldots, s_n]$. Then there exists some $a_{ij} \in R$ such that

$$bt_i = \sum_{j=1}^{d} a_{ij} t_j$$

Letting $A = (a_{ij})$, we then have that $(bI - A)t = 0$. Multiplying through by $(bI - A)^*$ yields $\det(bI - A)t_j = 0$ for all j. Now, we can always find $c_j \in R$ such that $1 = \sum_{j=1}^{d} c_j t_j$. Multiplying this by $\det(bI - a)$ we get

$$\det(bI - A) = \sum_{j=1}^{d} \det(bI - A) c_j t_j$$

This is just equal to 0 and is monic when expanding out the definition of $\det(XI - A)$ so b is integral over R. □

Corollary 1.2.3. *Let R and S be rings. Suppose that $s_1, s_2 \in S$ are integral over R. Then $s_1 + s_2, s_1 s_2$ are also integral over R. In particular, the set of all elements in S that are integral over R is a ring called the **integral closure** of R in S.*

Proof. Suppose that $s_1, s_2 \in S$ are integral over R. Then by the Proposition, $R[s_1, s_2]$ is a finitely generated R-module. Using the Proposition in the opposite direction, it then follows that $s_1 + s_2, s_1 s_2$ are integral over R. □

1.3 Topological Rings

Definition 1.3.1. Let R be a ring and τ a topology of R. We say that τ is a **ring topology** if R's addition and multiplication operations are continuous maps. In this case, we refer to R as a **topological** ring.

Example 1.3.2. Let K be a valued field. Then K is a topological ring with the topology induced from the metric coming from the absolute value.

Definition 1.3.3. Let R be a ring and $I \triangleleft R$ an ideal. A subset $U \subseteq R$ is called I-adically open if for all $x \in U$ there exists an $n \geq 1$ such that $x + I^n \subseteq U$.

Proposition 1.3.4. *Let R be a ring and $I \triangleleft R$ be an ideal. The set of all I-adically open sets of R forms a topology on R called the **I-adic topology**.*

Proof. It is vacuously true that $\varnothing$ is I-adically open. It is also immediately obvious from the definition that R is I-adically open. Let $U, V \subseteq R$ be I-adically open subsets. Then it is immediate that their union is I-adically open. To see that their intersection is also open, fix an $x \in U \cap V$. Then there exists $m, n \geq 1$ such that $x + I^n \subseteq U$ and $x + I^m \subseteq V$. It follows that $x + I^{\max\{m,n\}} \subseteq U \cap V$. □

Proposition 1.3.5. *Let R be a ring and $I \triangleleft R$ an ideal. Then the I-adic topology on R is a ring topology.*

Proof. Fix $(x, y) \in R \times R$. We want to show that the map

$$\begin{aligned} + : R \times R &\to R \\ (a, b) &\mapsto a + b \end{aligned}$$

is continuous at (x, y). This amounts to showing that for any open neighbourhood W of $x + y$ in R, there exists an open neighbourhood $U \times V$ of (x, y) such that $f(U \times V) \subseteq W$. By the definition of the I-adic topology, it suffices to prove this when W is of the form $x + y + I^m$ for some $m \geq 1$. We claim that $U = x + I^m$ and $y + I^m$ define the required neighbourhood (U, V) of (x, y). Given any $(a, b) \in U \times V$, we have that $a + b$ is a sum of x, y and some multiples of elements in I^m which is exactly what it means to be an element of $x + y + I^m$. Hence $+$ is continuous. A similar argument applies to multiplication whence the I-adic topology is a ring topology. □

Definition 1.3.6. Let $R_1, R_2, \ldots$ be a sequence of topological rings equipped with continuous homomorphisms $f_n : R_{n+1} \to R_n$ for all $n \geq 1$. We define the **inverse limit** of the R_i to be the ring

$$\varprojlim_n R_n = \left\{ (x_n) \in \prod_n R_n \;\middle|\; f_n(x_{n+1}) = x_n \forall n \geq 1 \right\}$$

together with coordinate-wise operations. The inverse limit ring has the subspace topology induced from the product topology on $\prod_n R_n$.

Proposition 1.3.7. *Let $R_1, R_2, \ldots$ be a sequence of topological rings equipped with continuous homomorphisms $f_n : R_{n+1} \to R_n$ for all $n \geq 1$. Then the inverse limit topology on $\varprojlim_n R_n$ is a ring topology.*

Proof. We want to show that the mapping

$$+ : (\varprojlim_n R_n) \times (\varprojlim_n R_n) \to \varprojlim_n R_n$$

is continuous in the inverse limit topology. Since the inverse limit topology is just the subspace topology induced by the product topology, it suffices to show that

$$+ : \left(\prod_n R_n\right) \times \left(\prod_n R_n\right) \to \prod_n R_n$$

is continuous in the product topology. Observe that $+$ is continuous if and only if $+_m : \prod_n R_n \times \prod_n R_n \to R_m$ is continuous for all m. We note that $\prod_n R_n \times \prod_n R_n = \prod_n (R_n \times R_n)$ and that we have a continuous projection mapping $\pi_m : \prod_n (R_n \times R_n) \to R_m$ for each m. Since R_m is a topological ring, the addition mapping $\varphi_m : R_m \times R_m \to R_m$ is continuous whence $+_m = \pi_m \circ \varphi_m$ is continuous. □

Definition 1.3.8. Let R be a ring and $I \triangleleft R$ an ideal. We define the **I-adic completion** of R to be the ring

$$\hat{R}_I = \varprojlim_n R/I^n$$

Define the continuous ring homomorphism

$$\begin{aligned} \nu : R &\to \varprojlim_n R/I^n \\ r &\mapsto (r \pmod{I^n})_n \end{aligned}$$

We say that R is **I-adically complete** if ν is a bijection. Furthermore, if $I = xR$ for some $x \in R$, we shall often refer to the I-adic topology as the **x-adic** topology.

1.4 The p-adic numbers

Let p denote any prime number for the rest of this course.

Definition 1.4.1. Let $x \in \mathbb{Q} \setminus \{ 0 \}$ and write it in the form $x = p^n a/b$ where $n, a \in \mathbb{Z}, b \in \mathbb{Z} \setminus_{>0}$ and $(a, p) = (b, p) = 1$. We define the **p-adic** absolute value on $\mathbb{Q}$ to be the function

$$| \cdot |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$$

given by

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{if } x = p^n \frac{a}{b} \end{cases}$$

Proposition 1.4.2. *The p-adic absolute value is a non-archimedean absolute value on* $\mathbb{Q}$*.*

Proof. By construction, $|x|_p = 0$ if and only if $x = 0$. Now let $x = p^n a/b, y = p^m c/d \in \mathbb{Q}$ be non-zero with $m \geq n$. Then

$$|xy|_p = \left| p^{m+n} \frac{ac}{bd} \right|_p = p^{-m-n} = p^{-m} p^{-n} = |x|_p |y|_p$$

and

$$|x + y|_p = \left| p^n \frac{ad + p^{m-n} cb}{bd} \right| \leq p^{-n} = \max\{|x|_p, |y|_p\}$$

□

Definition 1.4.3. We define the **p-adic numbers**, denoted $\mathbb{Q}_p$, to be the completion of $\mathbb{Q}$ with respect to $| \cdot |_p$. The valuation ring

$$\mathbb{Z}_p = \{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \}$$

is called the **p-adic integers**.

Proposition 1.4.4. $\mathbb{Z}_p$ *is the closure of* $\mathbb{Z}$ *in* $\mathbb{Q}_p$*.*

Proof. Fix a non-zero $x \in \mathbb{Z}$ such that $x = p^n a$ with $n \geq 0$ and $(a, p) = 1$. Then $|x|_p \leq 1$ so $\mathbb{Z} \subseteq \mathbb{Z}_p$. Now, by definition, the set

$$\mathbb{Z}_{(p)} = \{ x \in \mathbb{Q} \mid |x|_p \leq 1 \}$$

is dense in $\mathbb{Z}_p$. Hence, it suffices to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. Fix some non-zero $x \in \mathbb{Q} \setminus \{ 0 \}$ with $x = p^n a/b$. It suffices to find a sequence $(x_i) \in \mathbb{Z}$ such that $x_i \to 1/b$ as $i \to \infty$. We can then multiply through by ap^n to achieve a sequence that converges to x. Now, $(b, p) = 1$ implies that there exists $x_i, y_i \in \mathbb{Z}$ such that

$$bx_i + p^i y_i = 1$$

for all $i \geq 1$. We claim that x_i is the desired sequence. We have that

$$\left| x_i - \frac{1}{b} \right|_p = \left| \frac{1}{b} \right|_p |bx_i - 1|_p = |p^i y_i|_p \leq p^{-i} \to 0$$

as desired. □

Proposition 1.4.5. *The non-zero ideals of* $\mathbb{Z}_p$ *are* $p^n\mathbb{Z}_p$ *for* $n \geq 0$*. Furthermore,* $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$*,*

Proof. Fix a non-zero ideal $I \lhd \mathbb{Z}_p$ and choose $x \in I$ such that $|x|_p$ is maximal (we can always do this since the absolute value is discrete on $\mathbb{Z}_p$). Let $y \in I$. By construction, $|y|_p \leq |x|_p$ so $|yx^{-1}|_p \leq 1$ and so $yx^{-1} \in \mathbb{Z}_p$. Then $y = (yx^{-1})x \in x\mathbb{Z}_p$ whence $I = x\mathbb{Z}_p$. It follows immediately that if $|x|_p = p^{-n}$ then $I = (p^n)$.

Now consider the mapping

$$f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$$

Observe that $p^n\mathbb{Z}_p = \{ x \mid |x|_p \leq p^{-n} \}$ and so

$$\ker f_n = \{ x \in \mathbb{Z} \mid |x|_p \leq p^{-n} \} = p^n\mathbb{Z}$$

Furthermore, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and so every equivalence class in $\mathbb{Z}_p/p^n\mathbb{Z}_p$ will contain the image of an integer whence f_n is surjective. f_n thus induces an isomorphism

$$\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$$

□

Corollary 1.4.6. $\mathbb{Z}_p$ *is a PID with a unique prime element* p *(up to units).*

Proposition 1.4.7. *The topology on* $\mathbb{Z}$ *induced by* $|\cdot|_p$ *is the* p*-adic topology.*

Proof. Fix a set $U \subseteq \mathbb{Z}$. By definition, U is open with respect to $|\cdot|_p$ if and only if for all $x \in U$, there exists $n \in \mathbb{N}$ such that $\{ y \in \mathbb{Z} \mid |y - x|_p \leq p^{-n} \} \subseteq U$. On the other hand, U is open in the p-adic topology if and only if for all $x \in U$, there exists $n \in \mathbb{N}$ such that $x + p^N\mathbb{Z} \subseteq U$. But $\{ y \in \mathbb{Z} \mid |y - x|_p \leq p^{-n} \} = x + p^n\mathbb{Z}$ so these topologies are equivalent (in fact, they are equal). □

Proposition 1.4.8. $\mathbb{Z}_p$ *is* p*-adically complete and is isomorphic to the* p*-adic completion of* $\mathbb{Z}$*.*

Proof. The second assertion follows directly from the first via the proof of Proposition 1.4.5. We thus need to show that the ring homomorphism

$$\nu : \mathbb{Z}_p \to \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p$$

is bijective. We have that

$$x \in \ker \nu \iff x \in p^n\mathbb{Z}_p \forall n \iff |x|_p \leq p^{-n} \forall n \iff |x|_p = 0 \iff x = 0$$

and so ν is injective. Now let $(z_n) \in \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p$. Define $a_i \in \{ 0, 1, \ldots, p-1 \}$ recursively such that $x_n = \sum_{i=0}^{n-1} a_i p^i$ is the unique representation of z_n in the set $0, 1, \ldots, p^{n-1}$. Then $x = \sum_{i=0}^{\infty} a_i p^i$ exists in $\mathbb{Z}_p$ and $x \equiv x_n \equiv z_n \pmod{p^n}$ for all $n \geq 0$ and so $v(x) = z_n$ whence ν is surjective. □

Corollary 1.4.9. *Every* $a \in \mathbb{Z}_p$ *has a unique expansion* $a = \sum_{i=0}^{\infty} a_i p^i$ *with* $a \in \{ 0, \ldots, p-1 \}$*.*

2 Valued fields

2.1 Hensel's Lemma

Definition 2.1.1. Let K be a field. We define a **valuation** on K to be a function $v : K \to \mathbb{R} \cup \{\infty\}$ such that

1. $v(x) = \infty \iff x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x + y) \geq \min\{v(x), v(y)\}$

for all $x, y \in K$. Here we are using the conventions that $r + \infty = \infty$ and $r \leq \infty$ for all $r \in \mathbb{R} \cup \{\infty\}$.

Remark. Let K be a valued field with valuation v. Then $|x| = c^{-v(x)}$ defines an absolute value for any $c \in \mathbb{R}_{\geq 1}$. Conversely, if $|\cdot|$ is an absolute value on K then $v(x) = -\log|x|$ is a valuation on K.

Example 2.1.2. Let $x \in \mathbb{Q}_p$ and define $v_p(x) = -\log_p |x|_p$. Then v_p is a valuation on $\mathbb{Q}$ and if $x \in \mathbb{Z}_p \backslash 0$ then $v_p(x) = n$ if and only if $p^n \mid\mid x$.

Example 2.1.3. Let K be a field and consider the field of formal Laurent series over K

$$K((T)) = \left\{ \sum_{i>>-\infty}^{\infty} a_i T^i \;\middle|\; a_i \in K \right\}$$

Then $v\left(\sum a_i T^i\right) = \min\{ i \in \mathbb{N} \mid a_i \neq 0 \}$ is a valuation of $K((T))$.

Definition 2.1.4. Let K be a valued field with absolute value $|v|$. We write $\mathcal{O}_K = \{ x \in K \mid |x| \leq 1 \}$ for the valuation ring of K, $\mathfrak{m}_K = \{ x \in K \mid |x| = 1 \}$ for its unique maximal ideal and $\mathbb{F}_K = \mathcal{O}_K / \mathfrak{m}_k$ for its residue field. We say that K is a complete valued field if it is complete with respect to the $\mathfrak{m}_K$-adic topology. Moreover, if $f(X) \in K[X]$ is a polynomial then we say F is **primitive** if $\max_i |a_i| = 1$.

Theorem 2.1.5 (Hensel's Lemma)**.** *Let K be a complete valued field . Suppose that $F(X) \in K[X]$ is a primitive polynomial with reduction $f(X) \equiv F(X) \pmod{\mathfrak{m}_K} \in K[X]$. If $f(X)$ admits a factorisation $f(X) = g(X)h(X)$ with g and h coprime then $F(X)$ admits a factorisation $F(X) = G(X)H(X)$ satisfying $G(X), H(X) \in \mathcal{O}_K[X]$, $G(X) \equiv g(x) \pmod{\mathfrak{m}_K}$, $H(X) \equiv h(x) \pmod{\mathfrak{m}_K}$ and $\deg g = \deg G$*

Proof. Let $d = \deg F$ and $m = \deg g$ so that $\deg h \leq d - m$. Let $G_0, H_0 \in \mathcal{O}_K[X]$ be lifts of g, h such that $\deg G_0 = \deg g$ and $\deg H_0 \leq d - m$. Since g and h are coprime, the division algorithm for polynomials implies that there exists $A, B \in \mathcal{O}_K[X]$ such that

$$AG_0 + BH_0 \equiv 1 \pmod{\mathfrak{m}_K}$$

Fix $\pi \in \mathfrak{m}_K$ such that

$$F - G_0 H_0 \equiv AG_0 + BH_0 - 1 \pmod{\pi}$$

We claim that, by induction, we can construct sequences of polynomials $G_n = G_0 + \sum_{i=1}^n \pi^i P_i$ and $H_n = H_0 + \sum_{i=1}^n \pi Q_i$ such that for all $n \geq 1$ we have $F \equiv G_{n-1} H_{n-1} \pmod{\pi^n}$ with each $P_i, Q_i \in \mathcal{O}_K[X]$ satisfying $\deg P_i < m$ and $\deg Q_i \leq d - m$. We will then be able to pass to the limit $n \to \infty$ to obtain the desired G and H.

We now proceed by induction. First assume $n = 1$. Then it is clear that the G_0 and H_0 we have constructed satisfy the hypotheses. Now assume that we have constructed G_{n-1} and H_{n-1}. We will construct polynomials $P_n, Q_n \in \mathcal{O}_K[X]$ such that $\deg P_i < m$ and $\deg Q_i \leq d - m$ so that if we set $G_n = G_{n-1} + \pi^n P_n$ and $H_n = H_{n-1} + \pi^n Q_n$ then we have $F \equiv G_n H_n \pmod{\pi^{n+1}}$. The latter requirement is equivalent to

$$F - G_{n-1}H_{n-1} \equiv \pi^n (G_{n-1}Q_n + H_{n-1}P_n) \pmod{\pi^{n+1}}$$

Rearranging and dividing by π^n yields

$$G_0 Q_n + H_0 P_n \equiv G_{n-1}Q_n + H_{n-1}P_n \equiv \frac{1}{\pi^n}(F - G_{n-1}H_{n-1}) \pmod{\pi}$$

Now, $AG_0 + BH_0 \equiv 1 \pmod{\pi}$ implies that $F_n \equiv AG_0F_n + BH_0F_n \pmod{\pi}$ where $F_n = \pi^{-n}(F - G_{n-1}H_{n-1})$. Since the leading coefficient of G_0 is a unit, we can use the division algorithm to write $BF_n = QG_0 + P_n$ with $\deg P_n < \deg G_0, P_n \in \mathcal{O}_K[X]$. Then

$$F_n \equiv AG_0F_n + H_0(P_n + Q_nQ_0) \equiv G_0(AF_n + H_0Q) + H_0P_n \equiv F_n \pmod{\pi}$$

We can then define Q_n to be the polynomial given by ignoring all the coefficients of $AF_n + H_0Q$ that are divisible by π and we are done. □

Corollary 2.1.6. *Let K be a complete valued field and $F(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ a polynomial. If $a_0 a_n \neq 0$ and F is irreducible then for all $1 \leq i \leq n$ we have $|a_i| \leq \max\{|a_0|, |a_n|\}$.*

Proof. After scaling the coefficients of F we may assume, without loss of generality, that F is primitive. Let $r \in K$ be minimal such that $|a_r| = 1$. Then

$$F(X) = X^r(a_r + a_{r+1}X + \cdots + a_n X^{n-r}) \pmod{\mathfrak{m}}$$

Suppose that $\max\{|a_0|, |a_n|\} \neq 1$. Then $0 < r < n$ and the above congruence lifts to a non-trivial factorisation of G by Hensel's Lemma. But F is irreducible and so we must have that $\max\{|a_0|, |a_n|\} = 1$. □

Corollary 2.1.7. *Let K be a complete valued field and $F \in \mathcal{O}_K[X]$ monic. If $F \pmod{\mathfrak{m}_K}$ has a simple root $\overline{\alpha} \in \mathbb{F}_K$ then F has a unique simple root $\alpha \in \mathcal{O}_K$ lifting $\overline{\alpha}$.*

Corollary 2.1.8. *$\mathbb{Z}_p$ contains all $(p-1)^{th}$ roots of unity.*

Proof. First observe that $\mathbb{Q}_p$ is complete with respect to the p-adic topology. Now consider the polynomial $X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Then this polynomial is primitive and its reduction splits into distinct linear factors over $\mathbb{F}_p[X]$. We may lift these simple roots to simple roots in $\mathbb{Z}_p$ via Hensel's Lemma. □

Remark. Let K be a non-archimedean valued field. Observe that if $|x| > |y|$ then $|x + y| = |x|$. Indeed, $|x_y| \leq \max\{|x|, |y|\} = |x|$ and $|x| \leq \max\{|x + y|, |y|\} = |x + y|$. More generally, if $x = \sum_{i=0}^{\infty} x_i$ and the $|x_i|$ are distinct then $|x| = \max_i |x_i|$.

2.2 Extension of Absolute Values

Definition 2.2.1. Let K be a non-archimedean valued field and V a K-vector space. A **norm** on V is a function $||\cdot|| : V \to \mathbb{R}_{\geq 0}$ such that

1. $||x|| = 0 \iff x = 0$
2. $||\lambda x|| = |\lambda|\,||x||$ for all $\lambda \in K$ and $x \in V$
3. $||x + y|| \leq \max\{||x||, ||y||\}$ for all $x, y \in V$

Moreover, we say that two norms $||\cdot||_1$ and $||\cdot||_2$ are **equivalent** if they induce the same topology on V. In other words, there exists $C, D > 0$ such that $C||x||_1 \leq ||x||_2 \leq D||x||_1$ for all $x \in V$.

Proposition 2.2.2. *Let K be a complete valued field and V a finite dimensional K-vector space. Given a K-basis $x_1, \ldots, x_n$ of V let any element $x \in V$ be written as $x = \sum_{i=1}^n a_i x_i$. Then $||x||_{\max} = \max_i |a_i|$ defines a norm on V and V is complete with respect to this norm. Moreover, if $||\cdot||$ is any other norm on V then $||\cdot||$ is equivalent to $||\cdot||_{\max}$ and hence V is complete with respect to $||\cdot||$.*

Proof. We first check that x is a norm. Indeed, we have

$$||x||_{\max} = 0 \iff \max_i |a_i| = 0 \iff a_i = 0 \text{ for all } i \iff x = 0$$

Furthermore

$$||\lambda x||_{\max} = \max_i |\lambda a_i| = |\lambda| \max_i |a_i| = |\lambda|\,||x||_{\max}$$

Finally,

$$\begin{aligned} ||x + y||_{\max} = \max_i |a_i + b_i| \leq \max_i(\max\{|a_i|, |b_i|\}) &\leq \max\{\max_i |a_i|, \max_i |b_i|\} \\ &= \max\{||x||_{\max}, ||y||_{\max}\} \end{aligned}$$

It is readily verified that V is complete with respect to K. Indeed, given a Cauchy sequence of vectors in V, we may take the limit of the coordinate-wise sequences which exist since K is complete. The vector whose coordinates are such limits is exactly the limit of the original Cauchy sequence.

Now let $||\cdot||$ be any other norm on V. We need to exhibit $C, D > 0$ such that $C||x||_{\max} \leq ||x|| \leq D||x||_{\max}$ for all $x \in V$. Let $D = \max_i(||x_i||)$. Then

$$||x|| = \left|\left|\sum_{i=1}^n x_i a_i\right|\right| \leq \max_i(|a_i, ||x_i||) \leq (\max_i |a_i|)(\max_i ||x_i||) = D||x||_{\max}$$

We find C by induction on $n = \dim V$. Suppose $n = 1$. Then

$$||x|| = ||a_1 x_1|| = |a_1|\,||x_1|| = ||x||_{\max}||x_1||$$

so in this case we have $C = ||x_1||$. Now suppose that $n \geq 2$. Let

$$V_i = Kx_1 \oplus \ldots Kx_{i-1} \oplus Kx_{i+1} \oplus \cdots \oplus kx_n$$

By the induction hypothesis, each V_i is complete with respect to the restriction of $||\cdot||$ to V_i. Hence V_i is closed in V and so, in particular, $W = \cup_{i=1}^n (x_i + V_i)$ is closed in V. By the definition of V_i, W does not contain 0. It then follows that there exists $C > 0$ such that if $x \in W$ then $||x|| \geq C$. We claim that this C satisfies the claim.

Fix $0 \neq x = \sum_{i=1}^n a_i x_i \in V$ and choose an index r such that $|a_r| = ||x||_{\max}$. Then

$$||x||_{\max}^{-1}||x|| = ||a_r^{-1}x|| = \left|\left|\frac{a_1}{a_r}x_1 + \cdots + \frac{a_{r-1}}{a_r}x_{r-1} + x_r + \frac{a_{r+1}}{a_r}x_{r+1} + \cdots + \frac{a_n}{a_r}x_n\right|\right|$$
$$\geq C$$

since this last vector is an element of $x_r + V_r$. □

Lemma 2.2.3. *Let K be a valued field. Then $\mathcal{O}_K$ is integrally closed in K.*

Proof. Let $x \in K$ be such that $|x| > 1$. Now let $a_0, \ldots, a_{n-1 \in \mathcal{O}_K}$. Then

$$|a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}| \leq \max_i |a_i x^i| \leq \max_i |x^i| = |x^{n-1} \leq |x^n|$$

Now suppose that x is integral over $\mathcal{O}_K$ so that we have

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

Then we would have that

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

so that $|x^n| = |a_{n-1}x^{n-1} + \cdots + a_0|$ which is a contradiction. Hence x cannot be integral over $\mathcal{O}_K$. □

Lemma 2.2.4. *Let K be a field and $|\cdot| : K \to \mathbb{R}_{\geq 0}$ a function satisfying the first two axioms of an absolute value. Then $|\cdot|$ is a non-archimedean absolute value on K if and only if $|x| < 1$ implies that $|x + 1| < 1$ for all $x \in K$.*

Proof. First suppose that $|\cdot|$ is a non-archimedean absolute value on K. Suppose that $|x| < 1$. Then $|x + 1| \leq \max\{|x|, 1\} < 1$. Conversely, suppose that $|x + 1| < 1$. Then $|x| = |x + 1 - 1| \leq \max\{|x + 1|, 1\} < 1$ as desired.

Now suppose that $|x| < 1$ implies that $|x + 1| < 1$ for all $x \in K$. We need to show that for all $x, y \in K$ we have $|x + y| \leq \max\{|x|, |y|\}$. Suppose, without loss of generality, that $|x| \leq |y|$. Then $|x/y| < 1$ so that $|x/y + 1| < 1$ whence $|x + y| \leq |y|$. Hence, clearly, $|x + y| \leq \max\{|x|, |y|\}$. □

Theorem 2.2.5. *Let K be a complete valued field and L/K a finite extension. Then $|\cdot|$ extends uniquely to an absolute value on L given by*

$$|\alpha|_L = |\,\mathbf{N}_{L/K}(\alpha)|^{1/[L:K]}$$

Moreover, L is complete with respect to $|\alpha|_L$.

Proof. We first show that if such an absolute value $|\cdot|_L$ on L were to exist then it is unique and L is complete with respect to $|\cdot|_L$. Indeed, suppose that $|\cdot|_L'$ is another absolute value on L extending L. Then we can view $|\cdot|_L$ and $|\cdot|_L'$ as norms on the finite dimensional K-vector space L. By Proposition 2.2.2, these norms are equivalent and so generate the same topology on L with respect to which L is complete. Going back to the viewpoint of absolute values, Proposition 1.1.4 then implies that there exists $s > 0$ such that $|\cdot|_L = |\cdot|_L'^{\,s}$. But $|\cdot|_L|_K = |\cdot|_L'|_K$ so we must have that $s = 1$.

We now show that the given formula indeed defines an absolute value on L. First note that, given $\alpha \in K$, we have

$$|\alpha|_L = 0 \iff \mathbf{N}_{L/K}(\alpha) = 0 \iff \alpha = 0$$

Moreover, given $\alpha, \beta \in K$ we have

$$\begin{aligned} |\alpha\beta|_L = |\,\mathbf{N}_{L/K}(\alpha\beta)|^{1/[L:K]} = |\,\mathbf{N}_{L/K}(\alpha)\,\mathbf{N}_{L/K}(\beta)|^{1/[L:K]} &= |\,\mathbf{N}_{L/K}(\alpha)|^{1/[L:K]}|\,\mathbf{N}_{L/K}(\beta)|^{[L:K]} \\ &= |\alpha|_L|\beta|_L \end{aligned}$$

It remains to show that $|\cdot|_L$ satisfies the ultrametric inequality. Note that by Lemma 2.2.4, it suffices to show that for all $\alpha \in L$ we have $|\alpha|_L < 1$ if and ony if $|\alpha + 1|_L < 1$.

To this end, we first observe that

$$\{\, \alpha \in L \mid |\alpha|_L \leq 1 \,\} = \{\, \alpha \in L \mid \mathbf{N}_{L/K}(\alpha) \in \mathcal{O}_K \,\}$$

We claim that this set is the integral closure of $\mathcal{O}_K$ in L. If this were indeed the case then we would have that $|\alpha + 1|_L \leq 1$ since the integral closure is a ring.

Hence fix $0 \neq \alpha \in L$ such that $\mathbf{N}_{L/K}(\alpha) \in \mathcal{O}_K$ and let $f(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n \in K[X]$ be the minimal polynomial of α over K. By Corollary 2.1.6, we know that for all i we have $|a_i| \leq \max\{|a_0|, 1\}$. By the properties of the field norm, there exists an $m \geq 1$ such that $\mathbf{N}_{L/K}(\alpha) = \pm a_0^m$. Then

$$|a_i| \leq \max\{|a_0|, 1\} = \max\{|\,\mathbf{N}_{L/K}(\alpha)|^{1/m}, 1\} = 1$$

and so $f(X) \in \mathcal{O}_K[X]$ and so α is integral over $\mathcal{O}_K$.

Conversely, suppose that $\alpha \in L$ is integral over $\mathcal{O}_K$. We need to show that $\mathbf{N}_{L/K}(\alpha) \in \mathcal{O}_K$. Indeed, fix an algebraic closure $\bar{K}$ of K and let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of L into $\bar{K}$ where $n = [L : K]$. Then

$$\mathbf{N}_{L/K}(\alpha) = \left(\prod_{i=1}^{n} \sigma_i(\alpha) \right)^d$$

for some $d \in \mathbb{N}_{\geq 1}$. But each $\sigma_i(\alpha)$ is integral over $\mathcal{O}_K$ since α is and so $\mathbf{N}_{L/K}(\alpha)$ is integral over $\mathcal{O}_K$ as claimed. □

Corollary 2.2.6. *Let K be a complete valued field and L/K a finite extension of K admitting a unique extension $|\cdot|_L$ extending $|\cdot|$. Then $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.*

Corollary 2.2.7. *Let K be a complete valued field and L/K an algebraic extension of K. Then $|\cdot|$ extends uniquely to an absolute value on L.*

Corollary 2.2.8. *Let K be a complete valued field and L/K a finite extension of K. Then any $\sigma \in \mathrm{Aut}(L/K)$ acts as an isometry of the unique extension of $|\cdot|$ to L.*

Proof. Let $|\cdot|_L$ be the unique extension of $|\cdot|$ to L. Then it is easy to see that $\alpha \mapsto |\sigma(\alpha)|_L$ is also an absolute value on L which extends $|\cdot|$ to L. Hence $|\sigma(\alpha)|_L = |\alpha|_L$ for all $\alpha \in L$ whence σ is an isometry of $|\cdot|_L$. □

2.3 Newton Polygons

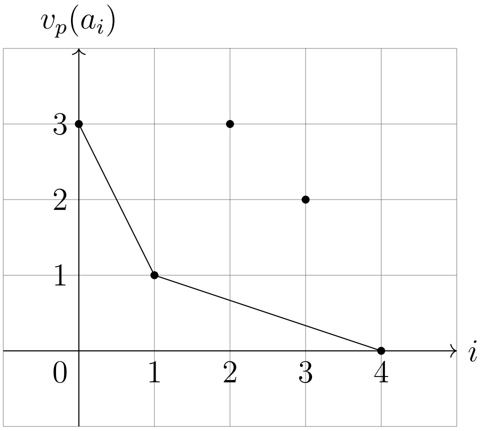
Definition 2.3.1. Let $S \subseteq \mathbb{R}^2$ be a subset. We say that S is **lower convex** if S is convex and $(x, y) \in S$ implies that $(x, z) \in S$ for all $z \geq y$. Moreover, given any subset $T \subseteq \mathbb{R}^2$, we define the **lower convex hull** of T to be the minimal lower convex superset $S \supseteq T$ of T. Explicitly, the lower convex hull of T is given by the intersection of all lower convex sets containing T.

Definition 2.3.2. Let K be a non-archimidean valued field with valuation v and $f(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ a polynomial. We define the **Newton polygon** of f to be the lower convex hull of the set

$$\{\,(i, v(a_i)) \mid 0 \leq i \leq n \text{ where } a_i \neq 0\,\}$$

We will usually identify the Newton polygon of f with the line in $\mathbb{R}^2$ that bounds the lower convex hull from below as in the following example.

Example 2.3.3. Consider $\mathbb{Q}_p$ with the p-adic valuation v_p. Let $f(X) = X^4 + p^2X^3 - p^3X^2 + pX + p^3$. Then the Newton polygon of $f(X)$ is



Definition 2.3.4. Let K be a non-archimidean valued field with valuation v and $f(X) \in K[X]$. Let N be the Newton polygon of f. We make the following definitions:

1. We call the vertices of N the **break points**.

2. We call the edges of N the **line segments**.

3. We call the horizontal length of a line segment its **multiplicity**.

Theorem 2.3.5. *Let K be a complete non-archimidean valued field with valuation v and $f(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ a polynomial. Let L be a splitting field of f over K and let w be the unique extension of v to L. If $(r, v(a_r)) \to (s, v(a_s))$ is a line segment of the Newton polygon of f with slope $-m$ then f has $s - r$ roots in L with valuation m.*

Proof. Without loss of generality, we may assume that $a_n = 1$. Indeed, dividing $f(X)$ through by a_n only shifts the Newton polygon of $f(X)$ vertically and so does not change any of its structure. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(X)$ in L and label them so that

$$\begin{aligned} w(\alpha_1) = \cdots = w(\alpha_{s_1}) &= m_1 \\ w(\alpha_{s_1+1}) = \cdots = w(\alpha_{s_2}) &= m_2 \\ &\vdots \\ w(\alpha_{s_t+1}) = \cdots = w(\alpha_n) &= m_{t+1} \end{aligned}$$

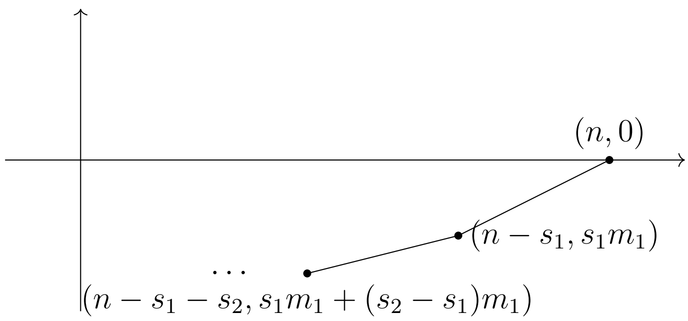
with $m_1 < \cdots < m_{t+1}$. Now, each coefficient of f can be expressed in terms of symmetric polynomials of the roots of f, we have

$$\begin{aligned}
v(a_n) &= v(1) = 0 \\
v(a_{n-1}) &= w\left(\sum_{i=1}^{n} \alpha_i\right) \geq \min_{1\leq i\leq n} w(\alpha_i) = m_1 \\
v(a_{n-2}) &= w\left(\sum_{1\leq i\neq j\leq n} \alpha_i\alpha_j\right) \geq \min_{1\leq i\neq j\leq n} w(\alpha_i\alpha_j) = 2m_1 \\
&\vdots \\
v(a_{n-s_1}) &= w\left(\sum_{1\leq i_1\neq\cdots\neq i_{s_1}\leq n} \alpha_{i_1}\ldots\alpha_{i_{s_1}}\right) = \min_{1\leq i_1\neq\cdots\neq i_{s_1}\leq n} w(\alpha_{i_1}\ldots\alpha_{i_{s_1}}) = s_1 m_1
\end{aligned}$$

where in the last line we have equality as one of the terms in the summation attains a minimal valuation. Continuing in this fashion, we have

$$\begin{aligned}
v(a_{n-(s_1+1)}) &= w\left(\sum_{1\leq i_1\neq\cdots\neq i_{s_1+1}\leq n} \alpha_{i_1}\ldots\alpha_{i_{s_1+1}}\right) \geq \min_{1\leq i_1\neq\cdots\neq i_{s_1+1}\leq n} w(\alpha_{i_1}\ldots\alpha_{i_{s_1+1}}) = s_1m_1 + m_2 \\
&\vdots \\
v(a_{n-s_2}) &= w\left(\sum_{1\leq i_1\neq\cdots\neq i_{s_2}\leq n} \alpha_{i_1}\ldots\alpha_{i_{s_2}}\right) \geq \min_{1\leq i_1\neq\cdots\neq i_{s_2}\leq n} w(\alpha_{i_1}\ldots\alpha_{i_{s_2}}) = s_1m_1 + s_2m_2
\end{aligned}$$

and so on. Plotting the points $(n - s_i, \sum_{i=1}^{n} s_i m_i)$ (where $s_0 = 0$) and drawing a line through them gives us the Newton polygon of f. Indeed, the inequalities we have just demonstrated show that all the points $(i, v(a_i))$ lie either above or on this line. We thus have the following picture



Now, the first line segment (counting from the right), has length $n-(n-s_1) = s_1$ and slope $\frac{0-s_1m_1}{n-(n-s_1)} = -m_1$ as claimed. In general, the length of the k^{th} segment is $(n-s_{k-1})-(n-s_k) = s_k - s_{k-1}$ and slope

$$\begin{aligned}
\frac{(s_1m_1 + \sum_{i=1}^{k-2}(s_{i+1} - s_i)m_{i+1} - (s_1m_1 + \sum_{i=1}^{k-1}(s_{i+1} - s_i)m_{i+1}}{(n - s_k) - (n - s_{k-1})} &= \frac{-(s_k - s_{k-1)m_k}}{s_k - s_{k-1}} \\
&= -m_k
\end{aligned}$$

as claimed. □

Corollary 2.3.6. *Let K be a complete non-archimedean valued field with valuation v and $f(X) \in K[X]$ an irreducible polynomial. Then the Newton polygon of f has a single line segment.*

Proof. It suffices to show that all roots of f have the same valuation. Let α and β be roots in the splitting field L of f. Then there exists $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(\alpha) = \beta$. But then $v(\alpha) = v(\beta)$ by Corollary 2.2.8. $\square$

3 Discretely Valued Fields

3.1 Basic Facts

Definition 3.1.1. Let K be a nonarchimidean valued field with valuation v. We say that K is a **discretely** valued field (and v is a **discrete** valuation) if $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$. This is equivalent to $v(K^\times)$ being an infinite cyclic group.

Definition 3.1.2. Let K be a complete discrete valuation field. We say that K is a **local field** if it has finite residue field.

Definition 3.1.3. Let K be a discrete valuation field. We define a **uniformiser** of K to be any element $\pi \in K$ such that $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$. This is equivalent to $v(\pi)$ having minimal positive valuation.

Example 3.1.4. $\mathbb{Q}, \mathbb{Q}_p$ with valuation v_p are discrete valuation fields. $\mathbb{Q}_p$ is a local field with uniformiser p. Moreover, $K((T))$ with valuation $v\left(\sum_{n>>-\infty}^{\infty} a_n T^n\right) = \inf n | a_n \neq 0$ is a discrete valuation field with uniformiser T and $\mathcal{O}_{K((T))} = K[[T]]$.

Proposition 3.1.5. *Let K be a discrete valuation field with uniformiser π. Let $S \subseteq \mathcal{O}_K$ be a complete set of coset representatives of $\mathcal{O}_K/\mathfrak{m}_K = \mathbb{F}_K$ containing 0. Then*

1. *The non-zero ideals of $\mathcal{O}_K$ are $\pi^n \mathcal{O}_K$.*

2. *$\mathcal{O}_K$ is a principal ideal domain with unique prime π (up to multiplication by units) and $\mathfrak{m}_K = \pi \mathcal{O}_K$.*

3. *The topology on $\mathcal{O}_K$ induced by the absolute value is the π-adic topology.*

4. *If K is complete then $\mathcal{O}_K$ is π-adically complete.*

5. *If K is complete then any $x \in K$ admits a unique expansion*

$$x = \sum_{n>>-\infty}^{\infty} a_n \pi^n$$

   for some $a_n \in S$.

6. *The completion $\widehat{K}$ is also a discrete valuation field with π a uniformiser and*

$$\mathcal{O}_K / \pi^n \mathcal{O}_K \cong \mathcal{O}_{\widehat{K}} / \pi^n \mathcal{O}_{\widehat{K}}$$

   via the natural map.

Proof. The proof of this Proposition is exactly the same as that for $\mathbb{Q}_p$ with K replacing $\mathbb{Q}_p$ and π replacing p. $\square$

Proposition 3.1.6. *Let K be a discretely valued field. Then K is a local field if and only if $\mathcal{O}_K$ is compact.*

Proof. Fix a uniformiser π of K and suppose that K is a local field. We claim that $\mathcal{O}_K$ is sequentially compact. This is indeed sufficient since the topology on K is the metric topology induced by the absolute value. By induction, it is easy to see that for all $n \geq 1$, $\mathcal{O}_K/\pi^n\mathcal{O}_K$ is finite. Indeed, the base case is clear since K is a local field. Now,

$$\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K \cong \left(\mathcal{O}_K/\pi^n\mathcal{O}_K\right)\left(\pi^n\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K\right)$$

The first term is finite by the induction hypothesis and the second term is isomorphic to $\mathbb{F}_K$ via the isomorphism $x \mapsto \pi^{1-n}x$.

Now let $(x_i) \subseteq \mathcal{O}_K$ be a sequence. Then we can always find a subsequence $(x_{1,i})$ of (x_i) which is constant modulo π since $\mathbb{F}_K$ is finite. Similarly, we can find a subsequence $(x_{2,i})$ of $(x_{1,i})$ which is constant modulo π^2. Continuing in this way, we construct a sequence (x_{ii}) of $\mathcal{O}_K$ such that $(x_{n,i})$ is constant modulo π^n. Then the sequence $(x_{i,i})_{i=1}^{\infty}$ is Cauchy since $|x_{i,i} - x_{j,j}| \leq |\pi|^j$ for all $j \leq i$. Since $\mathcal{O}_K$ is π-adically complete, this sequence converges to an element of $\mathcal{O}_K$ so that (x_i) has a convergent subsequence. Hence $\mathcal{O}_K$ is sequentially compact as claimed.

Now suppose that $\mathcal{O}_K$ is compact. We need to show that K is complete and $\mathbb{F}_K$ is finite. Observe that $\mathcal{O}_K$ and $\pi^{-n}\mathcal{O}_K$ are isomorphic as topological rings for any $n \geq 0$ and so the latter is also compact and thus complete[1]. Since any element of K takes the form $\pi^n u$ for some $n \in \mathbb{Z}$ and unit $u \in \mathcal{O}_K^\times$, it follows that

$$K = \bigcup_{n \geq 0} \pi^{-n}\mathcal{O}_K$$

is complete. Moreover, the canonical projection map $\mathcal{O}_K \to \mathbb{F}_K$ is continuous when $\mathbb{F}_K$ is equipped with the discrete topology and so $\mathbb{F}_K$ is compact. But a discrete space is compact if and only if it is finite so we must have that $\mathbb{F}_K$ is finite as desired. □

Definition 3.1.7. Let R be a ring. We say that R is a **discrete valuation ring** if it is a principal ideal domain with a unique prime element up to multiplication by units.

Proposition 3.1.8. *Let R be a ring. Then R is a discrete valuation ring if and only if R is the valuation ring of some discrete valuation field.*

Proof. First suppose that R is a discrete valuation ring with π its unique prime. Then by uniqueness of prime factorisation we have that every $0 \neq x \in R$ admits a unique factorisation $x = \pi^n u$ for some $n \in \mathbb{N}$ and $u \in R^\times$. Define a discrete valuation on R by

$$v(x) = \begin{cases} n & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases}$$

which extends uniquely to $K = \mathrm{Frac}(R)$ so that K is a discrete valuation field. We claim that $R = \mathcal{O}_K$. We first observe that $K = R[\frac{1}{\pi}]$ since any non-zero element of K is of the form $\pi^n u$ for some $n \in \mathbb{Z}$ and $u \in R^\times$. Then $v(\pi^n u) = n \in \mathbb{N} \iff \pi^n u \in R$ and so $R = \mathcal{O}_K$ as claimed.

Conversely, suppose that R is the valuation ring of some discrete valuation field. Then it is immediate by Proposition 3.1.5 that R is a principal ideal domain with a unique prime element up to units. □

[1] Recall that any compact metric space is complete.

Definition 3.1.9.] Let K be a valued field with residue field $\mathbb{F}_K$. We say that K is of **equal characteristic** if $\operatorname{char} K = \operatorname{char} \mathbb{F}_K$. On the other hand, we say that K has **mixed characteristic** otherwise.

Remark. We remark that the only possible examples of mixed characteristic valued fields are the ones where $\operatorname{char} K = 0$ and $\operatorname{char} \mathbb{F}_K > 0$.

3.2 Teichmüller Lifts

Definition 3.2.1. Let R be a ring. We say that R is **perfect** if either $\operatorname{char} R = 0$ or if when $\operatorname{char} R = p$ then the Frobenius endomorphism $x \mapsto x^p$ is an automorphism. The latter case is equivalent to every element of R having a unique p^{th} root.

Remark. We remark that a field K is perfect if and only if every extension of K is separable.

Definition 3.2.2. Let K be a discrete valuation field and $\pi \in K$ a uniformiser. We define the **normalised valuation** of K to be the unique valuation v_K in the equivalence class of v such that $v_K(\pi) = 1$.

Example 3.2.3. $v_{\mathbb{Q}_p} = v_p$

Lemma 3.2.4. *Let R be a ring and $x \in R$ an element. Assume that R is x-adically complete and that R/xR is perfect of characteristic p. Then there exists a unique map*

$$[\cdot] : R/xR \to R$$

called the ***Teichmüller lift*** *such that $[a] \equiv a \pmod{x}$ and $[ab] = [a][b]$ for all $a, b \in R/xR$. Furthermore, if R itself has characteristic p then $[\cdot]$ is a ring homomorphism.*

Proof. Fix $a \in R/xR$. Since R is perfect, for each $n \geq 0$ there exists a unique $(p^{-n})^{th}$ root of a, label it $a^{p^{-n}}$. Now let $\alpha_n \in R$ be an arbitrary lift of $a^{p^{-n}}$. Write $\beta_n = \alpha_n^{p^n}$. We first claim that $[a] = \lim_{n\to\infty} \beta_n$ exists and is independent of the choice of lifts. To ease notation, write $[a] = \lim_{n\to\infty} \beta_n$.

First observe that if the limit exists then $[a]$ is independent of the choice of lifts. Indeed, suppose that β_n and β'_n are a choice of lifts. Then $\beta_1, \beta'_2, \beta_3, \beta'_4, \ldots$ is also a choice of lifts and converges and so we must have that $\lim_{n\to\infty} \beta_n = \lim_{n\to\infty} \beta'_n$. We must hence show that $\beta_{n+1} - \beta_n \to 0$ x-adically. We have that

$$\beta_{n+1} - \beta_n = \alpha_{n+1}^{p^{n+1}} - \alpha_n^{p^n} = (\alpha_{n+1}^p)^{p^n} - \alpha_n^{p^n}$$

Now,

$$\alpha_{n+1}^p \equiv (a^{p^{-(n+1)}})^p \equiv \alpha_n \pmod{x}$$

so that $\alpha_{n+1}^p - \alpha_n \equiv 0 \pmod{x}$. Raising this to the $(p^n)^{th}$ power and using the Binomial Theorem and the fact that R/xR has characteristic p shows that, in fact,

$$(\alpha_{n+1}^p)^{p^n} - \alpha_n^{p^n} \equiv 0 \pmod{x^{p^n}}$$

and so (β_n) is Cauchy. Since R is complete, it then follows that $\lim_{n\to\infty} \beta_n$ exists. To see that $a \equiv [a] \pmod{x}$, we first note that the natural projection map $R \to R/xR$ is continuous if we equip R/xR with the discrete topology so that

$$\lim_{n\to\infty} (\alpha^{p^n}) \equiv \lim_{n\to\infty} (a^{p^{-n}})^{p^n} = \lim_{n\to\infty} a = a \pmod{x}$$

We next show that $[\cdot]$ is multiplicative. Fix $b \in R/xR$ with $\gamma_n \in R$ lifting $b^{p^{-n}}$ for all $n \geq 0$. Then $\alpha_n\gamma_n$ lifts $(ab)^{p^{-n}} = a^{p^{-n}}b^{p^{-n}}$. Then

$$[ab] = \lim_{n\to\infty} \alpha_n^{p^n}\gamma_n^{p^n} = \left(\lim_{n\to\infty} \alpha_n^{p^n}\right)\left(\lim_{n\to\infty} \gamma_n^{p^n}\right) = [a][b]$$

We next show uniqueness of $[\cdot]$. Suppose that $\phi : R/xR \to R$ another map satisfying the above properties. Then $\phi(a^{p^{-n}}) \equiv a^{p^{-n}} \mod x$ and so

$$[a] = \lim_{n\to\infty} \phi(a^{p^{-n}})^{p^n} = \lim_{n\to\infty} \phi(a) = \phi(a)$$

Finally, suppose that R has characteristic p. Then $\alpha_n + \gamma_n$ lifts $a^{p-1} + b^{p-1} = (a+b)^{p^{-n}}$ by Freshman's Dream so that

$$[a+b] = \lim_{n\to\infty} (\alpha_n + \beta_n)^{p^n} = \lim_{n\to\infty} a_n^{p^n} + \gamma_n^{p^n} = [a] + [b]$$

So $[\cdot]$ is additive and multiplicative and $[1] = 1$ so that $[\cdot]$ is a ring homomorphism. □

Example 3.2.5. $[0] = 0$ and $[1] = 1$. If $R = \mathbb{Z}_p$ then $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$ satisfies $[x]^{p-1} = [x^{p-1}] = [1] = 1$ for all non-zero x so that $[x]$ is the unique $(p-1)^{th}$ root of unity lifiting $x \in \mathbb{F}_p$. Recall that by Hensel's Lemma, we proved the existence of these roots and the Teichmüller Lift then gives us an explicit description of them.

Theorem 3.2.6. *Let K be a complete discretely valued field of equal characteristic p such that $\mathbb{F}_K$ is perfect. Then $K \cong \mathbb{F}_K((T))$.*

Proof. Since every discrete valuation field is the field of fractions of its valuation ring, it suffices to show that $\mathcal{O}_K \cong \mathbb{F}_K[[T]]$. Since K has characteristic p, so does $\mathbb{F}_K$ so that $[\cdot] : \mathbb{F}_K \to \mathcal{O}_K$ is an injective ring homomorphism. Fix a uniformiser $\pi \in \mathcal{O}_K$ and define a ring homomorphism

$$\begin{aligned} \mathbb{F}_K &\to \mathcal{O}_K \\ \sum_{n=0}^{\infty} a_n T^n &\mapsto \sum_{n=0}^{\infty} [a_n]\pi^n \end{aligned}$$

By Part 5 of Proposition 3.1.5, this mapping is surjective. The injectivity is clear by injectivity of $[a_n]$. □

Corollary 3.2.7. *Let K be a local field of equal characteristic p. Then $K \cong \mathbb{F}_q((T))$ where $q = |\mathbb{F}_K|$.*

4 p-adic analysis

4.1 Mahler's Theorem

Lemma 4.1.1. *Let K be a complete valued field with absolute value $|\cdot|$ and assume that $\mathbb{Q}_p \subseteq K$ and $|\cdot||_{\mathbb{Q}_p} = |\cdot|_p$. Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in K[[X]]$ be a power series. If $f(X)$ converges on a (closed or open) disc D then $f(X)$ is continuous on that disc.*

Proof. Let $x, y \in D$. We assume that $x \neq 0$. Suppose there exists a $\delta > 0$ such that $|x - y| < \delta$ and $\delta < |x|$. It follows immediately from the ultrametric inequality that $|x| = |y|$. Then

$$\begin{aligned} |f(x) - f(y)| &= \left| \sum_{i=0}^{\infty} (a_i x^i - a_i y^i) \right| \\ &\leq \max_{i \geq 0} \{ |a_i x^i - a_i y^i| \} \\ &= \max_{i \geq 0} \{ |a_i|(x - y)(x^{i-1} + x^{i-2}y + \cdots + xy^{i-2} + y^{i-1}) \} \end{aligned}$$

We now observe that

$$|x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}| \leq \max_{1 \leq i \leq n} \{ |x^{n-1} y^{i-1}| \} = |x|^{n-1}$$

Hence

$$|f(x) - f(y)| \leq \max_{i \geq 0} \{ |a_i||x - y||x|^{i-1} \} < \frac{\delta}{|x|} \max_{i \geq 0} (|a_i x^i|)$$

Now by hypothesis, $f(X)$ converges on a disc which means the absolute values of its terms converges to 0 on the same disc. Hence $|a_n x^n|$ is bounded above by some real constant. We may therefore, given $\varepsilon > 0$, make $|f(x) - f(y)| < \varepsilon$ by choosing a reasonable $\delta < |x|$.

The case where $x = 0$ is an immediate consequence of the convergence of $f(X)$ on D. □

Definition 4.1.2. Let R be a ring. We define the **formal exponential series** over R to be

$$\exp(X) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \in R[[X]]$$

and the **formal logarithm series** over R to be

$$\log(1 + X) = \sum_{n=0}^{\infty} (-1)^{n-1} \frac{x^n}{n}$$

Proposition 4.1.3. *Let K be a complete valued field with absolute value $|\cdot|$ and assume that $\mathbb{Q}_p \subseteq K$ and that $|\cdot||_{\mathbb{Q}_p} = |\cdot|_p$. Then $\exp(x)$ converges when $|x| < p^{-1/(p-1)}$ and $\log(1 + x)$ converges for $|x| < 1$. Moreover, they define continuous maps*

$$\begin{aligned} \exp &: \{ x \in K \mid |x| < p^{-1/(p-1)} \} \to \mathcal{O}_K \\ \log &: \{ x \in K \mid |x| < 1 \} \to K \end{aligned}$$

Proof. Let $v = -\log_p |\cdot|$ be the valuation on K extending v_p. Trivially, we have $v(n) \leq \log_p(n)$ and so

$$v\left(\frac{x^n}{n}\right) \geq nv(x) - v(n) \geq nv(x) - \log_p(n)$$

which tends to ∞ if $v(x) > 0$ and so log converges when $|x| < 1$.

To prove the assertion concerning exp, first observe[2] that $v(n!) = \frac{n - s_p(n)}{p-1}$ where $s_p(n)$ is the sum of the p-adic digits of n. Then

$$v\left(\frac{x^n}{n!}\right) \geq nv(x) - v(n!) = nv(x) - \frac{n - s_p(n)}{p - 1} \geq nv(x) - \frac{n}{p - 1} = n\left(v(x) - \frac{1}{p - 1}\right) \geq 0$$

which tends to ∞ as $n \to \infty$ if $v(x) > \frac{1}{p-1}$. □

[2]This follows from Legendre's Theorem

Remark. Fix $n \geq 1$. Recall that the binomial coefficient

$$\binom{X}{2} = \frac{X(X-1)\dots(X-n+1)}{n!}$$

is a polynomial in X and hence defines a continuous function $\mathbb{Z}_p \to \mathbb{Q}_p$. If $n = 0$, set $\binom{x}{n} = 1$ for all $x \in \mathbb{Z}_p$.

Now if $x \in \mathbb{Z}_{\geq 0}$ then $\binom{x}{n} \in \mathbb{Z}$. But $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ so by continuity, we must have that $\binom{x}{n} \in \mathbb{Z}_p$ for all $x \in \mathbb{Z}_p$.

Proposition 4.1.4. *Let $C(\mathbb{Z}_p, \mathbb{Q}_p)$ be the $\mathbb{Q}_p$-vector space of continuous functions $\mathbb{Z}_p \to \mathbb{Q}_p$ equipped with the norm*[3]

$$||f|| = \sup_{x \in \mathbb{Z}_p} |f(x)|_p$$

Then $||\cdot||$ is a non-archimidean norm on $C(\mathbb{Z}_p, \mathbb{Q}_p)$ and $f_n \to f$ with respect to $||\cdot||$ if and only if $f_n \to f$ uniformly. Moreover, $C(\mathbb{Z}_p, \mathbb{Q}_p)$ is complete with respect to $||\cdot||$.

Proof. It is clear that $||f|| = 0$ if and only if $f = 0$ and that $||\lambda f|| = |\lambda|_p ||f||$. The ultrametric inequality also immediately follows from that for $|\cdot|_p$ and so $||\cdot||$ is a non-archimidean norm.

The fact that convergence with respect to $||\cdot||$ is equivalent to uniform convergence is immediate from the definitions. Indeed, the following are equivalent

$$\forall \varepsilon > 0\ \exists N \in \mathbb{N} \text{ such that } \forall n \geq N, |f_n(x) - f(x)|_p \leq \varepsilon\ \forall x \in \mathbb{Z}_p$$
$$\forall \varepsilon > 0\ \exists N \in \mathbb{N} \text{ such that } \forall n \geq N, \sup_{x \in \mathbb{Z}_p} |f_n(x) - f(x)|_p < \varepsilon$$

To show that $C(\mathbb{Z}_p, \mathbb{Q}_p)$ is complete, it thus suffices to show that every Cauchy sequence (f_n) in $C(\mathbb{Z}_p, \mathbb{Q}_p)$ converges uniformly to some limit in $C(\mathbb{Z}_p, \mathbb{Q}_p)$. Given such a sequence (f_n) and $x \in \mathbb{Z}_p$, $(f_n(x))$ is a Cauchy sequence in $\mathbb{Q}_p$. But $\mathbb{Q}_p$ is complete so this sequence converges, say to some $f(x) \in \mathbb{Q}_p$. We claim that this function f, defined pointwise, is the desired limit of (f_n) in $C(\mathbb{Z}_p, \mathbb{Q}_p)$.

To this end, we must first show that $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$. By definition, we need to show that for all $\varepsilon > 0$, we can find a $\delta > 0$ such that if $|x - y|_p < \delta$ then $|f(x) - f(y)|_p < \delta$. Observe that

$$\begin{aligned} |f(x) - f(y)|_p &= |f(x) + f_n(x) - f_n(x) + f_n(y) - f_n(y) - f(y)|_p \\ &\leq \max\{|f(x) - f_n(x)|_p, |f_n(x) - f_n(y)|_p, |f_n(y) - f(y)|_p\} \end{aligned}$$

Since $f_n \to f$ pointwise and f_n is continuous, we can always find a δ that ensures that each of these three terms is less than ε. Such a δ then ensures that $|f(x) - f(y)|_p < \varepsilon$ as required.

We must now show that $f_n \to f$ uniformly. In other words, we need to show that for all $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $|f_n(x) - f(x)|_p < \varepsilon\ \forall x \in \mathbb{Z}_p$. Given $m > n$ we have

$$|f_n(x) - f(x)|_p = |f_n(x) + f_m(x) - f_m(x) - f(x)|_p \leq \max\{|f_n(x) - f_m(x)|_p, |f_m(x) - f(x)|_p\}$$

Now f_n is Cauchy and f_n converges to f pointwise so we can always find an $N \in \mathbb{N}$ that makes each of these two terms less than ε. Such an N then ensures that $|f_n(x) - f(x)|_p < \varepsilon$ as required. □

[3] This is well-defined since $\mathbb{Z}_p$ is compact and so the supremum exists and is attained.

Definition 4.1.5. Let c_0 denote the $\mathbb{Q}_p$-vector space of sequences $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}_p$ such that $a_n \to 0$ equipped with the norm $||(a_n)_n|| = \max_{n\in\mathbb{N}} |a_n|_p$.

Remark. It is clear that c_0 is complete since $\mathbb{Q}_p$ is itself complete.

Definition 4.1.6. Let $\Delta : C(\mathbb{Z}_p, \mathbb{Q}_p) \to C(\mathbb{Z}_p.\mathbb{Q}_p)$ be the **forward difference operator** given by $\Delta f(x) = f(x+1) - f(x)$. Note that Δ is clearly a linear operator

Proposition 4.1.7. *The linear operator Δ is norm-decreasing and satisfies*

$$\Delta^n f(x) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(x+n-i)$$

Proof. We have that

$$|\Delta f(x)|_p = |f(x+1) - f(x)|_p \leq ||f||$$

and so $||\Delta f|| \leq ||f||$.

To prove the formula, introduce the **forward shift** operator $Sf(x) = f(x+1)$ so that we can write $\Delta f(x) = (S - I)f(x)$ where I is the identity operator. Then

$$\Delta^n = (S-I)^n = \sum_{i=0}^{n} \binom{n}{i} S^{n-i} = \sum_{i=0}^{n} \binom{n}{i} f(x+n-i)$$

as claimed. □

Definition 4.1.8. Let $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$ be a continuous function. We define the n^{th} **Mahler coefficient** of f, denoted $a_n(f) \in \mathbb{Q}_p$, to be

$$a_n(f) = \Delta^n f(0) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(n-i)$$

Lemma 4.1.9. *Let $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$ be a continuous function. Then there exists $k \in \mathbb{N}$ such that $||\Delta^{p^k} f|| \leq \frac{1}{p}||f||$.*

Proof. If $f = 0$ then there is nothing to prove so suppose f is not the 0 function. Moreover, after scaling, we may assume that $||f|| = 1$. We thus need to exhibit a $k \in \mathbb{N}$ such that $\Delta^{p^k} f(x) \equiv 0 \pmod{p}$ for all $x \in \mathbb{Z}_p$. We have that

$$\Delta^{p^k} f(x) = \sum_{i=0}^{p^k} (-1)^i \binom{p^k}{i} f(x+p^k-i) \equiv f(x+p^k) - f(x) \pmod{p}$$

since the binomial coefficients are all divisible by p except when $i = 0$ and $i = p^k$. For this to be 0 modulo p, we thus require that $f(x+p^k) - f(x) \equiv 0 \pmod{p}$.

Now observe that since $\mathbb{Z}_p$ is compact, f is uniformly continuous on $\mathbb{Z}_p$ so we can always find a $k \in \mathbb{N}$ such that

$$|x-y|_p \leq p^{-k} \implies |f(x) - f(y)|_p \leq p^{-1}$$

for all $x, y \in \mathbb{Z}_p$. In particular, this holds for $y = x + p^k$ so we may just choose such a k. □

Proposition 4.1.10. *Consider the mapping*

$$\begin{aligned}\phi : C(\mathbb{Z}_p, \mathbb{Q}_p) &\to c_0 \\ f &\mapsto (a_n(f))_{n\in\mathbb{N}}\end{aligned}$$

The ϕ *is an injective norm-decreasing* $\mathbb{Q}_p$*-linear map.*

Proof. $\mathbb{Q}_p$-linearity of ϕ is immediate from $\mathbb{Q}_p$-linearity of Δ. We now check that ϕ is well-defined. In other words, we must show that $a_n(f) \to 0$ as $n \to \infty$. First observe that

$$|a_n|_p = |\Delta^n f(0)|_p \leq \sup_{x\in\mathbb{Z}_p} |\Delta^n f(x)|_p = ||\Delta^n f||$$

so that it suffices to show that $||\Delta^n f|| \to 0$ as $n \to \infty$. Recall that $||\Delta^n f||$ is monotonically decreasing so we only have to find a subsequence of $||\Delta^n f||$ which converges to 0. But by Lemma 4.1.9, we can always find a sequence $k_1, k_2, \ldots$ of natural numbers such that

$$||\Delta^{p^{k_1+\cdots+k_n}}|| \leq \frac{1}{p^n}||f||$$

so the subsequence $||\Delta^{p^{\sum_{i=1}^n k_i}}||$ converges to 0 as required. To see that ϕ is norm-decreasing, observe that

$$||\phi(f)|| = ||(a_n(f))|| = \max_{n\in\mathbb{N}} |a_n(f)|_p \leq ||\Delta^n f|| \leq ||f||$$

We must finally show injectivity. Suppose that $a_n(f) = 0$ for all $n \in \mathbb{N}$. By induction, we have that

$$f(n) = \Delta^n f(0) = a_n(f) = 0$$

for all $n \geq 0$. Hence f is identically zero on $\mathbb{Z}_{\geq 0}$. Now density and cotinuity imply that f is identically zero on $\mathbb{Z}_p$ itself so that ϕ is injective. □

Lemma 4.1.11. *Let* $x \in \mathbb{Z}_p$ *and* $n \in \mathbb{N}_{\geq 1}$*. Then*

$$\binom{x}{n} + \binom{x}{n-1} = \binom{x+1}{n}$$

Proof. This is true when $x \in \mathbb{Z}_{\geq 0}$ (this is just Pascal's Identity) and so, by density and continuity, it must hold for all $x \in \mathbb{Z}_p$. □

Proposition 4.1.12. *Conisder the mapping*

$$\begin{aligned}\psi : c_0 &\to C(\mathbb{Z}_p, \mathbb{Q}_p) \\ (a_n)_{n\in\mathbb{N}} &\mapsto f_a(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}\end{aligned}$$

Then ψ *is a norm-decreasing* $\mathbb{Q}_p$*-linear map such that* $a_n(f_a) = a_n$ *for all* $n \geq 0$*.*

Proof. We first note that this definition is well-defined since the series is uniformly convergent. Moreover, the $\mathbb{Q}_p$-linearity is immediate from the definition. To see that ψ is norm-decreasing, note that

$$|\psi(a)|_p = \left|\sum_{n=0}^{\infty} a_n \binom{x}{n}\right| \leq \sup_{n\in\mathbb{N}} |a_n|_p \left|\binom{x}{n}\right|_p \leq \sup_{n\in\mathbb{N}} |a_n|_p = ||a||$$

for all $x \in \mathbb{Z}_p$. In particular, we may pass to the supremum to yield $||\psi(a)|| \leq ||a||$.

To prove the assertion concerning coefficients let $a^{(k)} = (a_k, a_{k+1}, \dots)$. Then

$$\begin{aligned}
\Delta f_a(x) &= f_a(x+1) - f_a(x) \\
&= \sum_{n=1}^{\infty} a_n \left(\binom{x+1}{n} - \binom{x}{n} \right) \\
&= \sum_{n=1}^{\infty} a_n \binom{x}{n-1} \\
&= \sum_{n=0}^{\infty} a_{n+1} \binom{x}{n} \\
&= f_{a^{(1)}}(x)
\end{aligned}$$

Iterating this process, we see that $\Delta^k f_a = f_{a^{(k)}}$ so that

$$a_n(f_a) = \Delta^n f_a(0) = f_{a^{(n)}}(0) = a_n$$

□

Lemma 4.1.13. *Let V and W be normed spaces and $\phi : V \to W, \psi : W \to V$ linear maps such that ϕ is injective and norm-decreasing, ψ is norm-decreasing and $\phi\psi = \mathrm{id}_W$. Then $\psi\phi = \mathrm{id}_V$ and ϕ and ψ are isometries.*

Proof. Fix $v \in V$.

$$\phi(v - \psi\phi v) = \phi(v) - \phi\psi\phi(v) = \phi(v) - \phi(v) = 0$$

But ϕ is injective so we must have that $\psi\phi(v) = v$ so that $\psi\phi = \mathrm{id}_V$. Moreover

$$||v|| \geq ||\phi(v)|| \geq ||\psi\phi(v)|| = ||v||$$

so we must have equality throughout. Similarly, $||v|| = ||\psi(v)||$ thereby proving the Lemma.

□

Theorem 4.1.14 (Mahler's Theorem)**.** *The $\mathbb{Q}_p$-vector spaces $C(\mathbb{Z}_p, \mathbb{Q}_p)$ and c_0 are isometric. In particular, every function $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$ admits a unique expansion $f(x) = \sum_{n-0}^{\infty} a_n \binom{x}{n}$.*

Proof. By Propositions 4.1.12 and 4.1.10 we have a pair of maps

$$C(\mathbb{Z}_p, \mathbb{Q}_p) \underset{\psi}{\overset{\phi}{\rightleftarrows}} c_0$$

such that ϕ is injective and norm-decreasing, ψ is norm-decreasing and $\psi\phi = \mathrm{id}$. Lemma 4.1.13 then implies that ψ and ϕ are mutually inverse isometries. □

5 Ramification Theory of Local Fields

From now on, we shall assume that the characteristic of the residue of every local field is p unless otherwise explicitly stated.

5.1 Finite Extensions

Remark. Let R be a principal ideal domain and M a finitely generated R-module. Recall that the Structure Theorem for Finitely Generated Modules over a Principal Ideal Domain asserts that $M \cong M_{\text{tors}} \oplus \mathbb{R}^n$ where M_{tors} is the finite torsion part of M and $n \in \mathbb{N}$ is the rank of M. Moreover, if N is an R-submodule of M then N is also finitely generated and $N \cong N_{\text{tors}} \oplus R^m$ for some $m \leq n$

Proposition 5.1.1. *Let K be a local field and L/K a finite extension of degree n. Then $\mathcal{O}_L$ is a finitely generated free $\mathcal{O}_K$-module of rank n and $\mathbb{F}_L/\mathbb{F}_K$ is an extension of degree at most n. Furthermore, L is a local field.*

Proof. Fix a K-basis $\alpha_1, \ldots, \alpha_n$ of L and let $|| \cdot ||$ denote the max-norm on L. If $| \cdot |$ is the unique absolute value on L extending the absolute value on K then $| \cdot |$ and $|| \cdot ||$ are equivalent as norms on L. We can always find constants $r > s > 0$ such that

$$M = \{ x \in L \mid ||x|| \leq s \} \subseteq \mathcal{O}_L \subseteq \{ x \in L \mid ||x|| \leq r \} = N$$

We may assume, without loss of generality, that $r = |a|$ and $s = |b|$ for some $a, b \in K^\times$. Then

$$M = \bigoplus_{i=1}^{n} \mathcal{O}_K b\alpha_i \subseteq \mathcal{O}_L \subseteq \bigoplus_{i=1}^{n} \mathcal{O}_K a\alpha_i = N$$

But both M and N are finitely generated free $\mathcal{O}_K$-modules of rank n so we must also have that $\mathcal{O}_L$ is a finitely generated free $\mathcal{O}_K$-module of rank n.

Now, $\mathfrak{m}_K = \mathfrak{m}_L \cap \mathcal{O}_K$ since $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L so we obtain a natural injection

$$\mathbb{F}_K = \mathcal{O}_K/\mathfrak{m}_K \to \mathcal{O}_L/\mathfrak{m}_L = \mathbb{F}_L$$

Since $\mathcal{O}_L$ is generated over $\mathcal{O}_K$ by n-elements, $\mathbb{F}_L$ is generated by n elements over $\mathbb{F}_K$ so that $[\mathbb{F}_L : \mathbb{F}_K] \leq n$.

To see that L is a local field, we must show that it is a complete discrete valuation field with finite residue field. The latter is immediate as $\mathbb{F}_K$ is finite and $\mathbb{F}_L/\mathbb{F}_K$ is a finite extension so $\mathbb{F}_L$ must be a local field. Moreover, L is complete by Theorem 2.2.5. Now let v_K be the normalised valuation on K and v_L the unique valuation on L extending v_K. Then

$$v_L(\alpha) = \frac{1}{n} v_K(\mathbf{N}_{L/K}(\alpha))$$

so that

$$v_L(L^\times) \subseteq \frac{1}{n} v_K(K^\times) = \frac{1}{n}\mathbb{Z}$$

which is discrete. □

Definition 5.1.2. Let L/K be a finite extension of local fields. We define the **inertial degree** of L/K to be $f_{L/K} = [\mathbb{F}_L : \mathbb{F}_K]$.

Definition 5.1.3. Let L/K be a finite extension of local fields. We define the **ramification index** of L/K to be $e_{L/K} = v_L(\pi_K)$ where v_L is the normalised valuation on L and π_K is a uniformiser for K.

Theorem 5.1.4. *Let L/K be a finite extension of local fields. Then $[L : K] = e_{L/K}f_{L/K}$ and there exists $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_L[\alpha] = \mathcal{O}_K$.*

Proof. To ease notation, write $e = e_{L/K}$ and $f = f_{L/K}$. Since $\mathbb{F}_L/\mathbb{F}_K$ is a separable extension, the Primitive Element Theorem implies that there exists $\overline{\alpha} \in \mathbb{F}_L$ such that $\mathbb{F}_L = \mathbb{F}_K(\overline{\alpha})$. Let $\overline{f}(X) \in \mathbb{F}_K[X]$ be the minimal polynomial of $\overline{\alpha}$ over $\mathbb{F}_K$ and let $f \in \mathcal{O}_K[X]$ be a monic lift of $\overline{f}$ with $\deg f = \deg \overline{f}$. We claim that there exists $\alpha \in \mathcal{O}_L$ lifting $\overline{\alpha}$ and satisfying $v_L(f(\alpha)) = 1$ so that $f(\alpha)$ is a uniformiser for L. Fix a lift $\beta \in \mathcal{O}_L$ of $\overline{\alpha}$. If $v_L(f(\beta)) = 1$ then we are done and set $\alpha = \beta$. If not then set $\alpha = \beta + \pi_L$ where π_L is the uniformiser for L. Taylor expanding $f(\alpha)$ around β we have

$$f(\alpha) = f(\beta + \pi_L) = f(\beta) + f'(\beta)\pi_L + b\pi_L^2$$

for some $b \in \mathcal{O}_L$. From this we see that

$$v_L(f(\alpha)) \geq \min\{v_L(f(\beta)), v_L(f'(\beta)) + 1, v_L(b) + 1\}$$

By assumption, $v_L(f(\beta)) \geq 2$ and $v_L(f'(\beta)) = 0$ since $f'(\beta)$ is a unit ($\overline{f}$ is separable so that $f'(\beta)$ cannot vanish modulo $\mathfrak{m}$). It then follows that $v_L(f(\alpha)) = 1$.

Now write $\pi = f(\alpha)$. We claim that $\alpha^i\pi^j$ for $i = 0, \ldots, f-1$ and $j = 0, \ldots, e-1$ are an $\mathcal{O}_K$-basis for $\mathcal{O}_L$.

We first show that the $\alpha^i\pi^j$ are linearly independent over K. Indeed, suppose we have $\sum_{i,j} a_{ij}\alpha^i\pi^j$ for some $a_{ij} \in K$ not all 0. Let $s_j = \sum_{i=0}^{f-1} a_{ij}\alpha^i$. Since $1, \alpha^i, \ldots, \alpha^{f-1}$ are linearly independent over $\mathcal{O}_K$, their reductions are linearly independent over $\mathbb{F}_K$. Hence there exists some j such that $s_j \neq 0$.

We claim that $e \mid v_L(s_j)$ if $s_j \neq 0$. Indeed, let k be an index for which $|a_{ij}|$ is maximal. Then $a_{kj}^{-1}s_j = \sum_{i=0}^{f-1} a_{kj}^{-1}a_{ij}\alpha^i$. Now, $|a_{kj}^{-1}a_{ij}| \leq 1$ and is exactly 1 if and only if $i = k$. Now, $a_{kj}^{-1}s_j \not\equiv 0 \pmod{\pi_L}$ since $1, \overline{\alpha}, \ldots, \overline{\alpha}^{f-1}$ are linearly independent over $\mathbb{F}_K$. Hence $a_{kj}^{-1}s_j$ is a unit whence $v(a_{kj}^{-1}s_j) = 0$. Therefore

$$v_L(s_j) = v_L(a_{kj}) + v_L(a_{kj}^{-1}s_j) \in v_L(K^\times) = ev_L(L^\times) = e\mathbb{Z}$$

and so $e|v_L(s_j)$ as claimed.

We can now write $\sum_{i,j} a_{ij}\alpha^i\pi^j = \sum_{j=0}^{e-1} s_j\pi^j = 0$. Suppose that $s_j \neq 0$ for some j. Then $v_L(s_j\pi^j) = v_L(s_j) + j \in j + e\mathbb{Z}$. Hence no two terms in the summation can have the same valuation. This then forces the summation to be non-zero which is a contradiction. Hence $\alpha^i\pi^j$ are linearly independent over K.

We now claim that

$$\mathcal{O}_L = \bigoplus_{i,j} \mathcal{O}_K\alpha^i\pi^j$$

To this end, we make the following definitions

$$M = \bigoplus_{i,j} \mathcal{O}_K\alpha^i\pi^j$$

$$N = \bigoplus_{i=0}^{f-1} \mathcal{O}_K\alpha^i$$

so that $M = N + \pi_L N + \cdots + \pi^{e-1}N$. Now, $1, \overline{\alpha}, \ldots, \overline{\alpha}^{f-1}$ span $\mathbb{F}_L$ over $\mathbb{F}_K$ so that $\mathcal{O}_L = N + \pi\mathcal{O}_L$. Iterating this, we have

$$\begin{aligned}
\mathcal{O}_L &= N + \pi(N + \pi\mathcal{O}_L) \\
&= N + \pi N + \pi^2(\mathcal{O}_L) \\
&\vdots \\
&= N + \pi N + \pi^2 N + \cdots + \pi^{e-1}N + \pi^e\mathcal{O}_L \\
&= M + \pi_K\mathcal{O}_L
\end{aligned}$$

where we have used the fact that π^e and π_K have the same valuation so that they differ by a unit. Iterating this process again, we have that $\mathcal{O}_L = M + \pi_K^n\mathcal{O}_L$ for all $n \geq 1$. In particular, $\mathcal{O}_L = M + \pi_L^n\mathcal{O}_L$ for all $n \geq 1$ so that M is dense in $\mathcal{O}_L$. Now, M is the closed unit ball in $\bigoplus_{ij} K\alpha^i\pi^j \subseteq L$ with respect to the maximum norm on V (with respect to the K-basis of L $\alpha^i\pi^j$). Hence M must be complete whence $M = \mathcal{O}_L$.

Finally, since $\alpha^i\pi^j = \alpha^i f(\alpha)^j$ is a polynomial in α, it follows that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. □

Corollary 5.1.5. *Let $M/L/K$ be finite extensions of local fields. Then*

$$\begin{aligned}
f_{M/K} &= f_{L/K}f_{M/L} \\
e_{M/K} &= e_{L/K}e_{M/L}
\end{aligned}$$

Proof. The statement concerning the inertial degrees is immediate from the Tower Law. The statement concerning the ramification indices follows from the Tower Law and the fact that $[M : K] = f_{M/K}e_{M/K}$. □

5.2 Unramified Extensions

Definition 5.2.1. Let L/K be a finite extension of local fields. We say that L/K is unramified if $e_{L/K} = 1$ (equivalently, $f_{L/K} = [L : K]$) and **totally ramified** if $f_{L/K} = 1$ (equivalently, $f_{L/K} = 1$).

Lemma 5.2.2. *Let L/K be a finite unramified extension of local fields and let M/K be a finite extension. Then there is a natural bijection*

$$\mathrm{Hom}_{K-\mathrm{alg}}(L, M) \to \mathrm{Hom}_{\mathbb{F}_K-\mathrm{alg}}(\mathbb{F}_L, \mathbb{F}_M) \quad (1)$$

given by restriction to $\mathcal{O}_L$ then reducing.

Proof. Fix a K-algebra homomorphism $\phi : L \to M$. By the uniqueness of extended absolute values, ϕ acts as an isometry of the extended absolute values. In particular, $\phi(\mathcal{O}_L) \subseteq \mathcal{O}_M$ and $\phi(\mathfrak{m}_L) \subseteq \mathfrak{m}_M$. We then get an induced $\mathbb{F}_K$-algebra homomorphism

$$\begin{aligned}
\overline{\phi} : \mathbb{F}_L &\to \mathbb{F}_M \\
[x] &\mapsto [\varphi(x)]
\end{aligned}$$

and so we get a homomorphism

$$\mathrm{Hom}_{K-\mathrm{alg}}(L, M) \to \mathrm{Hom}_{\mathbb{F}_K-\mathrm{alg}}(\mathbb{F}_L, \mathbb{F}_M)$$

We claim that this homomorphism is bijective. To this end, let $\overline{\alpha} \in \mathbb{F}_L$ be a primitive element of $\mathbb{F}_L$ over $\mathbb{F}_K$ and $\overline{f}(X) \in \mathbb{F}_K[X]$ its minimal polynimal. Let $f(X) \in \mathcal{O}_K[X]$ be a monic lift of $\overline{f}$ and $\alpha \in \mathcal{O}_L$ the unique root of f that lifts $\overline{\alpha}$ by Hensel's Lemma.

Since L is unramified over K, we have that $[L : K] = f_{L/K} = [\mathbb{F}_L : \mathbb{F}_K] = \deg \overline{f} = \deg f$. But f is irreducible over K and so we must have that $L = K(\alpha)$. We thus have the following diagram

$$
\begin{array}{ccccc}
\phi & \operatorname{Hom}_{K-\mathrm{alg}}(L, M) & \longrightarrow & \operatorname{Hom}_{\mathbb{F}_K-\mathrm{alg}}(\mathbb{F}_L, \mathbb{F}_M) & \overline{\phi} \\
\big\downarrow & \big\downarrow \wr & & \big\downarrow \wr & \big\downarrow \\
\phi(\alpha) & \{\, x \in M \mid f(x) = 0 \,\} & \xrightarrow{\text{mod } \mathfrak{m}_M} & \{\, \overline{x} \in \mathbb{F}_M \mid \overline{f}(\overline{x}) = 0 \,\} & \overline{\phi}(\overline{\alpha})
\end{array}
$$

Now the map in the second row of this diagram is an isomorphism by Hensel's Lemma thereby forcing the map in the top row to also be an isomorphism. □

Theorem 5.2.3. *Let K be a local field. For every finite extension $\ell/\mathbb{F}_K$ there is a unique unramified extension L/K with $\mathbb{F}_L \cong \ell$. Moreover, L/K is Galois with $\operatorname{Gal}(L/K) \cong \operatorname{Gal}(\ell/\mathbb{F}_L)$.*

Proof. Fix a primitive element $\overline{\alpha}$ of $\ell/\mathbb{F}_K$ with minimal polynomial $\overline{f}[X] \in \mathbb{F}_K$. Let $f(X) \in \mathcal{O}_K$ be a monic lift of $\overline{f}$ such that $\deg f = \deg \overline{f}$. Set $L = K(\alpha)$ where α is a root of f. Since $\overline{f}$ is irreducible, it follows that f is irreducible and so $[L : k] = [\ell : \mathbb{F}_K]$. Moreover, $\mathbb{F}_L$ contains a root of $\overline{f}$ (namely the reduction of α) so that $\ell \hookrightarrow \mathbb{F}_L$ over $\mathbb{F}_K$ via $\overline{\alpha} \to \alpha \pmod{\mathfrak{m}_L}$. Hence

$$[L : K] \geq [\mathbb{F}_L : \mathbb{F}_K] \geq [\ell : \mathbb{F}_K] = [L : K]$$

Equality must therefore hold throughout so that $\ell = \mathbb{F}_L$ and so L is unramified since $[L : K] = [\ell : \mathbb{F}_K]$.

To show uniqueness, suppose we have two unramified extensions L and M of the same degree over K. Then we have an isomorphism of their residue fields $\phi : \mathbb{F}_L \to \mathbb{F}_M$ which lifts uniquely to K-embedding $\phi : L \to M$ by Lemma 5.2.2. Since $[L : K] = [M : K]$, it then follows that we must have $M = L$.

To prove the assertion regarding the Galois groups, note that Lemma 5.2.2 also provides us with an isomorphism $\operatorname{Aut}_K(L) \to \operatorname{Aut}_{\mathbb{F}_K}(\mathbb{F}_L)$ and so

$$|\operatorname{Aut}_K(L)| = |\operatorname{Aut}_{\mathbb{F}_K}(\mathbb{F}_L)| = [\mathbb{F}_L : \mathbb{F}_K] = [L : K]$$

and so L/K is Galois with Galois group isomorphic to $\operatorname{Gal}(\mathbb{F}_L/\mathbb{F}_K)$. □

Proposition 5.2.4. *Let K be a local field and L/K an unramified extension. Let M/K be a finite extension and fix an algebraic closure $\bar{K}$ so that $L, M \subseteq \bar{K}$. Then*

1. *LM/M is unramified.*
2. *Any subextension of L/K is unramified over K.*
3. *If M/K is unramified then LM/K is unramified.*

Proof. Fix a primitive element $\overline{\alpha}$ of $\mathbb{F}_L/\mathbb{F}_K$ with minimal polynomial $\overline{f}[X] \in \mathbb{F}_K$. Let $f(X) \in \mathcal{O}_K$ be a monic lift of $\overline{f}$ such that $\deg f = \deg \overline{f}$. Then $L = K(\alpha)$ for some root α of f whence $ML = M(\alpha)$.

Let $\overline{g}(X) \in \mathbb{F}_M[X]$ be the minimal polynomial of $\overline{\alpha}$ over $\mathbb{F}_M$. Then $\overline{g} | \overline{f}$. Hensel's Lemma then implies that f admits a factorisation $f = gh$ with g monic and lifting $\overline{g}$. Then $g(\alpha) = 0$ and g is irreducible over $M[X]$ so that g is the minimal polynomial of α over M. Then

$$[LM : M] = [M(\alpha) : M] = \deg g = \deg \overline{g} \leq [\mathbb{F}_{LM} : \mathbb{F}_M] \leq [LM : M]$$

and so equality must hold throughout whence LM/M is unramified.

To prove the second part, let F be an intermediate extension of L/K. Then $e_{L/K} = e_{L/F} e_{F/K}$. Since $e_{L/K} = 1$ and ramification indices are positive integers, it follows that $e_{F/K} = 1$.

For the third assertion, we observe that

$$[LM : K] = [LM : M][M : K] = f_{LM/M}f_{M/K} = f_{LM/K}$$

since both LM/M and M/K are unramified. □

Corollary 5.2.5. *Let L/K be a finite extension of local fields. Then there exists a unique maximal unramified intermediate field T of L/K. Moreover, $[T : K] = f_{L/K}$.*

Proof. Fix an algebraic closure $\bar{K}$ of K and let T be the compositum of all unramified intermediate extensions of L/K. Then by Proposition 5.2.4, T/K is an unramified extension. We clearly have that $[T : K] = f_{T/K} \leq f_{L/K}$ by multiplicativity of the inertial degrees. Now let T' be the unique unramified extension of K with residue field extension $\mathbb{F}_L/\mathbb{F}_K$. Then the id : $\mathbb{F}_{T'} = \mathbb{F}_L \to \mathbb{F}_L$ lifts to a K-embedding $T' \to L$ by Lemma 5.2.2. Then

$$[T : K] \geq [T' : K] = f_{L/K} \geq [T : K]$$

so equality holds throughout and so we must have that $[T : K] = f_{L/K}$. □

5.3 Totally Ramified Extensions

Theorem 5.3.1 (Eisenstein's Criterion)**.** *Let K be a local field and $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathcal{O}_K[X]$ a monic polynomial and π_K a uniformiser for K. If $\pi_K | a_0, \ldots, a_{n-1}$ but $\pi_K^2 \nmid a_0$ then f is irreducible.*

Proof. Suppose that $f \in \mathcal{O}_K[X]$ is reducible. Then we can write $f = gh$ for some $g, h \in \mathcal{O}_K[X]$ monic and non-constant. Reducing modulo π_K we have

$$\overline{g}\overline{h} = \overline{f} = X^n$$

$\mathbb{F}_K$ is an integral domain and so both $\overline{g}$ and $\overline{h}$ have zero constant term. This implies that the constant terms of g and h are both divisible by π_K. But this would imply that the constant term of f is divisible by π_K^2 which is a contradiction. □

Proposition 5.3.2. *Suppose that L/K is finite extension of local fields and v_K is the normalised valuation on K, w the unique extension of v_K to L. Then*

$$e_{L/K}^{-1} = w(\pi_L) = \min\{w(x) | x \in \mathfrak{m}_L\}$$

Proof. Let v_L be the normalised valuation on L. Then w and v_L differ by a constant - we claim that such a constant is $e_{L/K}^{-1}$. By definition we have

$$e_{L/K} = v_L(\pi_K) \implies 1 = e_{L/K}^{-1} v_L(\pi_K)$$

Since w extends v_K we necessarily have that $w(\pi_K) = 1$ so that $w(\pi_K) = e_{L/K}^{-1} v_L(\pi_K)$ as claimed. Hence for all $x \in L$ we have $w(x) = e_{L/K}^{-1} v_L(x)$. In particular for $x = \pi_L$ we then have that $w(\pi_L) = e_{L/K}^{-1}$. The final equality in the Proposition follows immediately since w attains its minimum on π_L. □

Theorem 5.3.3. *Let L/K be a totally ramified extension of local fields. Then $L = K(\pi_L)$ and the minimum polynomial of π_L over K is an Eisenstein polynomial. Conversely, if $L = K(\alpha)$ for some primitive element $\alpha \in L$ and the minimum polynomial of α over K is Eisenstein then L/K is totally ramified and α is a uniformiser for L.*

Proof. Write $n = [L : K]$ and denote by v_K the normalised valuation on K and w the unique extension of v_K to L. Then

$$[K(\pi_L) : K]^{-1} \leq e^{-1}_{K(\pi_L)/K} = \min_{x \in \mathfrak{m}_{K(\pi_L)/K}} w(x) = \min_{x \in \mathfrak{m}_{K(\pi_L)/K}} (-\log_p |\mathbf{N}_{L/K}(x)|^{1/n}) \leq \frac{1}{n}$$

since $\pi_L \in \mathfrak{m}_{K(\pi_L)}$. Hence $[K(\pi_L) : K] \geq [L : K]$ so that $L = K(\pi_L)$.

Now let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ be the minimal polynomial of π_L over K so that $\pi_L^n = a_0 + a_1\pi_L + \cdots + a_{n-1}\pi_L^{n-1}$. Then

$$w(\pi_L^n) = nw(\pi_L) = ne^{-1}_{L/K} = \frac{n}{n} = 1$$

and on the other hand

$$\begin{aligned} w(\pi_L^n) &= w(a_0 + a_1\pi_1 + \cdots + a_{n-1}\pi_L^{n-1}) \\ &= \min_{0 \leq i \leq n-1} (v_K(a_i) + i/n) \end{aligned}$$

so that $v_K(a_0) = 1$ and $v_K(a_i) \geq 1$ for all other coefficients. Hence f is an Eisenstein polynomial.

Conversely, suppose that $L = K(\alpha)$ where the minimal polynomial $f(X) \in \mathcal{O}_K[\alpha]$ of α over K is an Eisenstein polynomial. Write $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Since f is irreducible, all the roots of f have the same valuation. Indeed, the roots of f are just the Galois conjugates of α and the action of Galois is an isometry on the absolute value. Hence

$$1 = w(a_0) = nw(\alpha)$$

so that $w(\alpha) = 1/n$. Hence

$$e^{-1}_{L/K} = \min_{x \in \mathfrak{m}_L} w(x) \leq \frac{1}{n} = [L : K]^{-1}$$

But $[L : K] = e_{L/K} f_{L/K}$ so we must have that $[L : K] = e_{L/K} = n$ whence L/K is totally ramified and α is a uniformiser. □

Remark. In fact, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

5.4 Ramification Groups

Definition 5.4.1. Let K be a local field and write $U_K = \mathcal{O}_K^\times$ for its unit group. We define the **higher unit groups** of K to be the filtration

$$\cdots \subseteq U_K^{(2)} \subseteq U_K^{(1)} \subseteq U_K^{(0)} = U_K$$

where $U_K^{(s)} = U^{(s)} = 1 + \pi_K^s \mathcal{O}_K$.

Proposition 5.4.2. *Let K be a local field. Then*

$$U_K / U_K^{(1)} \cong \mathbb{F}_K^\times$$

$$U_K^{(s)} / U_K^{(s+1)} \cong \mathbb{F}_K \text{ for all } s \in \mathbb{N}_{\geq 1}$$

Proof. To prove the first isomorphism, note that the natural projection map $U_K = \mathcal{O}_K^\times \to \mathbb{F}_K^\times$ is surjective with kernel $\mathfrak{m}_K^\times = 1 + \pi_K\mathcal{O}_K$.

To prove the second isomorphism, define a surjective mapping

$$\begin{aligned} \phi : U_K^{(s)} &\to \mathbb{F}_K \\ 1 + \pi_K^s x &\mapsto x \pmod{\pi_K} \end{aligned}$$

We must first check that this is a group homomorphism. Indeed, fix $1+\pi_K^s x, 1+\pi_K^s y \in U_K^{(s)}$. Then

$$(1 + \pi_K^s x)(1 + \pi_K^s y) = 1 + \pi_K^s(x + y + \pi_K^s xy)$$

which reduces to $x+y$ modulo π_K so that ϕ is indeed a homomorphism. It's kernel consists of those elements that are elements of $1 + \pi_k^s(\pi_K)\mathcal{O}_K = U_K^{(s+1)}$ so the isomorphism follows. □

Proposition 5.4.3. *Let L/K be a finite Galois extension of local fields. Then there exists a surjective homomorphism* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$.

Proof. Let T/K be the maximal unramified subextension of L/K. By Galois Theory, we know that the natural map

$$\begin{aligned} \mathrm{Gal}(L/K) &\to \mathrm{Gal}(T/K) \\ \sigma &\mapsto \sigma_T \end{aligned}$$

is a surjection. Moreover, Lemma 5.2.2 gives us a diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K) \\ \downarrow\!\!\downarrow & & \downarrow\wr \\ \mathrm{Gal}(T/K) & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_T/\mathbb{F}_K) \end{array}$$

It then follows that the mapping in the first row is a surjection. □

Definition 5.4.4. Let L/K be a finite Galois extension of local fields. We define the **inertia group**, denoted $I(L/K)$, to be the kernel of the surjection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$. Moreover, if T is the maximal unramified subextension in L/K then we call T the **inertia field** of L/K.

Proposition 5.4.5. *Let L/K be a finite Galois extension of local fields. Then $I(L/K)$ is trivial if and only if L is unramified.*

Proof. This is immediate since $I(L/K)$ is trivial if and only if $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$ if and only if L is unramified. □

Lemma 5.4.6. *Let L/K be a finite Galois extension of local fields. Let $\overline{\sigma}$ be the image of σ under the surjective mapping* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\mathbb{F}_L/\mathbb{F}_K)$. *Then for all $x \in \mathbb{F}_L$ we have $[\overline{\sigma}(x)] = \sigma([x])$ where $[\cdot]$ is the Teichmüller Lift.*

Proof. Consider the map

$$\begin{aligned} \phi : \mathbb{F}_L &\to \mathcal{O}_L \\ x &\mapsto \sigma^{-1}([\overline{\sigma}(x)]) \end{aligned}$$

Then ϕ is clearly multiplicative and satsifies $\phi(x) \equiv x \pmod{\pi_L}$. But the Teichmüller Lift is the unique map satisfying these properties so we must have that $\sigma^{-1}([\overline{\sigma}(x)]) = [x]$ whence $[\overline{\sigma}(x)] = \sigma([x])$. □

From now on, given a local field K, let v_K denote the normalised valuation on K.

Definition 5.4.7. Let L/K be a finite Galois of local fields and $s \geq -1 \in \mathbb{R}$. We define the **s-ramification group** of L/K to be

$$G_s(L/K) = \{\, \sigma \in \mathrm{Gal}(L/K) \mid v_L(\sigma(x) - x) \geq s + 1 \text{ for all } x \in \mathcal{O}_L \,\}$$

Remark. We remark that the higher an s-ramification group that $\sigma \in \mathrm{Gal}(L/K)$ belongs to, the less that it 'moves an element of $\mathcal{O}_L$ around'.

Proposition 5.4.8. *Let L/K be a finite Galois extension of local fields. Then*

$$\begin{aligned} G_{-1}(L/K) &\cong \mathrm{Gal}(L/K) \\ G_0 &\cong I(L/K) \end{aligned}$$

Proof. It suffices to unravel the definitions. Indeed

$$\begin{aligned} G_{-1}(L/K) &= \{\, \sigma \in \mathrm{Gal}(L/K) \mid v_L(\sigma(x) - x) \geq 0 \text{ for all } x \in \mathcal{O}_L \,\} \\ &= \mathrm{Gal}(L/K) \end{aligned}$$

since $\mathcal{O}_L$ is $\mathrm{Gal}(L/K)$-invariant. Moreover

$$\begin{aligned} G_0 &= \{\, \sigma \in \mathrm{Gal}(L/K) \mid v_K(\sigma(x) - x) \geq 1 \text{ for all } x \in \mathcal{O}_L \,\} \\ &= \{\, \sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \pmod{\mathfrak{m}_L} \text{ for all } x \in \mathcal{O}_L \,\} \\ &= I(L/K) \end{aligned}$$

□

Proposition 5.4.9. *Let L/K be a finite Galois extension of local fields and π_L a uniformiser of L. Then $G_{s+1}(L/K)$ is a normal subgroup of $G_s(L/K)$ for all $s \in \mathbb{N}$. Moreover, the map*

$$\begin{aligned} \phi : G_s(L/K) \big/ G_{s+1}(L/K) &\to U_L^{(s)} \big/ U_L^{(s+1)} \\ \sigma &\mapsto \frac{\sigma(\pi_L)}{\pi_L} \end{aligned}$$

is a well-defined injective group homomorphism which is independent of the choice of uniformiser π_L.

Proof. Let ϕ be as defined in the Proposition but without the quotient. We first show that ϕ is well-defined. Indeed, fix $\sigma \in G_s(L/K)$. Then

$$v(\sigma(\pi_L) - \pi_L) \geq s + 1$$

so that $\sigma(\pi_L) = \pi_L + \pi_L^{s+1} x$ for some $x \in \mathcal{O}_L$. Hence $\frac{\sigma(\pi_L)}{\pi_L} = 1 + \pi^s x \in U_L^{(s)}$.

We next show that ϕ is independent of the choice of uniformiser. Recall that uniformisers are unique up to multiplication by units. Hence fix a unit $u \in \mathcal{O}_L^\times$. Then $\sigma(u) = u + \pi_L^{s+1} y$ for some $y \in \mathcal{O}_L$. Then

$$\begin{aligned} \frac{\sigma(\pi_L u)}{\pi_L u} &= \frac{(\pi_L + \pi_L^{s+1} x)(u + \pi_L^{s+1} y)}{\pi_L u} \\ &= (1 + \pi_L^{s+1} x)(1 + \pi_L^{s+1} u^{-1} y) \\ &\equiv 1 + \pi_L^s \pmod{U_L^{(s+1)}} \\ &\equiv \frac{\sigma(\pi_L)}{\pi_L} \pmod{U_L^{(s+1)}} \end{aligned}$$

We now verify that ϕ is a homomorphism. Indeed,

$$\begin{aligned}\phi(\sigma\tau) &= \frac{\sigma(\tau(\pi_L))}{\pi_L} = \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)}\frac{\tau(\pi_L)}{\pi_L} \\ &\equiv \frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L} \pmod{U_L^{(s+1)}} \\ &\equiv \phi(\sigma)\phi(\tau) \pmod{U_L^{(s+1)}}\end{aligned}$$

where we have used the fact that $\tau(\pi_L)$ is a uniformiser for L.

It remains to show that $\ker\phi = G_{s+1}(L/K)$. On one hand, comparing definitions, we have

$$\begin{aligned}\ker\phi &= \{\, \sigma \in G_s(L/K) \mid v(\sigma(\pi_L) - \pi) \geq s+2 \,\} \\ G_{s+1}(L/K) &= \{\, \sigma \in G_s(L/K) \mid v(\sigma(z) - z) \geq s+2 \text{ for all } z \in \mathcal{O}_L \,\}\end{aligned}$$

so, clearly, $G_{s+1}(L/K) \subseteq \ker\phi$.

Conversely, fix $\sigma \in \ker\phi \subseteq I(L/K)$. Given $x \in \mathcal{O}_L$, write $x = \sum_{i=0}^{i} nfty[x_n]\pi_L^n$ where $x_n \in \mathbb{F}_L$ and $[\cdot]$ is the Teichmüller Lift. Then $\sigma(\pi_L) = \pi_L + \pi_L^{s+2}y$ for some $y \in \mathcal{O}_L$ and so

$$\begin{aligned}\sigma(x) - x &= \sum_{n=1}^{\infty}[x_n](\sigma(\pi_L)^n - \pi_L^n) \\ &= \sum_{n=1}^{\infty}[x_n]((\pi_L + \pi_L^{s+2}y)^n - \pi_L^n)\end{aligned}$$

After expanding using the Binomial Theorem, it is then clear that $v(\sigma(x) - x) \geq s - 2$ so that $\sigma \in G_{s+1}(L/K)$ as claimed.

It now follows immediately that $G_{s+1}(L/K)$ is normal in $G_s(L/K)$ since it is the kernel of a group homomorphism. □

Corollary 5.4.10. *Let L/K be a finite Galois extension of local fields. Then* Gal(L/K) *is solvable.*

Proof. First observe that

$$\bigcap_{s\in\mathbb{Z}_{\geq 1}} G_s(L/K) = 1$$

so that $(G_s(L/K))_{s\in\mathbb{Z}_{\geq 1}}$ is a subnormal series of Gal(L/K) by Proposition 5.4.9. Moreover

$$G_s(L/K) \big/ G_{s+1}(L/K) \cong U_L^{(s)} \big/ U_L^{(s+1)} \cong \mathbb{F}$$

which is abelian for all $s \geq 0$. The case where $s = -1$ is simply $Gal(L/K)/I(L/K) \cong$ Gal$(\mathbb{F}_L/\mathbb{F}_K)$ which is also abelian. Hence Gal(L/K) is solvable. □

Corollary 5.4.11. *Let L/K be a finite Galois extension of local fields and let $p = \operatorname{char}\mathbb{F}_K$. Then $G_1(L/K)$ is a p-group and it is the unique Sylow p-subgroup of $G_0(L/K) = I(L/K)$.*

Proof. By Proposition 5.4.9, we have an embedding $G_s(L/K)/G_{s+1}(L/K) \hookrightarrow \mathbb{F}_L$. Now, $\mathbb{F}_L$ is a p-group so the quotient

$$\frac{|G_s(L/K)|}{|G_{s+1}(L/K)|}$$

is a power of p. In particular, so is the quotient

$$\frac{|G_1(L/K)|}{|G_t(L/K)|}$$

for any $t \geq 1$. But $G_t(L/K)$ is trivial for large enough t so that $|G_1(L/K)|$ is a power of p and so is a p-group. To see that it is a Sylow p-subgroup of $G_0(L/K)$, note that we also have an injection

$$G_0(L/K)/G_1(L/K) \hookrightarrow \mathbb{F}_L^\times$$

which has order prime to p so $|\operatorname{Gal}(L/K)|$ must be the highest power of p dividing $|G_0(L/K)|$. Moreover, $G_1(L/K)$ is normal in $G_0(L/K)$ so by Sylow's Theorems, $G_1(L/K)$ is the unique Sylow p-subgroup of $G_0(L/K)$. □

Definition 5.4.12. Let L/K be a finite Galois extension of local fields. We call $G_1(L/K)$ the **wild inertia group** and $G_0(L/K)/G_1(L/K)$ the **tame quotient**.

Proposition 5.4.13. *Let $M/L/K$ be finite extensions of local fields with M/K Galois. Then*

$$G_s(M/K) \cap \operatorname{Gal}(M/L) = G_s(M/L)$$

Proof. This follows immediately from the definition. Indeed

$$\begin{aligned} G_s(M/L) &= \{ \sigma \in \operatorname{Gal}(M/L) \mid v_M(\sigma(x) - x) \geq s + 1 \text{ for all } x \in \mathcal{O}_M \} \\ &= G_s(M/K) \cap \operatorname{Gal}(M/L) \end{aligned}$$

□

5.5 Herbrand's Theorem

Definition 5.5.1. Let L/K be a finite Galois extension of local fields. We define a map

$$\begin{aligned} i_{L/K} : \operatorname{Gal}(L/K) &\to \mathbb{Z} \cup \infty \\ \sigma &\mapsto \min_{x \in \mathcal{O}_L} v_L(\sigma(x) - x) \end{aligned}$$

Proposition 5.5.2. *Let L/K be a finite Galois extension of local fields. Then*

$$G_s(L/K) = \{ \sigma \in \operatorname{Gal}(L/K) \mid i_{L/K}(\sigma) \geq s + 1 \}$$

Proof. This is immediate from the definition of the s-ramification group. □

Proposition 5.5.3. *Let L/K be a finite Galois extension of local fields and let $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Then for all $\sigma \in \operatorname{Gal}(L/K)$ we have*

$$i_{L/K}(\sigma) = v_L(\sigma(\alpha) - \alpha)$$

and is independent of the choice of α.

Proof. Choose a $\sigma \in \mathrm{Gal}(L/K)$. Then it is immediate that $i_{L/K}(\sigma) \leq v_L(\sigma(\alpha) - \alpha)$. We thus need to show that $v_L(\sigma(\alpha)-\alpha) \leq i_{L/K}(\sigma)$. To this end, fix $x \in \mathcal{O}_L$. Since $\mathcal{O}_L$ is finitely generated over $\mathcal{O}_K$ by $1, \alpha, \ldots, \alpha^{n-1}$, we can always find a polynomial $g(X) = \sum_{i=0}^{n} b_i X^i \in \mathcal{O}_K[X]$ such that $x = g(\alpha)$. Since the b_i are fixed by $\mathrm{Gal}(L/K)$, we then have

$$\begin{aligned} v_L(\sigma(x) - x) &= v_L(\sigma(g(\alpha) - g(\alpha)) \\ &= v_L\left(\sum_{i=1}^{n} b_i(\sigma(\alpha)^i - \alpha^i)\right) \\ &\geq v_L(\sigma(\alpha) - \alpha)) \end{aligned}$$

where we have used the fact that $\sigma(\alpha) - \alpha | \sigma(\alpha)^i - \alpha^i$ for all $i \geq 1$ and so we are done.

Moreover, it is clear that this definition is independent of the choice of α since any other α' generating $\mathcal{O}_L$ over $\mathcal{O}_K$ is necessarily a conjugate of α. □

Corollary 5.5.4. *Let $M/L/K$ be finite Galois extensions of local fields. Then*

$$i_{M/L}(\sigma) = i_{M/K}(\sigma)$$

for all $\sigma \in \mathrm{Gal}(M/L)$.

Proof. Suppose that $\alpha \in \mathcal{O}_M$ is such that $\mathcal{O}_M = \mathcal{O}_K[\alpha]$. Then also $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ so the Corollary follows immediately. □

Proposition 5.5.5. *Let $M/L/K$ be finite extensions of local fields such that M/L and L/K are Galois. Then for all $\sigma \in \mathrm{Gal}(L/K)$ we have*

$$i_{L/K}(\sigma) = e_{M/L}^{-1} \sum_{\substack{\tau \in \mathrm{Gal}(M/K) \\ \tau|_L = \sigma}} i_{M/K}(\tau)$$

Proof. If σ is the identity then both sides reduce to ∞ so we may assume that $\sigma \in \mathrm{Gal}(L/K)$ is not the identity. Let $\mathcal{O}_M = \mathcal{O}_K[\alpha]$ and $\mathcal{O}_L = \mathcal{O}_K[\beta]$ for some $\alpha \in \mathcal{O}_M$ and $\beta \in \mathcal{O}_L$. Then

$$e_{M/L} i_{L/K}(\sigma) = e_{M/L} v_L(\sigma(\beta) - \beta) = v_M(\sigma(\beta) - \beta)$$

Now, given $\tau \in \mathrm{Gal}(M/K)$ we have $i_{M/K} = v_M(\tau(\alpha) - \alpha)$. Fix $\tau \in \mathrm{Gal}(M/K)$ such that $\tau|_L = \sigma$ and denote $H = \mathrm{Gal}(M/L)$. Then

$$\begin{aligned} \sum_{\substack{\tau' \in \mathrm{Gal}(M/K) \\ \tau'|_L = \sigma}} i_{M/K}(\tau') &= \sum_{\substack{\tau' \in \mathrm{Gal}(M/K) \\ \tau'|_L = \sigma}} v_M(\tau(\alpha) - \alpha) \\ &= \sum_{g \in H} v_M((\tau g)(\alpha) - \alpha) \\ &= v_M\left(\prod_{g \in H} [(\tau g)(\alpha) - \alpha]\right) \end{aligned}$$

Label $a = \prod_{g \in H}[(\tau g)(\alpha) - \alpha]$ and $b = \sigma(\beta) - \beta = \tau(\beta) - \beta)$. It suffices to show that $v_M(b) = v_M(a)$. *A fortiori*, it suffices to show that $b \mid a$ and $a \mid b$.

First observe that if $z \in \mathcal{O}_L$ then we can write $z = \sum_{i=0}^{n} z_i \beta^i$ for some $z_i \in \mathcal{O}_K$. Then $\tau(z) - z = \sum_{i=1}^{n} z_i(\tau(\beta)^i - \beta^i)$ is divisible by $\tau(\beta) - \beta = b$.

Now let $F(x) \in \mathcal{O}_L[X]$ be the minimal polynomial of α over L. Explicitly, we can write $F(X) = \prod_{g \in H}(X - g(\alpha))$. If τF is the polynomial obtained by applying τ to each of the coefficients of F then we have $(\tau F)(X) = \prod_{g \in H}(X - (\tau g)(\alpha))$. Then all the coefficients of $\tau F - F$ are of the form $\tau(z) - z$ for some $z \in \mathcal{O}_L$ so they are thus divisible by b. Hence $b \mid (\tau F - F)(\alpha) = \pm a$.

Conversely, pick $f \in \mathcal{O}_K[X]$ such that $f(\alpha) = \beta$. Since $f(\alpha) - \beta = 0$, we see that α is a root of the polynomial $f(X) - \beta$ so, in particular, it is divisible by the minimal polynomial of α F so we must have that $f(X) - \beta = F(X)h(x)$ for some $h(x) \in \mathcal{O}_L[X]$. Then

$$(f - \tau\beta)(X) = (\tau f - \tau\beta)(X) = (\tau f)(X) \cdot (\tau h)(X)$$

Setting $X = \alpha$ we then have that

$$-b = \beta - \tau\beta = (\pm a)(\tau h)(\alpha)$$

so that $a \mid b$ as claimed. $\square$

Definition 5.5.6. Let L/K be a finite Galois extension of local fields. Define a map

$$\eta_{L/K}(s) : [1, \infty) \to [-1, \infty)$$

by the formula

$$\eta_{L/K}(s) = \left(e_{L/K}^{-1} \sum_{\sigma \in \mathrm{Gal}(L/K)} \min\{i_{L/K}(\sigma), s+1\} \right) - 1$$

Theorem 5.5.7 (Herbrand's Theorem)**.** *Let $M/L/K$ be finite extensions of local fields with M/K and L/K Galois. Then*

$$G_s(M/K)H\big/_{H} = G_t(L/K)$$

where $t = \eta_{M/L}(s)$ and $H = \mathrm{Gal}(M/L)$.

Proof. To ease notation, write $G = \mathrm{Gal}(M/K)$. Fix a $\sigma \in \mathrm{Gal}(L/K)$ and let τ be an extension of σ to M such that $i_{M/K}(\tau) \geq i_{M/K}(\tau g)$ for all $g \in H$. We claim that

$$i_{L/K}(\sigma) - 1 = \eta_{M/L}(i_{M/K}(\tau) - 1)$$

If this were indeed the case then we would have that

$$\begin{aligned} \sigma \in \frac{G_s(M/K)H}{H} &\iff \tau \in G_s(M/K) \\ &\iff i_{M/K}(\tau) - 1 \geq s \end{aligned}$$

Now, η is strictly increasing so

$$\begin{aligned} \sigma \in \frac{G_s(M/K)H}{H} &\iff \eta_{M/L}(i_{M/K}(\tau) - 1) \geq \eta_{M/L}(s) \\ &\iff \eta_{M/L}(i_{M/K}(\tau) - 1) \geq t \\ &\iff i_{L/K}(\sigma) - 1 \geq t \\ &\iff i_{L/K}(\sigma) \geq t + 1 \\ &\iff \sigma \in G_t(L/K) \end{aligned}$$

We now prove the claim $i_{L/K}(\sigma)-1=\eta_{M/L}(i_{M/K}(\tau)-1)$. Observe that this is equivalent to showing that

$$e_{M/L}^{-1}\sum_{g\in H} i_{M/K}(\tau g)=e_{M/L}^{-1}\sum_{g\in H}\min\{i_{M/L}(g),i_{M/K}(\tau)\}$$

To demonstrate this, it suffices to show that

$$i_{M/K}(\tau g)=\min\{i_{M/L}(g),i_{M/K}(\tau)\}$$

for all $g\in H$. We have that

$$\begin{aligned}
i_{M/K}(\tau g) &= v_M((\tau g)(\alpha)-\alpha)\\
&v_M((\tau g)(\alpha)+g(\alpha)-g(\alpha)-\alpha)\\
&\geq \min\{v_M((\tau g)(\alpha)-g(\alpha)),v_M(g(\alpha)-\alpha)\}\\
&= \min\{i_{M/K}(\tau),i_{M/K}(g)\}\\
&= \min\{i_{M/L}(g),i_{M/K}(\tau)\}
\end{aligned}$$

Now if $i_{M/L}(g)<i_{M/K}(\tau)$ then equality clearly holds throughout by the properties of the ultrametric inequality. Conversely, if $i_{M/L}(g)>i_{M/K}(\tau)$ then the previous calculation shows that $i_{M/K}(\tau g)\geq i_{M/K}(\tau)$. But by assumption we have $i_{M/K}(\tau)\geq i_{M/K}(\tau g)$ so we must have the equality $i_{M/K}(\tau g)\geq i_{M/K}(\tau)$.

Hence in either case the claim holds and we are done. □

5.6 Upper Numbering

Proposition 5.6.1. *Let L/K be a finite Galois extension of local fields. Then*

$$\eta_{L/K}(s)=\int_0^s\frac{dx}{[G_0(L/K):G_x(L/K)]}$$

where for $-1\leq x<0$ we take the convention

$$\frac{1}{[G_0(L/K):G_x(L/K)]}=[G_x(L/K):G_0(L/K)]$$

which equals 1 when $1<x<0$ so $\eta_{L/K}(s)=s$ if $-1\leq s\leq 0$.

Proof. Denote the integral by $\theta(s)$. Since $i_{L/K}(\sigma)$ is always an integer, it is clear that both these functions are piecewise linear and the breakpoints occur at integers. It therefore suffices to show that both functions agree at a point and have the same derivative away from the breakpoints. We have

$$\begin{aligned}
\eta_{L/K}(0) &= \left(e_{L/K}^{-1}\sum_{\sigma\in\mathrm{Gal}(L/K)}\min\{i_{L/K}(\sigma),1\}\right)-1\\
&= \frac{|\{\,\sigma\in\mathrm{Gal}(L/K)\mid i_{L/K}(\sigma)\geq 1\,\}|}{e_{L/K}}-1\\
&= \frac{|G_0(L/K)|}{e_{L/K}}-1\\
&= \frac{|I(L/K)|}{e_{L/K}}-1\\
&= 0\\
&= \theta(0)
\end{aligned}$$

Now let $s \in [-1, \infty) \setminus \mathbb{Z}$. Observe that $\partial_y \min\{x, y\}$ is 0 if $x \leq y$ and 1 if $x > y$ so by the Fundamental Theorem of Calculus we have

$$\begin{aligned}
\eta'_{L/K}(s) &= \frac{|\{\sigma \in \mathrm{Gal}(L/K) \mid i_{L/K}(\sigma) \geq s+1\}|}{e_{L/K}} \\
&= \frac{|G_s(L/K)|}{|G_0(L/K)|} \\
&= \frac{1}{[G_0(L/K) : G_s(L/K)]} \\
&= \theta'(s)
\end{aligned}$$

□

Remark. Since $\eta_{L/K} : [1, \infty) \to [1, \infty)$ is continuous, strictly increasing and satisfies $\eta_{L/K}(-1) = -1$ and $\eta_{L/K}(s) \to \infty$ as $s \to \infty$ we see that it is invertible. Write $\psi_{L/K} = \eta_{L/K}^{-1}$.

Lemma 5.6.2. *Let $M/L/K$ be finite extensions of local fields such that M/K and L/K are Galois. Then*

$$\eta_{M/K} = \eta_{L/K} \circ \eta_{M/L}$$

so that

$$\psi_{M/K} = \psi_{M/L} \circ \psi_{L/K}$$

Proof. Let $s \in [-1, \infty)$ and set $t = \eta_{M/L}(s)$ and $H = \mathrm{Gal}(M/L)$. By Herbrand's Theorem, we have

$$G_t(L/K) \cong \frac{G_s(M/K)H}{H} \cong \frac{G_s(M/K)}{H \cap G_s(M/K)} \cong \frac{G_s(M/K)}{G_s(M/L)}$$

Hence

$$\frac{|G_s(M/K)|}{e_{M/K}} = \frac{|G_t(L/K)|}{e_{L/K}} \frac{|G_s(M/L)|}{e_{M/L}}$$

Now, the Fundamental Theorem of Calculus implies that

$$\eta'_{M/K}(s) = \frac{|G_s(M/K)|}{|e_{M/K}|}$$

So that by the Chain Rule we have

$$\eta'_{M/K}(s) = \eta'_{L/K}(t)\eta'_{M/L}(s) = \eta'_{L/K}(\eta_{M/L}(s))\eta'_{M/L}(s) = (\eta_{L/K} \circ \eta_{M/L})'(s)$$

Since $\eta_{M/K}$ and $\eta_{L/K} \circ \eta_{M/L}$ both agree at 0, these functions must be the same. □

Definition 5.6.3. Let L/K be a finite Galois extension of fields. We define the **upper numbering** of the rammification groups to be the groups

$$G^t(L/K) = G_{\psi_{L/K}(t)}(L/K)$$

for $t \in [1-, \infty)$. We refer to the previous numbering as the **lower numbering**.

Corollary 5.6.4. *Let $M/L/K$ be finite Galois extensions of local fields and $H = \mathrm{Gal}(M/L)$. Given $t \in [-1, \infty)$ we have*

$$\frac{G^t(M/K)H}{H} \cong G^t(L/K)$$

Proof. Let $s = \psi_{L/K}(t)$. By Herbrand's Theorem we have

$$\begin{aligned}\frac{G^t(M/K)H}{H} &= \frac{G_{\psi_{M/K}(t)}H}{H} \\ &= G_{\eta_{M/L}(\psi_{M/K}(t))}(L/K) \\ &= G_{\psi_{L/K}(t)}(L/K) \\ &= G_s(L/K) \\ &= G^t(L/K)\end{aligned}$$

□

5.7 Application to Cyclotomic Fields

We will apply the results of this section in calculating the ramification groups of the $(p^n)^{th}$ cylcotomic field $\mathbb{Q}_p(\zeta_{p^n})$. Indeed, fix a rational prime p and a primitive $(p^n)^{th}$ root of unity $\zeta_{p^n} \in \overline{\mathbb{Q}_p}$.

We first claim that the $(p^n)^{th}$ cyclotomic polynomial

$$\Phi_{p^n}(X) = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + X^{p^n-1} + 1$$

is the minimal polynomial of ζ_{p^n} over $\mathbb{Q}_p$. Indeed, we have

$$\Phi_{p^n}(X) = \frac{X^{p^n} - 1}{X - 1}$$

so that, indeed, $\Phi_{p^n}(\zeta_{p^n}) = 0$. Note that $\mathbb{Q}_p(\zeta_{p^n}) = \mathbb{Q}_p(\zeta_{p^n} - 1)$ so it suffices to show that $\Phi_{p^n}(X+1)$ is the minimal polynomial of $\zeta_{p^n} - 1$ over $\mathbb{Q}_p$. It is clear that $\zeta_{p^n} - 1$ is a root of this polynomial so we have that

$$\Phi_{p^n}(X+1) = \frac{(X+1)^{p^n} - 1}{X} \equiv X^{p^n-1} \pmod{p}$$

From this we see that every coefficient of $\Phi_{p^n}(X+1)$ is divisible by p except for the leading coefficient. Moreover, $\Phi_{p^n}(0+1) = \Phi_{p^n}(1) = p$ so that the constant term is not divisible by p^2. Hence $\Phi_{p^n}(X+1)$ is Eisenstein at p so it is irreducible. This furthermore implies that $L = \mathbb{Q}_p(\zeta_{p^n}) = \mathbb{Q}_p(\zeta_{p^n} - 1)$ is totally ramified of degree $p^{n-1}(p-1)$ with uniformiser $\zeta_{p^n} - 1$ and ring of integers $\mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^n} - 1] = \mathbb{Z}_p[\zeta_{p^n}]$.

We have an isomorphism

$$\begin{aligned}\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times &\to \mathrm{Gal}(L/\mathbb{Q}_p) \\ m &\mapsto \sigma_m\end{aligned}$$

where σ_m is the map $\sigma_m(\zeta_{p^n}) = \zeta_{p^n}^m$. Fix $\sigma_m \in \mathrm{Gal}(L/K)$ and $s \in (0, \infty)$. We want to determine when $\sigma_m \in G_s(L/K)$. We calculate

$$i_{L/\mathbb{Q}_p}(\sigma_m) = v_L(\sigma_m(\zeta_{p^n}) - \zeta_{p^n}) = v_L(\zeta_{p^n}^m - \zeta_{p^n}) = v_L(\zeta_{p^n}) + v_L(\zeta_{p^n}^{m-1} - 1) = v_L(\zeta_{p^n}^{m-1} - 1)$$

since ζ_{p^n} is a unit in $\mathcal{O}_L$. Note that $\zeta_{p^n}^{m-1}$ is a primitive $(p^{n-k})^{th}$ for the maximal k such that $p^k \mid m-1$ and that we have a containment of fields $K = \mathbb{Q}_p(\zeta_{p^{n-k}}) \subseteq L$ so that $\zeta_{p^n}^{m-1} - 1$ is a uniformiser for K. By definition, we have that $e_{L/K} = v_L(\zeta_{p^n}^{m-1} - 1)$. But we know that $e_{L/K} = e_{L/\mathbb{Q}_p} e_{K/\mathbb{Q}_p}^{-1}$. Since both extensions are totally ramified, it then follows that

$$v_L(\zeta_{p^n}^{m-1} - 1) = \frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k$$

Hence

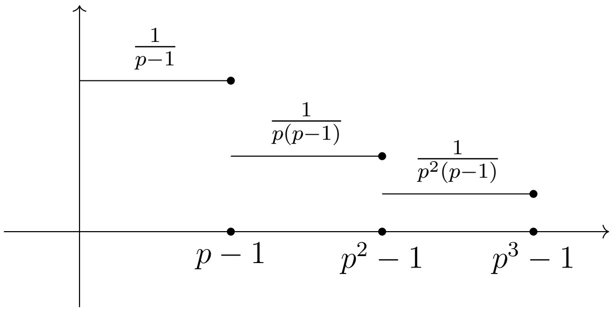
$$\sigma_m \in G_s(L/K) \iff i_{L/K}(\sigma_m) \geq s+1 \iff p^k \geq s+1$$

Now, since $p^k \mid m-1$, it follows that $m = 1 + dp^k$ for some integer d. But then $\sigma_m(\zeta_{p^k}) = \zeta_{p^k}^{1+dp^k} = \zeta_{p^k}$. We thus have that $\sigma_m \in \mathrm{Gal}(L/\mathbb{Q}_p(\zeta_{p^k}))$. Putting all this together, we have that for all $p^k \leq s \leq p^{k-1} + 1$ where $s \in \mathbb{N}$ and $1 \leq k \leq n-1$, we have

$$G_s(L/\mathbb{Q}_p) = \mathrm{Gal}(L/\mathbb{Q}_p(\zeta_{p^k}))$$

Finally, when $s \geq p^{n-1}$, we have that $G_s(L/K) = 1$.

We would now like to transfer this to the upper numbering. We claim that $\eta_{L/\mathbb{Q}_p}(p^k - 1) = k$ so that $G^k(L/\mathbb{Q}_p) \cong \mathrm{Gal}(L/\mathbb{Q}_p(\zeta_{p^k}))$. Indeed, the following is the graph of the function we must integrate to obtain $\eta_{L/\mathbb{Q}_p}$



where we have used the fact that the jumps in the lower numbering are at $p^k - 1$ for $1 \leq k \leq n-1$. We can verify that this is the case by first calculating

$$[I(L/K) : G_1(L/K)] = \frac{e_{L/K}^{-1}}{p^{n-1}} = \frac{p^{n-1}(p-1)}{p^{n-1}} = p-1$$

and then continuing calculating indices. Then

$$\begin{aligned}\eta_{L/K}(k) &= \frac{1}{p-1}(p-1) + \frac{1}{p(p-1)}(p^2 - 1 - (p-1)) + \cdots + \frac{1}{p^k(p-1)}(p^k - 1 - (p^{k-1} - 1)) \\ &= k\end{aligned}$$

as claimed.

6 Local Class Field Theory

6.1 Infinite Galois Theory

Definition 6.1.1. Let L/K be an algebraic extension of fields. We say that L/K is **separable** if for every $\alpha \in L$, the minimal polynomial of α over K is separable. We say that L/K is **normal** if the minimal polynomial of α over K splits into linear factors in $L[X]$ for all $\alpha \in L$. We say that L/K is **Galois** if it is normal and separable. If so, we write $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$.

Definition 6.1.2. Let M/K be a Galois extension. We define the **Krull topology** on $\mathrm{Gal}(M/K)$ to be the one with basis

$$\{\, \sigma\,\mathrm{Gal}(M/L) \mid \sigma \in G, L/K \text{ is finite} \,\}$$

Proposition 6.1.3. *Let M/K be a Galois extension. Then $\mathrm{Gal}(M/K)$ is a profinite group*[4].

Proof. Proof omitted. □

Remark. If M/K is finite then the Krull topology is just the discrete topology.

Definition 6.1.4. Let I be a poset with ordering $\leq$. We say that I is a **directed system** if for all $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 6.1.5. Let I be a directed system. An **inverse system** indexed by I is a collection of topological groups G_i for $i \in I$ and continuous homomorphisms $f_{ij} : G_j \to G_i$ for $i, j \in I$ such that $i \leq j$, $f_{ii} = \mathrm{id}_{G_i}$ and $f_{ik} = f_{ij} \circ f_{jk}$ whenever $i \leq j \leq k$.

Moreover, we define the **inverse limit** of the system (G_i, f_{ij}) to be the topological group (with the subspace topology coming from the product topology)

$$\varprojlim_{i \in I} G_i = \left\{ (g_i) \in \prod_{i \in I} G_i \;\middle|\; f_{ij}(g_j) = g_i \text{ for all } i \leq j \right\}$$

Proposition 6.1.6. *Let M/K be a Galois extension. The set I of finite intermediate Galois extensions L of M/K is a directed system under inclusion. If $L, L' \in I$ with $L \subseteq L'$ then we have a map*

$$\cdot|_L^{L'} : \mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$$

Then $(\mathrm{Gal}(L/K), \cdot|_L^{L'})_{L \in I, L \subseteq L'}$ is an inerse system and the map

$$\begin{aligned} \mathrm{Gal}(M/K) &\to \varprojlim_{L \in I} \mathrm{Gal}(L/K) \\ \sigma &\mapsto (\sigma|_L)_{L \in I} \end{aligned}$$

is an isomorphism of topological groups.

Proof. Proof omitted. □

Theorem 6.1.7 (Fundamental Theorem of Galois Theory). *Let M/K be a Galois extension. The map $L \mapsto \mathrm{Gal}(M/L)$ defines an inclusion reversing bijection between intermediate extensions L/K of M/K and closed subgroups of $\mathrm{Gal}(M/K)$ with inverse $H \mapsto M^H = \{\, m \in M \mid \sigma(m) = m \text{ for all } \sigma \in H \,\}$.*

Moreover, L/K is finite if and only if $\mathrm{Gal}(M/L)$ is open in $\mathrm{Gal}(M/K)$ and L/K is Galois if and only if $\mathrm{Gal}(M/L)$ is normal in $\mathrm{Gal}(M/K)$ from which we establish an isomorphism

$$\begin{aligned} \frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)} &\to \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

Proof. Proof omitted. □

[4] Recall that a topological group is profinite if and only if it is compact Hausdorff and totally disconnected

6.2 Unramified Extensions and Weil Groups

Definition 6.2.1. Let K be a local field and M/K an algebraic extension. We say that M/K is **unramified** (resp. **totally ramified**) if L/K is unramified (resp. **totally ramified**) for all finite intermediate extensions L of M/K.

Proposition 6.2.2. *Let M/K be an unramified extension of local fields*[5]*. Then M/K is Galois and $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_K)$ via the reduction map.*

Proof. Every finite subextension of M/K is unramified and, in particular, Galois so M/K is Galois as well. We then have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(M/K) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_K) \\ \big\downarrow \wr & & \big\downarrow \wr \\ \varprojlim\limits_{L/K} \mathrm{Gal}(L/K) & \xrightarrow{\sim} & \varprojlim\limits_{L/K} \mathbb{F}_L/\mathbb{F}_K \end{array}$$

so we must have that the top row is an isomorphism as well. $\square$

Definition 6.2.3. Let M/K be a finite unramified extension of local fields. We define the **Frobenius element** of $\mathrm{Gal}(M/K)$, denoted $\mathrm{Frob}_{M/K}$, to be the unique element of $\mathrm{Gal}(M/K)$ that acts as Frobenius on $\mathbb{F}_M/\mathbb{F}_K$. Moreover, since $\mathrm{Frob}_{M/K}$ is compatible with restriction, we can also define the Frobenius element for arbitrary unramified extensions of local fields in the exact same way.

Definition 6.2.4. Let K be a local field and M/K a Galois extension. Let $T = T_{M/K}$ be the maximal unramified subextension of M/K. We define the **Weil group** of M/K to be

$$W(M/K) = \{\, \sigma \in \mathrm{Gal}(M/K) \mid \sigma|_T = \mathrm{Frob}_{T/K}^n \text{ for some } n \in \mathbb{Z} \,\}$$

which comes equipped with the topology induced by the basis

$$\{\, \sigma \, \mathrm{Gal}(L/T) \mid \sigma \in W(M/K), L/T \text{ is finite} \,\}$$

Remark. The above situation is summarised in the following commutative diagram of topological groups.

$$\begin{array}{ccccc} \mathrm{Gal}(M/T) & \hookrightarrow & W(M/K) & \twoheadrightarrow & \mathrm{Frob}_{T/K}^{\mathbb{Z}} \\ \big\downarrow \wr & & \big\downarrow & & \big\downarrow \\ \mathrm{Gal}(M/T) & \hookrightarrow & \mathrm{Gal}(M/K) & \twoheadrightarrow & \mathrm{Gal}(T/K) \end{array}$$

where $\mathrm{Frob}_{T/K}^{\mathbb{Z}}$ is equipped with the discrete topology. The topology that the Weil group is endowed with ensures that this diagram is indeed a commutative diagram in the category of topological groups.

Proposition 6.2.5. *Let K be a local field and M/K a Galois extension. Then $W(M/K)$ is dense in $\mathrm{Gal}(M/K)$. If L/K is a finite subextension of M/K then $W(M/L) = W(M/K) \cap \mathrm{Gal}(M/L)$. Moreover, if L/K is also Galois then we have an isomorphism*

$$\frac{W(M/K)}{W(M/L)} \cong \mathrm{Gal}(L/K)$$

via restriction.

[5] Note that an infinite extension of a local field is not necessarily a local field since it may be the case that the residue field of the extension is infinite.

Proof. By definition, $W(M/K)$ is dense in $\mathrm{Gal}(M/K)$ if and only if for every open subset $U \subseteq \mathrm{Gal}(M/K)$ we have $W(M/K) \cap U \neq \varnothing$. Recall that

$$\{\, \sigma \,\mathrm{Gal}(M/L) \mid \sigma \in \mathrm{Gal}(M/K),\ \text{finite } L/K \,\}$$

is a basis for $\mathrm{Gal}(M/K)$ so it just suffices to show that for all $\sigma \in \mathrm{Gal}(M/K)$ and finite subextensions L/K of M/K we have $W(M/K) \cap \sigma \,\mathrm{Gal}(M/L) \neq \varnothing$. But note that by the Fundamental Theorem of Galois Theory we have

$$\frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)} \cong \mathrm{Gal}(L/K)$$

and the $\sigma \,\mathrm{Gal}(M/K)$ are just the cosets of all such factor groups so it suffices to show that $W(M/K) \cap \mathrm{Gal}(L/K) \neq \varnothing$ for all finite subextensions L/K. Equivalently, we just need to show that $W(M/K)$ surjects onto $\mathrm{Gal}(L/K)$ for all finite subextensions L/K of M/K.

To this end, let L/K be a finite subextension of M/K. Let $T = T_{M/K}$ be the maximal unramified subextension of M so that $T_{L/K} = T \cap L$. Consider the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Gal}(M/T) & \longrightarrow & W(M/K) & \longrightarrow & \mathrm{Frob}_{T/K}^{\mathbb{Z}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Gal}(L/(T \cap L)) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}((T \cap L)/K) & \longrightarrow & 0
\end{array}$$

where the left hand side is surjective by field theory and the right hand side is surjective since $\mathrm{Gal}(T_{L/K}/K)$ is finite so is generated by the Frobenius element. The Five Lemma then implies that we must have a surjection in the middle.

To prove the second assertion, let L/K be a finite subextension of M/K so that $LT_{M/K} \subseteq T_{M/L}$. Consider the commutative diagram

$$\begin{array}{ccccc}
\mathrm{Frob}_{T_{M/K}/K}^{\mathbb{Z}} & \hookrightarrow & \mathrm{Gal}(T_{M/K}/K) & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_K) \\
\uparrow & & \uparrow & & \uparrow \\
\mathrm{Frob}_{T_{M/L}/L}^{\mathbb{Z}} & \hookrightarrow & \mathrm{Gal}(T_{M/L}/L) & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_L)
\end{array}$$

Which implies that the left-hand vertical map must be an inclusion. Hence

$$\mathrm{Frob}_{T_{M/L}/L}^{\mathbb{Z}} = \mathrm{Frob}_{T_{M/K}/K}^{\mathbb{Z}} \cap \mathrm{Gal}(T_{M/L}/L)$$

Hence if $\sigma \in \mathrm{Gal}(M/L)$ we have that

$$\begin{aligned}
\sigma \in W(M/L) &\iff \sigma|_{T_{M/L}} \in \mathrm{Frob}_{T_{M/L}/L}^{\mathbb{Z}} \\
&\iff \sigma|_{T_{M/L}} \in \mathrm{Frob}_{T_{M/K}/K}^{\mathbb{Z}} \\
&\iff \sigma \in W(M/K)
\end{aligned}$$

Finally, to prove the third assertion, suppose that L/K is a finite Galois subextension of M/K. Then $\mathrm{Gal}(M/L)$ is normal in $\mathrm{Gal}(M/K)$ whence Part 2 implies that $W(M/L)$ is normal in $W(M/K)$. Then

$$\begin{aligned}\frac{W(M/K)}{W(M/L)} &= \frac{W(M/K)}{W(M/K)\cap \mathrm{Gal}(M/L)}\\ &\cong \frac{W(M/K)\,\mathrm{Gal}(M/L)}{\mathrm{Gal}(M/L)}\\ &= \frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)}\\ &\cong \mathrm{Gal}(L/K)\end{aligned}$$

where the second isomorphism comes from an isomorphism theorem and the third equality from the fact that the Weil group is dense in the Galois group. □

6.3 Main Theorems of Local Class Field Theory

Definition 6.3.1. Let K be a local field and L/K a Galois extension. We say that L/K is **abelian** if $\mathrm{Gal}(L/K)$ is abelian.

Proposition 6.3.2. *Let L/K and M/K be Galois extensions of fields. Then we have an injective group homomorphism*

$$\begin{aligned}\mathrm{Gal}(LM/K) &\to \mathrm{Gal}(L/K)\times \mathrm{Gal}(M/K)\\ \sigma &\mapsto (\sigma|_L, \sigma|_M)\end{aligned}$$

Moreover, this injection is an isomorphism if and only if $L\cap M = K$.

Proof. We must first check that this is a group homomorphism. It suffices to show that it is a homomorphism in each component. To this end, fix $\sigma,\tau \in \mathrm{Gal}(LM/K)$. We need to show that $(\sigma\tau)|_L = \sigma|_L\tau|_L$. So fix $\alpha\in L$ so that $(\sigma\tau)_L(\alpha) = \sigma\tau(\alpha) = \sigma(\tau(\alpha))$. Since L/K is Galois, we must have that $\tau(\alpha)\in L$ so that $\sigma(\tau(\alpha)) = \sigma|_L(\tau|_L(\alpha)) = (\sigma|_L\circ\tau|_L)(\alpha)$ whence $(\sigma\tau)|_L = \sigma|_L\circ\tau|_L$. Similarly, $(\sigma\tau)|_M = \sigma|_M\circ\tau|_M$ so it is indeed a group homomorphism.

The kernel is clearly trivial since if σ is trivial on L and M then it must be trivial on LM.

Now, the embedding is an isomorphism if and only if $[LM : K] = [L : K][M : K]$ or, equivalently, $[LM : M] = [L : K]$. Consider the restriction homomorphism

$$\begin{aligned}\mathrm{Gal}(LM/M) &\to \mathrm{Gal}(L/K)\\ \sigma &\mapsto \sigma|_L\end{aligned}$$

Any automorphism in the kernel of this homomorphism necessarily fixes both L and M so, in particular, it must fix LM. But the only such automorphism is the trivial one so the kernel of this homomorphism must be trivial. Now, the image of this map is of the form $\mathrm{Gal}(L/E)$ for some intermediate extension E of L/K. More precisely, E is the subfield of L fixed by those automorphisms of $\mathrm{Gal}(LM/M)$ when restricted to L. Now, an element of LM is fixed by $\mathrm{Gal}(LM/M)$ if and only if it lies in M so the image of the restriction map is $\mathrm{Gal}(L/(L\cap M))$. In particular, $[LM : M] = [L : L\cap M]$ and this is $[L : K]$ if and only if $L\cap M = K$. □

Corollary 6.3.3. *Let K be a local field and fix an algebraic closure $\overline{K}$ of K. Then there exists a unique maximal abelian extension of K inside $\overline{K}$. Moreover, K^{ab} contains K^{ur}, the maximal unramified extension of K.*

Proof. Let K^{ab} be the compositum of all abelian extensions of K inside $\overline{K}$. Then Proposition 6.3.2 implies that K^{ab} is abelian and it must be the maximal such extension since any other abelian extension must be contained in K^{ab}.

Let $K^{\text{ur}} = T_{K^{\text{sep}}/K} \subseteq K^{\text{ab}}$ where K^{sep} is the separable closure of K. Then K^{ur} is clearly the maximal unramified extension of K contained in K^{ab}. □

Theorem 6.3.4 (Local Artin Reciprocity). *Let K be a local field. Then there exists a unique isomorphism of topological groups*

$$\text{Art}_K : K^\times \to W(K^{\text{ab}}/K)$$

*called the **Artin map** such that*

1. *If π_K is a uniformiser for K and $\text{Frob}_K = \text{Frob}_{K^{\text{ur}}/K}$ then*

$$\text{Art}_K(\pi_K) = \text{Frob}_K$$

2. *If L/K is a finite abelian extension then*

$$\text{Art}_K(\mathbf{N}_{L/K}(\cdot))|_L = \text{id}_L$$

3. *If M/K is a finite extension of local fields then for all $x \in M^\times$ we have*

$$\text{Art}_M(x)|_{K^{\text{ab}}} = \text{Art}_K(\mathbf{N}_{M/K}(x))$$

4. *If M/K is a finite extension of local fields and $\mathbf{N}(M/K) = \mathbf{N}_{M/K}(M^\times)$ then the Artin map induces an isomorphism*

$$\text{Art}_K : K^\times / \mathbf{N}(M/K) \to \text{Gal}((M \cap K^{\text{ab}})/K)$$

Proof. To be proven later on. □

Corollary 6.3.5. *Let L/K be a finite extension of local fields. Then*

$$\mathbf{N}(L/K) = \mathbf{N}((L \cap K^{\text{ab}})/K)$$

and

$$[K^\times : \mathbf{N}(L/K)] \leq [L : K]$$

with equality if and only if L/K is abelian.

Proof. Denote $M = L \cap K^{\text{ab}}$. We then have isomorphisms

$$\frac{K^\times}{\mathbf{N}(L/K)} \cong \text{Gal}((L \cap K^{\text{ab}})/K) = \text{Gal}(M/K) = \text{Gal}((M \cap K^{\text{ab}}/K) \cong \frac{K^\times}{\mathbf{N}(M/K)}$$

The second equality is immediate from the same isomorphism. □

Theorem 6.3.6 (Existence Theorem)**.** *Let K be a local field. Then there is a one-to-one inclusion reversing correspondence*

$$\left\{ \begin{array}{c} \textit{open finite-index} \\ \textit{subgroups of } K^\times \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{finite abelian} \\ \textit{extensions of } K \end{array} \right\}$$
$$H \longmapsto (K^{\mathrm{ab}})^{\mathrm{Art}_K(H)}$$
$$\mathbf{N}(L/K) \longleftarrow L/K$$

In particular, given finite abelian extensions L/K and M/K then

$$\mathbf{N}(LM/K) = \mathbf{N}(L/K) \cap \mathbf{N}(M/K)$$
$$\mathbf{N}((L \cap M)/K) = \mathbf{N}(L/K)\,\mathbf{N}(M/K)$$

Proof. We shall only prove the following aspect of this Theorem. Let L/K be a finite extension and M/K abelian. Then $\mathbf{N}(L/K) \subseteq \mathbf{N}(M/K)$ if and only if $M \subseteq L$. By Corollary 6.3.5, we may assume that L is abelian. First suppose that $M \subseteq L$. Then we have isomorphisms

$$\frac{K^\times}{\mathbf{N}(M/K)} \cong \mathrm{Gal}(M/K) \subseteq \mathrm{Gal}(L/K) \cong \frac{K^\times}{\mathbf{N}(L/K)}$$

so that $\mathbf{N}(L/K) \subseteq \mathbf{N}(M/K)$.

Now assume that $\mathbf{N}(L/K) \subseteq \mathbf{N}(M/K)$. By Galois Theory, it suffices to show that if $\sigma \in \mathrm{Gal}(K^{\mathrm{ab}}/L)$ and $\sigma|_M = \mathrm{id}_M$. Now since $W(K^{\mathrm{ab}}/L)$ is dense in $\mathrm{Gal}(K^{\mathrm{ab}}/L)$, it suffices to prove the claim when $\sigma \in W(K^{\mathrm{ab}}/L)$. By Artin Reciprocity we have an isomorphism

$$W(K^{\mathrm{ab}}/L) \cong \mathrm{Art}_K(\mathbf{N}(L/K)) \subseteq \mathrm{Art}_K(\mathbf{N}(M/K))$$

Hence we can always find $x \in M^\times$ such that $\sigma = \mathrm{Art}_K(\mathbf{N}_{M/K}(x))$. Artin Reciprocity then also tells us that $\sigma_M = \mathrm{id}_M$. □

7 Lubin-Tate Theory

This section shall be concerned with explicitly constructing the maximal abelian extension K and the Artin Map Art_K.

7.1 Local Class Field Theory for $\mathbb{Q}_p$

We first provide a motivating example before continuing on to Lubin-Tate Theory.

Lemma 7.1.1. *Let L/K be a finite abelian extension of local fields. Then*

$$e_{L/K} = [\mathcal{O}_K^\times : \mathbf{N}_{L/K}(\mathcal{O}_L)^\times]$$

Proof. Fix $x \in L^\times$, w the unique valuation on L extending v_K and set $n = [L : K]$. By the construction of w, we know that

$$v_K(\mathbf{N}_{L/K}(x)) = nw(x) = f_{L/K} v_L(x)$$

We then have a surjection

$$\frac{K^\times}{\mathbf{N}(L/K)} \to \frac{\mathbb{Z}}{f_{L/K}\mathbb{Z}}$$

It is readily verified that the kernel of this homomorphism is

$$\frac{\mathcal{O}_K^\times}{\mathcal{O}_K^\times \cap \mathbf{N}(L/K)} = \frac{\mathcal{O}_K^\times}{\mathbf{N}_{L/K}(\mathcal{O}_L^\times)}$$

By Class Field Theory we have

$$n = [K^\times : \mathbf{N}(L/K)] = f_{L/K}[\mathcal{O}_K^\times : \mathbf{N}_{L/K}(\mathcal{O}_L^\times)]$$

□

Corollary 7.1.2. *Let L/K be a finite abelian extension of local fields. Then L/K is unramified if and only if $\mathbf{N}_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$.*

Let π_K be a uniformiser for K so that $K^\times$ is topologically isomorphic to $\langle \pi_K \rangle \times \mathcal{O}_K^\times$. By the Existence Theorem, abelian extensions of K correspond to open finite-index subgroups of $K^\times$. The groups

$$\langle \pi_K^m \rangle \times U_K^{(n)}$$

for all $m, n \geq 0$ are a basis for the topology of $K^\times$ so every open finite-index subgroup of K must contain a subgroup of this form. Hence to find the maximal abelian extension of K, it suffices to take the compositum of all abelian extensions of K corresponding to such subgroups. However, we know that $\mathbf{N}(LM/K) = \mathbf{N}(L/K) \cap \mathbf{N}(M/K)$ so it suffices to consider subgroups of the form

$$\langle \pi_K \rangle \times U_K^{(m)}$$
$$\langle \pi_K^m \rangle \times \mathcal{O}_K$$

The extension corresponding to the latter group is easy to understand. By the Corollary, it is just the unramfied extension of K of degree m. The former is harder to understand and is what we shall need Lubin-Tate Theory for. In any case, if we write K_m/K for the extensions of K corresponding to the former groups then we have $K^{\text{ab}} = K^{\text{ur}}L$ where L is the union over m of all the K_m.

Lemma 7.1.3. *Let K be a local field. Then we have isomorphisms*

$$\begin{aligned} W(K^{\text{ab}}/K) &\cong W(K^{\text{ur}}L/K) \\ &\cong W(K^{\text{ur}}/K) \times \text{Gal}(L/K) \\ &\cong \text{Frob}_K^{\mathbb{Z}} \times \text{Gal}(L/K) \end{aligned}$$

Proof. The first isomorphism follows from the previous discussion. The second follows from the fact that $K^{\text{ab}} \cap L = K$ since L must be totally ramified. The third is because K^{ur}/K is unramified and, in particular, coincides to its maximal unramified subextension. □

Example 7.1.4. Let $K = \mathbb{Q}_p$ for some rational prime p and $\pi_K = p$ its uniformiser. Let

$$K_m = K(\mathbb{Q}_p(\zeta_{p^m}))$$

where ζ_{p^m} is a primitive $(p^m)^{th}$ root of unity in $\overline{\mathbb{Q}_p}$. We first calculate the norm group of this extension. Recall that $\zeta_{p^m} - 1$ is a uniformiser for this extension and the ring of integers of $\mathbb{Q}_p(\zeta_{p^m})$. First observe that $\mathbb{Q}_p(\zeta_{p^m})^\times = \langle \zeta_{p^m} - 1 \rangle \times \mathbb{Z}_p[\zeta_{p^m}]^\times$. Now, $\mathbf{N}_{K_m/K}(\zeta_{p^m} - 1) = \pm\Phi_{p^m}(1) = \pm p$. Moreover, Lemma 7.1.1 implies that

$$n = [K_m : K] = e_{K_m/K} = [\mathcal{O}_K^\times : \mathbf{N}(\mathbb{Z}_p[\zeta_{p^m}])^\times]$$

So that

$$\mathbf{N}(K_m/K) = \mathbf{N}_{K_m/K}(K_m^\times) = \langle p \rangle \times (1 + p^n\mathbb{Z}_p)$$

Now define

$$\mathbb{Q}_p(\zeta_{p^\infty}) = \bigcup_{m=1}^{\infty} \mathbb{Q}_p(\zeta_{p^m})$$

which is totally ramified since it is the nested union of totally ramified extensions. Hence $W(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$. To calculate the latter, we notice that

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) &\cong \lim_{n} \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \\ &\cong (\mathbb{Z}/p^n\mathbb{Z})^\times \\ &\cong \mathbb{Z}_p^\times\end{aligned}$$

It turns out that the inverse of this isomorphism is actually $\mathrm{Art}_{\mathbb{Q}_p}$ restricted to $\mathbb{Z}_p^\times$. Explicitly if $m = \sum_{i=0}^\infty a_i p^i \in \mathbb{Z}_p^\times$ for some $a_i \in \{ 0, \dots, p-1 \}$ and $a_0 \neq 0$, we have $\mathrm{Art}_{\mathbb{Q}_p}(m) = \sigma_m$ where $\sigma_m \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ acts as

$$\sigma_m(\zeta_{p^n}) = \zeta_{p^n}^m = \lim_{k \to \infty} \zeta_{p^n}^{\sum_{i=0}^k a_i p^i} = \zeta_{p^n}^{a_0 + a_1 + \cdots + a_{n-1}p^{n-1}}$$

We can then read off the full Artin map from the diagram

$$\begin{array}{ccccc} \mathbb{Q}_p^\times & \xrightarrow{\mathrm{Art}_{\mathbb{Q}_p}} & W(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) & & \sigma \\ \downarrow\wr & & \downarrow\wr & & \downarrow \\ \langle p \rangle \times \mathbb{Z}_p^\times & \longrightarrow & W(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) & & (\sigma|_{\mathbb{Q}_p^{\mathrm{ur}}}, \sigma|_{\mathbb{Q}_p(\zeta_{p^\infty})}) \\ & & & & \\ (p^n, m) & \longmapsto & (\mathrm{Frob}_{\mathbb{Q}_p}^n, \sigma_m^{-1}) & & \end{array}$$

Theorem 7.1.5 (Local Kronecker-Weber Theorem)**.** *Given $n \in \mathbb{N}_{\geq 1}$, let ζ_n be a primitive n^{th} root of unity. Then*

$$\begin{aligned}\mathbb{Q}_p^{\mathrm{ab}} &= \bigcup_{i=1}^{\infty} \mathbb{Q}_p(\zeta_n) \\ \mathbb{Q}_p^{\mathrm{ur}} &= \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n)\end{aligned}$$

Proof. To be proven later on. □

Definition 7.1.6. Let K be a local field, M/K a Galois extension and I the collection of all finite Galois subextensions of M/K. For all $s \in [-1, \infty)$ we define the **higher ramification group**

$$G^s(M/K) = \{ \sigma \in \mathrm{Gal}(M/K) \mid \sigma|_L \in G^s(L/K) \text{ for all } L \in I \}$$

Remark. Note that we could equivalently define

$$G^s(M/K) = \varprojlim_{L/K} G^s(L/K)$$

Example 7.1.7. Let $K = \mathbb{Q}_p$ for some rational prime p. We are interested in calculating $G^s(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$. Let $\mathbb{Q}_{p^n}$ be the unique unramified extension of $\mathbb{Q}_p$ of degree n. Completely analogously to the case for $\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p$, we have

$$G^s(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_p) = \begin{cases} \mathrm{Gal}(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_p) & \text{if } s = -1 \\ \mathrm{Gal}(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_{p^n}) & \text{if } -1 < s \leq 0 \\ \mathrm{Gal}(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_{p^n}(\zeta_{p^k})) & \text{if } k-1 < s \leq k \leq m-1 \\ 1 & \text{if } s > m-1 \end{cases}$$

for $k = 1, \ldots, m-1$. Recall that by Artin Reciprocity, we have an isomorphism

$$\frac{K^\times}{\mathbf{N}(M/K)} \cong \mathrm{Gal}((K^{\mathrm{ab}} \cap M)/K)$$

for any finite extension M of a local field K. Via some clever uses of isomorphism theorems to determine the quotients, we may thus pass to the Artin map to obtain

$$G^s(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_p) = \begin{cases} \dfrac{\langle p \rangle \times U^{(0)}}{\langle p^n \rangle \times U^{(m)}} & \text{if } s = -1 \\ \dfrac{\langle p^n \rangle \times U^{(0)}}{\langle p^n \rangle \times U^{(m)}} & \text{if } -1 < s \leq 0 \\ \dfrac{\langle p^n \rangle \times U^{(k)}}{\langle p^n \rangle \times U^{(m)}} & \text{if } k-1 < s \leq k \leq m-1 \\ 1 & \text{if } s > m-1 \end{cases}$$

Hence

$$G^s(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \varprojlim_{n,m} G^s(\mathbb{Q}_{p^n}(\zeta_{p^m})/\mathbb{Q}_p) \cong \varprojlim_{n,m} \frac{\langle p^n \rangle \times U^{(k)}}{\langle p^n \rangle \times U^{(m)}} = U^{(k)}$$

via the Artin map where k is chosen so that $k - 1 \leq s \leq k$.

Corollary 7.1.8. *Let $L/\mathbb{Q}_p$ be a finite abelian extension. Then*

$$G^s(L/\mathbb{Q}_p) = \mathrm{Art}_{\mathbb{Q}_p}\left(\frac{\mathbf{N}(L/\mathbb{Q}_p)U^{(k)}}{\mathbf{N}(L/\mathbb{Q}_p)}\right)$$

where $k - 1 \leq s \leq k$. In particular, $L \subseteq \mathbb{Q}_{p^n}(\zeta_{p^m})$ for some n if and only if $G^s(L/\mathbb{Q}_p) = 1$ for all $s > m - 1$.

7.2 Formal Groups

Definition 7.2.1. Let R be a ring. A **formal group** over R is a formal power series $F(X,Y) \in R[[X,Y]]$ such that

1. $F(X,Y) \equiv X + Y \pmod{X^2, XY, Y^2}$
2. $F(X,Y) = F(Y,X)$

3. $F(X, F(Y, Z)) = F(F(X, Y), Z)$ in $R[[X, Y, Z]]$

Example 7.2.2. Let F be a formal group over $\mathcal{O}_K$ where K is a complete valued field. Then $F(X, Y)$ converges for all $x, y \in \mathfrak{m}_K$ so that $\mathfrak{m}_K$ is a group under the multiplication operation

$$(x, y) \mapsto F(x, y)$$

Example 7.2.3. $\widehat{\mathbb{G}_a}(X, Y) = X + Y$ is the formal additive group.

Example 7.2.4. $\widehat{\mathbb{G}_m}(X, Y) = X + Y + XY$ is the formal multiplicative group. Note that $X + Y + XY = (1 + X)(1 + Y) - 1$ so if K is a complete valued field then $\mathfrak{m} \xrightarrow{\sim} 1 + \mathfrak{m}$ via $x \mapsto 1 + x$ and the rule $(x, y) \mapsto x + y + xy$ is just the usual multiplication on $1 + \mathfrak{m}$ transported to $\mathfrak{m}$.

Lemma 7.2.5. *Let R be a ring and F a formal group over R. Then*

1. $F(X, 0) = X$
2. *There exists $i(X) \in R[[X]]$ such that $F(X, i(X)) = 0$*

Proof. We first claim that, given any formal power series $g(X) = \sum_{i \geq 1} a_i X^i \in R[[X]]$ such that $g(X) \equiv a_1 X \pmod{X^2}$ for some $a_1 \in R^\times$, there exists a power series $h(X) \in R[[X]]$ such that $g(h(X)) = X$. To do this, we shall inducitively construct polynomials $h_n(X) = \sum_{i=1}^n b_i X^i$ such that $g(h(X)) \equiv \pmod{X^{n+1}}$. We then obtain the desired power series as $h = \lim_{n \to \infty} h_n(X)$ which is well-defined since $R[X]$ is X-adically complete.

Indeed, suppose that $n = 1$. Then we may set $h_1(X) = b_1 X$ with $b_1 = a^{-1}$. Then, clearly, $g(h_1(X)) \equiv X \pmod{X^2}$. Now assume that we have constructed $h_{n-1}(X)$ such that $g(h_{n-1}(X)) \equiv X \pmod{X^n}$. Then $g(h_{n-1}(X)) \equiv X + c_n X^n \pmod{X^{n+1}}$ for some $c_n \in R$. Now consider

$$h_n(X) = h_{n-1}(X) + b_n X^n$$

We have

$$h_n(X)^k = (h_{n-1}(X) + b_n X^n)^k \equiv \begin{cases} h_{n-1}^k(X) & \text{if } k > 1 \\ h_{n-1}(X) + b_n X^n & \text{if } k = 1 \end{cases} \pmod{X^{n+1}}$$

So we have

$$\begin{aligned} g(h_n(X)) = \sum_{k \geq 1} a_k h_n(X)^k = \sum_{k \geq 1} a_k (h_{n-1}(X) + b_n X^n)^k &\equiv \sum_{k \geq 1} a_k h_{n-1}^k + a b_n X^n \\ &= X + c_n X^n + a_1 b_n X^n \end{aligned}$$

So we may take $b_n = -a_1^{-1} c_n$ and we are done.

Now, to prove the first assertion, write $f(X) = F(X, 0)$. Then $f(f(X)) = F(F(X, 0), 0) = F(X, F(0, 0)) = F(X, 0) = f(X)$. Now, by the claim, there exists $h(X) \in R[X]$ such that $f(h(X)) = X$. Then

$$F(X, 0) = f(X) = f(f(h(X)) = f(h(X)) = X$$

To prove the second assertion, first observe that by the first assertion and symmetricity, we have

$$F(X, Y) = \sum_{m, n \geq 1} a_{m,n} X^m Y^n$$

As in the proof of the claim, we shall construct $i_k(X)$ by induction such that $i_k(X) = \sum_{i=1}^k b_i X^i$ with $b_1 = -1$ and

$$F(X, i_k(X)) \equiv 0 \pmod{X^{k+1}}$$

We will then take $i(X) = \lim_{k\to\infty} i_k(X)$.

First suppose that $k = 1$. Set $i_1(X) = -X$. Then

$$F(X, -X) = X + (-X) + \sum_{m,n\geq 1} a_{m,n} X^m (-X)^n \equiv 0 \pmod{X^2}$$

Now suppose that we have constructed $i_{k-1}(X)$. Set $i_k(X) = i_{k-1} + b_k X^k$. We have

$$X^m (i_{k-1}(X) + b_n X^k)^n \equiv X^m i_{k-1}(X)^n \pmod{X^{k+1}}$$

so that

$$\begin{aligned} F(X, i_k(X)) &= X - i_{k-1}(X) + b_k X^k + \sum_{n,m\geq 1} X^m (i_{k-1}(X) + b_n X^k) \\ &\equiv X - i_{k-1}(X) + b_n X^k \sum_{n,m\geq 1} X^m i_{k-1}(X)^n \pmod{X^{k+1}} \\ &\equiv F(X, i_{k-1}) + b_n X^k \pmod{X^{k+1}} \end{aligned}$$

Now, $F(X, i_{k-1}) \equiv 0 \pmod{X}^k$ so $F(X, i_{k-1}) \equiv c_k X^K \pmod{X^{k+1}}$ so

$$F(X, i_k(X)) \equiv c_k X^K + b_n X^k \pmod{X^{k+1}}$$

so we can just take $b_n = -c_k$ and we are done. □

Definition 7.2.6. Let R be a ring and F, G formal groups over R. We define a **homomorphism of formal groups** $f : F \to G$ to be a formal power series $f \in R[[X]]$ such that $f(X) \equiv 0 \mod X$

$$f(F(X, Y)) = G(f(X), f(Y))$$

Remark. Let F be a formal group over a ring R. The endomorphisms $f : F \to F$ form a ring $\mathrm{End}_R(F)$ with addition $+_F$ given by $(f +_F g)(X) = F(f(X), g(X))$ and multiplication $(f \circ g)(X) = f(g(X))$.

Definition 7.2.7. Let $\mathcal{O}$ be a ring. By a **formal $\mathcal{O}$-module** we mean a formal group F over $\mathcal{O}$ together with a ring homomorphism

$$[\cdot]_F : \mathcal{O} \to \mathrm{End}_{\mathcal{O}}(F)$$

such that for all $a \in \mathcal{O}$ we have $[a]_F(X) \equiv aX \pmod{X^2}$.

Definition 7.2.8. Let K be a local field. We define a **Lubin-Tate module** over $\mathcal{O}_K$, with respect to a uniformiser π_K, to be a formal $\mathcal{O}_K$-module F such that

$$[\pi]_F(X) \equiv X^q \pmod{\pi}$$

where $q = |\mathbb{F}_K|$. In other words, π acts as Frobenius on F.

Example 7.2.9. $\widehat{\mathbb{G}_m}$ is a Lubin-Tate module over $\mathbb{Z}_p$ with respect to p. Indeed, if $a \in \mathbb{Z}_p$, define

$$[a]_{\hat{\mathbb{G}_m}}(X) = (1+X)^a - 1 = \sum_{n=1}^{\infty} \binom{a}{n} X^n$$

First note that $[a]_{\hat{\mathbb{G}_m}}(X) = aX \pmod{X)^2}$. To see that this is infact a ring homomorphism, we note that we have the identities $((1+X)^a)^b = (1+X)^{ab}$ and $(1+X)^a(1+X)^b = (1+X)^{ab}$ by the usual continuity and density arguments (they hold for $\mathbb{Z}$). Then

$$[p]_{\hat{\mathbb{G}_m}}(X) = \sum_{i=1}^{p} \binom{p}{n} X^n \equiv X^p \pmod{p}$$

Hence $\widehat{\mathbb{G}_m}$ is a Lubin-Tate module.

Definition 7.2.10. Let K be a local field with uniformiser π_K and $q = |\mathbb{F}_K|$. A **Lubin-Tate series** for π_K is a formal power series $e(X) \in \mathcal{O}_K[X]$ such that $e(X) \equiv \pi_K X \pmod{X^2}$ and $e(X) \equiv X^q \pmod{\pi_K}$. We let $\mathcal{E}_{\pi_K}$ denote the set of all Lubin-Tate series for π_K. A **Lubin-Tate polynomial** is a Lubin-Tate series of the form

$$uX^q + \pi_K(a_{q-1})X^{q-1} + \cdots + a_2X^2) + \pi_K X$$

for some unit $u \in U_K^{(1)}$ and $a_2, \ldots, a_{q-1} \in \mathcal{O}_K$.

Remark. Note that if F is a Lubin-Tate $\mathcal{O}_K$ module for π_K then $[\pi]_K$ is a Lubin-Tate series for π_K.

Proposition 7.2.11. *Let K be a local field and π_K a uniformiser for K. Let $e_1, e_2 \in \mathcal{E}_{\pi_K}$ be Lubin-Tate series for π_K and a linear form $L(X_1, \ldots, X_n) = \sum_{i=1}^n a_i X^i$ for some $a_i \in \mathcal{O}_K$. Then there exists a formal power series $F(X_1, \ldots, X_n) \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ such that $F(X_1, \ldots, X_n) \equiv L(X_1, \ldots, X_n) \pmod{(X_1, \ldots, X_n)^2}$ and $e_1(F(X_1, \ldots, X_n)) = F(e_2(X_1), \ldots, e_2(X_n))$.*

Proof. Proof omitted. □

Corollary 7.2.12. *Let K be a local field and π_K a uniformiser for K. Given a Lubin-Tate series $e \in \mathcal{E}_{\pi_K}$, there exists a unique power series $F_e(X, Y) \in \mathcal{O}_K[[X, Y]]$ such that*

$$F_e(X,Y) \equiv X + Y \pmod{(X,Y)^2}$$
$$e(F_e(X,Y))) = F_e(e(X), e(Y))$$

Corollary 7.2.13. *Let K be a local field and π_K a uniformiser for K. Given Lubin-Tate series, $e_1, e_2 \in \mathcal{E}_{\pi_K}$ and $a \in \mathcal{O}_K$, there exists a unique power series $[a]_{e_1,e_2}(X) \in \mathcal{O}_K[[X]]$ such that*

$$[a]_{e_1,e_2}(X) \equiv aX \pmod{X^2}$$
$$e_1([a]_{e_1,e_2}(X)) = [a]_{e_1,e_2}(e_2(X))$$

Moreover, if $e_1 = e_2 = e$ then we write $[a]_e = [a]_{e,e}$.

Theorem 7.2.14. *Let K be a local field with uniformiser π_K. Then the Lubin-Tate $\mathcal{O}_K$-modules are precisely the series $F_e(X,Y)$ with $e \in \mathcal{E}_{\pi_K}$ with formal $\mathcal{O}_K$-module structure given by*

$$a \mapsto [a]_e$$

Moreover, if $e_1, e_2 \in \mathcal{E}_{\pi_K}$ and $a \in \mathcal{O}_K$ then $[a]_{e_1,e_2}$ is a homomorphism $Fe_2 \to Fe_1$. If $a \in \mathcal{O}_K^\times$ then it is an isomorphism with inverse $[a^{-1}]_{e_2,e_1}$.

Proof. The proof of this theorem is lengthy but not hard, it amounts to using the uniqueness of all formal power series involved. □

7.3 Lubin-Tate Extensions

Throughout this section, let $\bar{K}$ be a fixed algebraic closure of a local field K and $\overline{\mathfrak{m}} = \mathfrak{m}_{\overline{K}}$ the unique maximal ideal of its ring of integers.

Proposition 7.3.1. *Let K be a local field. If F is a formal $\mathcal{O}_K$-module then $\overline{\mathfrak{m}}$ is an $\mathcal{O}_K$-module under the operations*

$$x +_F y = F(x,y) \text{ for } x, y \in \overline{\mathfrak{m}}$$
$$a \cdot x = [a]_F(x) \text{ for } a \in \mathcal{O}_K, x \in \overline{\mathfrak{m}}$$

Proof. If $x, y \in \overline{\mathfrak{m}}$ then $F(x,y)$ is a power series in $K(x,y) \subseteq \overline{K}$ with coefficients of absolute value less than 1. Since $K(x,y)$ is complete, this series thus converges to an alement of $\mathfrak{m}_{K(x,y)} \subseteq \overline{\mathfrak{m}}$. The rest of the assertions are now immediate from the definitions of formal groups. □

Definition 7.3.2. Let K be a local field with uniformiser π_K and F a Lubin-Tate module for π_K. Given $n \in \mathbb{N}_{\geq 1}$, we define the group of $\boldsymbol{\pi_K^n}$**-division points** of F to be

$$F(n) = \{\, x \in \overline{\mathfrak{m}_F} \mid \pi_K^n x = 0 \,\}$$

Example 7.3.3. Let $K = \mathbb{Q}_p$ with $\pi = p$ and consider the Lubin-Tate $\mathbb{Z}_p$-module F. Given $x \in F$ we have

$$p^n \cdot x = (1+x)^{p^n} - 1 = 0$$

so that $1 + x$ is a $(p^n)^{th}$ root of unity. In other words,

$$\widehat{\mathbb{G}_m}(n) = \{\, \zeta_{p^n}^i - 1 \mid 0 \leq i \leq p^n - 1 \,\}$$

where ζ_{p^n} is a primitive $(p^n)^{th}$ root of unity. We thus see that $\widehat{\mathbb{G}_m}(n)$ generates $\mathbb{Q}_p(\zeta_{p^n})$.

Lemma 7.3.4. *Let K be a local field with uniformiser π_K and $q = |\mathbb{F}_K|$. Let $e(X) = X^q + \pi_K X$ and $f_n(X) = e \circ \cdots \circ e$ with $f_0(X) = X$. Then f_n has no repeated roots.*

Proof. Fix $x \in \overline{K}$. We claim, by induction on n, that if $|f_i(x)| < 1$ for all $0 \leq i \leq n-1$ then $f_n'(x) \neq 0$. Indeed, first assume that $n = 1$. Then

$$f_1'(x) = e'(x) = qx^{q-1} + \pi_K = \pi_K \left(1 + \left(\frac{q}{\pi_K}\right) x^{q-1}\right)$$

Now, $|q/\pi_K| \leq 1$ since $q \equiv 0 \pmod{\pi_K}$ and $|x^{q-1}| < 1$ by hypothesis so $f_1'(x)$ cannot possibly vanish.

Now assume it holds true for arbitrary n. We have

$$f_{n+1}'(x) = (qf_n(x)^{q-1} + \pi_K)f_n'(x) = \pi_K \left(1 + \left(\frac{q}{\pi_K}\right) f_n(x)^{q-1}\right) f_n'(x)$$

By assumption, $|f_n(x)^{q-1}| < 1$ and $f_n'(X) \neq 0$ by the induction hypothesis so that $f_{n+1}(x)$ does not vanish.

To prove the lemma, assume that $f_n(x) = 0$. We claim that $|f_i(x)| < 1$ for all $0 \leq i \leq n-1$. If this were indeed the case then we would have that $f_n'(X) \neq 0$ by the claim. Indeed, by induction we have that

$$f_n(X) = X^{q^n} + \pi g_n(X)$$

for some $g_n(X) \in \mathcal{O}_K$. If $f_n(x) = 0$ then we must have that $|x| < 1$ whence $|f_i(x) < 1$ for all i. $\square$

Proposition 7.3.5. *Let K be a local field, π_K a uniformiser for K and $q = |\mathbb{F}_K|$. If F is a Lubin-Tate $\mathcal{O}_K$-module for π_K then $F(n)$ is a free $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module of rank 1. In particular, it has q^n elements.*

Proof. By Theorem 7.2.14, all Lubin-Tate $\mathcal{O}_K$-modules are isomorphic so all the $\mathcal{O}_K$-modules $F(n)$ are isomorphic. Now, by definition, $\pi^n F(n) = 0$ and so the $\mathcal{O}_K$-module structure on $F(n)$ descends to a $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module structure. Now let $F = F_e$ where $e(X) = X^q + \pi X$. Then $F(n)$ consists of the roots of the degree q^n polynomial $f_n(X) = e^n(X)$ which has no repeated roots by Lemma 7.3.4 so $|F(n)| = q^n$.

Now fix $\lambda_n \in F(n) \setminus F(n-1)$. Then we have a homomorphism of $\mathcal{O}_K$-modules

$$\begin{aligned} \mathcal{O}_K &\to F(n) \\ a &\mapsto a \cdot \lambda_n \end{aligned}$$

whose kernel is exactly $\pi^n\mathcal{O}_K$. But $|\mathcal{O}_K/\pi^n\mathcal{O}_K| = q^n = |F(n)|$ so this must be infact an isomorphism. $\square$

Corollary 7.3.6. *Let K be a local field and π_K a uniformiser for K. If F is a Lubin-Tate $\mathcal{O}_K$-module for π_K then*

$$\begin{aligned} \mathcal{O}_K/\pi^n\mathcal{O}_K &\cong \mathrm{End}_{\mathcal{O}_K}(F(n)) \\ U_K/U_K^{(n)} &\cong \mathrm{Aut}_{\mathcal{O}_K}(F(n)) \end{aligned}$$

Definition 7.3.7. Let K be a local field, π_K a uniformiser for K and F a Lubin-Tate $\mathcal{O}_K$-module for π_K. We define the **field of $\boldsymbol{\pi_K^n}$-division points** of F to be $L_{n,\pi} = L_n = K(F(n))$.

Remark. Let F and G be two Lubin-Tate $\mathcal{O}_K$-modules for π_K. Then $K(G(n)) = K(F(n))$. Indeed, there exits an isomorphism of formal $\mathcal{O}_K$-modules $f : F \to G$. Then $G(n) = f(F(n)) \subseteq K(F(n))$. By symmetry, $K(G(n)) \subseteq K(F(n))$.

Theorem 7.3.8. *Let K be a local field, $\pi = \pi_K$ a uniformiser and F a Lubin-Tate $\mathcal{O}_K$-module for π_K. Then $L_{n,\pi}/K$ is a totally ramified abelian extension of degree $q^{n-1}(q-1)$*

with Galois group $\mathrm{Aut}_{\mathcal{O}_K}(F(n)) \cong U_K/U_K^{(n)}$*. More explicitly, given* $\sigma \in \mathrm{Gal}(L_n/K)$ *there exists a unique* $u \in U_K/U_K^{(n)}$ *such that*

$$\sigma(\lambda) = [u]_F(\lambda) \text{ for all } \lambda \in F(n)$$

Moreover, if $F = F_e$ *where* $e(X) = X^q + \pi(a_{q-1}X^{q-1} + \cdots + a_2X^2) + \pi X$ *is a Lubin-Tate polynomial and* $\lambda_n \in F(n)\backslash F(n-1)$ *then* λ_n *is a uniformiser of* L_n *and*

$$\Phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = X^{q^n(q-1)} + \cdots + \pi$$

is the minimal polynomial of λ_n *and, in particular,* $\mathbf{N}_{L_n/K}(-\lambda_n) = \pi$.

Finally, the above isomorphism induces an isomorphism

$$\mathrm{Gal}(L_m/L_n) \cong {}^{U_K^{(n)}}\!\big/_{U_K^{(m)}}$$

for all $m \geq n$.

Proof. Fix a Lubin-Tate polynomial

$$e(X) = X^q + \pi(a_{q-1}X^{q-1} + \cdots + a_2X^2) + \pi X$$

and set $F = F_e$. Then

$$\Phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = [e^{n-1}(X)]^{q-1} + \pi(a_{q-1}[e^{n-1}(X)]^{q-2} + \cdots + a_2e^{n-1}(X)]) + \pi$$

is Eisenstein at π and is of degree $q^{n-1}(q-1)$. If $\lambda_n \in F(n) \setminus F(n-1)$ then λ_n is a root of $\Phi_n(X)$ so that $K(\lambda_n)/K$ is totally ramified of degree $q^{n-1}(q-1)$ and λ_n is a uniformiser of this extension with $\mathbf{N}_{K(\lambda_n)/K}(\lambda_n) = \pi$.

Now fix $\sigma \in \mathrm{Gal}(L_n/K)$. Then σ induces a permutation of $F(n)$ which is $\mathcal{O}_K$-linear. Indeed,

$$\sigma(x) +_F \sigma(y) = F(\sigma(x), \sigma(y)) = \sigma(F(x,y) = \sigma(x +_F y)$$
$$\sigma(a \cdot x) = \sigma([a]_F(x)) = [a]_F(\sigma(x) = a \cdot \sigma(x)$$

for all $x, y \in \overline{\mathfrak{m}_{L_n}}$ and $a \in \mathcal{O}_K$. We thus have an injective homomorphism

$$\mathrm{Gal}(L_n/K) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(F(n)) \cong {}^{U_K}\!\big/_{U_K^{(n)}}$$

But by Proposition 5.4.2 we have

$$\left| {}^{U_K}\!\big/_{U_k^{(n)}} \right| = q^{n-1}(q-1) = [K(\lambda_n) : K] \leq [L_n : K] = |\,\mathrm{Gal}(L_n/K)|$$

so we must have equality throughout so that $\mathrm{Gal}(L_n/K) \cong U_K/U_K^{(n)}$ and, moreover, $K(\lambda_n) = L_n$.

To prove the final assertion, note that we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L_m/K) & \xrightarrow{\sim} & {}^{U_K}\!\big/_{U_K^{(m)}} \\ \Big\downarrow{\scriptstyle \phi} & & \Big\downarrow{\scriptstyle \psi} \\ \mathrm{Gal}(L_n/K) & \xrightarrow{\sim} & {}^{U_K}\!\big/_{U_K^{(n)}} \end{array}$$

It is then clear that

$$\mathrm{Gal}(L_m/L_n) = \ker\phi \cong \ker\psi = {U_K^{(n)}}\big/{U_K^{(m)}}$$

□

Theorem 7.3.9. *Let K be a local field and π_K a uniformiser for K. Then the π_K^n-division field L_n has norm group*

$$\mathbf{N}(L_n/K) = \langle \pi_K \rangle \times U_K^{(n)}$$

Theorem 7.3.10 (Local Kronecker-Weber Theorem)**.** *Let K be a local field and π_K a uniformiser for K. If L_∞ denotes the union of all π_K^n-division fields then $K^{\mathrm{ab}} = K^{\mathrm{ur}} L_\infty$.*

Proof. Proof omitted. □

Theorem 7.3.11. *Let K be a local field and π_K a uniformiser for K. Then we have a topological isomorphism Art_K completing the diagram*

$$\begin{array}{ccccc} K^\times & \xrightarrow[\mathrm{Art}_K]{\sim} & W(K^{\mathrm{ab}}/K) & & \sigma \\ \downarrow \wr & & \downarrow \wr & & \downarrow \\ \langle \pi_K \rangle \times U_K & \xrightarrow{\sim} & W(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(L_\infty/K) & & (\sigma|_K, \sigma|_{L_\infty}) \end{array}$$

$$\langle \pi^m, u \rangle \longmapsto (\mathrm{Frob}_K^m, \sigma_u^{-1})$$

where σ_u is characterised by $\sigma_u(\lambda) = [u]_F(\lambda)$ for any $\lambda \in \bigcup_{i=1}^\infty F(n)$.

Proof. Proof omitted. □

7.4 Ramification Groups of Lubin-Tate Extensions

Theorem 7.4.1. *Let K be a local field with uniformiser $\pi = \pi_K$ and $q = |\mathbb{F}_K|$. Then*

$$G_s(L_n/K) = \begin{cases} \mathrm{Gal}(L_n/K) & \text{if } -1 \le s \le 0 \\ \mathrm{Gal}(L_n/L_k) & \text{if } q^{k-1} - 1 < s \le q^k - 1, 1 \le k \le n-1 \\ 1 & \text{if } s > q^{n-1} - 1 \end{cases}$$

Proof. Since L_n/K is totally ramified, $\mathrm{Gal}(L_n/K)$ coincides with its inertia subgroup so the case where $-1 \le s \le 0$ is clear. Now suppose that $0 < s \le 1$. Since jump-points occur at integers, it suffices to determine $G_1(L/K)$. By Corollary 5.4.11, $G^1(L/K)$ is a p-Sylow subgroup of $\mathrm{Gal}(L_n/K) \cong U_K/U_K^{(n)}$. This group has order $q^{n-1}(q-1)$ so that $G_s(L_n/K)$ is the unique subgroup of order q^{n-1}. But this is exactly $U_K^{(1)}/U_K^{(n)} \cong \mathrm{Gal}(L_n/L_1)$ so the Theorem is true in this case. □

Now fix $1 \ne u \in U_K^{(1)}/U_K^{(n)}$ and let $\sigma_u \in G_1(L_n/K)$ be the corresponding automorphism. Write $u = 1 + \varepsilon\pi^k$ for some $\varepsilon \in U_K$ and $1 \le k = k(u) < n$. Fix a Lubin-Tate $\mathcal{O}_K$-module F for π_K and $\lambda \in F(n) \setminus F(n-1)$. Then λ is a uniformiser for L_n and so $\mathcal{O}_{L_n} = \mathcal{O}_K[\lambda]$. We claim that $i_{L_n/K}(\sigma_u) = v_{L_n}(\sigma(\lambda) - \lambda) = q^n$. Indeed, we have

$$\sigma_u(\lambda) = [u]_F(\lambda) = [1 + \varepsilon\pi^k]_F(\lambda) = F(\lambda, [\varepsilon\pi^k]_F(\lambda))$$

Now,

$$[\varepsilon\pi^k]_F(\lambda) = [\varepsilon]_F([\pi^k]_F(\lambda)) \in F(n-k)\backslash F(n-k-1)$$

so that $[\varepsilon\pi^k]_F(\lambda)$ is a uniformiser for L_{n-k}. Since L_n/L_{n-k} is totally ramified of degree q^k we must have that

$$[\varepsilon\pi^k]_F(\lambda) = \varepsilon_0\lambda^{q^k}$$

for some $\varepsilon \in \mathcal{O}_{L_n}^\times$. Now recall that $F(X,0) = X$ and $F(0,Y) = Y$ so that $F(X,Y) = X + Y + XYG(X,Y)$ for some $G(X,Y) \in \mathcal{O}_K$ so we have

$$\begin{aligned}
\sigma(\lambda) - \lambda &= F(\lambda, [\varepsilon\pi^k]_F(\lambda]) - \lambda \\
&= F(\lambda, \varepsilon_0\lambda^{q^k}) - \lambda \\
&= \lambda + \varepsilon_0\lambda^{q^k} + \varepsilon_0\lambda^{q^k+1}G(\lambda, \varepsilon_0\lambda^{q^k}) - \lambda \\
&= \varepsilon_0\lambda^{q^k} + \varepsilon_0\lambda^{q^k+1}G(\lambda, \varepsilon_0\lambda^{q^k})
\end{aligned}$$

so that

$$i_{L_n/K} = v_{L_n}(\sigma(\lambda) - \lambda)) = q^k$$

Hence

$$i_{L_n/K}(\sigma_u) \geq s+1 \iff q^{k(u)-1\leq s}$$

and therefore

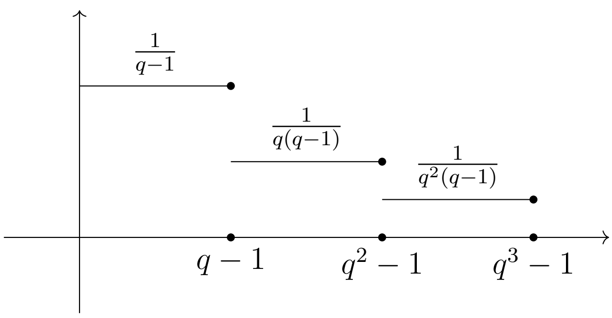
$$\begin{aligned}
G_s(L_n/K) &= \{\, \sigma_u \in G_1(L_n/K) \mid q^{k(u)} - 1 \geq s \,\} \\
&= \begin{cases} \mathrm{Gal}(L_n/L_k) & \text{if } q^{k-1} < s \leq q^k - 1, k = 1, \dots, n-1 \\ 1 & \text{if } s > q^{k-1} - 1 \end{cases}
\end{aligned}$$

Corollary 7.4.2. *Let K be a local field with uniformiser $\pi = \pi_K$ and $q = |\mathbb{F}_K|$. Then*

$$\begin{aligned}
G^t(L_n/K) &= \begin{cases} \mathrm{Gal}(L_n/K) & \textit{if } -1 \leq t \leq 0 \\ \mathrm{Gal}(L_n/L_k) & \textit{if } k-1 < t \leq k, 1 \leq k \leq n-1 \\ 1 & \textit{if } t > n-1 \end{cases} \\
&= \begin{cases} \mathrm{Gal}(L_n/L_{\lceil t \rceil}) & \textit{if } -1 \leq t \leq n-1 \\ 1 & \textit{if } t > n-1 \end{cases}
\end{aligned}$$

where we set $L_{-1} = L_0 = K$.

Proof. The function we need to integrate in order to obtain $\eta_{L_n/K}(s)$ is



After a moment's glance, we see that

$$\eta_{L_n/K}(s) = \begin{cases} s & \text{if } -1 \le s \le 0 \\ (k-1) + \dfrac{s-(q^{k-1}-1)}{q^{k-1}(q-1)} & \text{if } q^{k-1} \le s \le q^k - 1 \\ (n-1) + \dfrac{s-(q^{n-1}-1)}{q^{n-1}(q-1)} & \text{if } s > q^{n-1} \end{cases}$$

Inverting this, we have

$$\psi_{L_n/K}(t) = \begin{cases} t & \text{if } -1 \le t \le 0 \\ q^{\lceil t \rceil - 1}(q-1)(t - (\lceil t \rceil - 1)) + q^{\lceil t \rceil - 1} - 1 & \text{if } 1 \le t \le n-1 \\ q^{n-1}(q-1)(t-(n-1)) + q^{n-1} - 1 & \text{if } t > n-1 \end{cases}$$

Then

$$G^t(L_n/K) = G_{\psi_{L_n/K}(t)}(L_n/K)$$

is in the form asserted. □

Corollary 7.4.3. *Let K be a local field. Then*

$$\mathrm{Art}_K^{-1}(G^t(L_n/K)) = \begin{cases} U_K^{(\lceil t \rceil)} \big/ U_K^{(n)} & \textit{if } -1 \le t \le n-1 \\ 1 & \textit{if } t > n-1 \end{cases}$$

Lemma 7.4.4. *Let L/K be a finite unramified extension of local fields and M/K a finite totally ramified extension. Then LM/L is totally ramified and $\mathrm{Gal}(LM/L) \cong \mathrm{Gal}(M/K)$ via restriction to M. Moreover, $G^t(LM/K) \cong G^t(M/K)$ via this isomorphism when $t > -1$.*

Proof. Since L/K is unramified and M/K is totally ramified, we have $L \cap M = K$. Proposition 6.3.2 then implies that we have an isomorphism

$$\mathrm{Gal}(LM/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$$

But by Galois Theory, we have an isomorphism

$$\frac{\mathrm{Gal}(LM/K)}{\mathrm{Gal}(LM/L)} \cong \mathrm{Gal}(L/K)$$

We must therefore have that

$$\mathrm{Gal}(LM/L) \cong \{1\} \times \mathrm{Gal}(M/K) \cong \mathrm{Gal}(M/K)$$

The statement regarding the ramification groups is then immediately clear. □

Corollary 7.4.5. *Let K be a local field and $t > -1$. Then*

$$G^t(K^{\mathrm{ab}}/K) = \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}} L_{\lceil t \rceil})$$

and

$$\mathrm{Art}_K^{-1}(G^t(K^{\mathrm{ab}}/K)) = U_K^{(\lceil t \rceil)}$$

Proof. Let K_m/K be the unique unramified extension of K of degree m. By Lemma 7.4.4 and Corollary 7.4.2 we have

$$G^t(K_mL_n/K) \cong G^t(L_n/K) = \begin{cases} \mathrm{Gal}(L_n/L_{\lceil t\rceil}) & \text{if } -1 \le t \le n-1 \\ 1 & \text{if } t > n-1 \end{cases}$$

Now, $L_n/L_{\lceil t\rceil}$ is itself a totally ramified extension and $K_mL_{\lceil t\rceil}/L_{\lceil t\rceil}$ is unramified. Hence Lemma 7.4.4 again imples that

$$\mathrm{Gal}(K_mL_{\lceil t\rceil}L_n/K_mL_{\lceil t\rceil}) = \mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil}) \cong \mathrm{Gal}(L_n/L_{\lceil t\rceil})$$

So that

$$G^t(K_mL_n/K) = \begin{cases} \mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil}) & \text{if } -1 \le t \le n-1 \\ 1 & \text{if } t > n-1 \end{cases}$$

Hence

$$\begin{aligned} G^t(K^{\mathrm{ab}}/K) &= G^t(K^{\mathrm{ur}}L_\infty/K) \\ &= \varprojlim_{m,n} G^t(K_mL_n/K) \\ &= \varprojlim_{\substack{m,n \\ n\ge\lceil t\rceil}} \mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil}) \\ &= \mathrm{Gal}(K^{\mathrm{ur}}L_\infty/K^{\mathrm{ur}}L_{\lceil t\rceil}) \\ &= \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}L_{\lceil t\rceil}) \end{aligned}$$

Moreover,

$$\begin{aligned} \mathrm{Art}_K^{-1}(\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}L_{\lceil t\rceil})) &\cong \mathrm{Art}_K^{-1}\left(\varprojlim_{\substack{m,n \\ n\ge\lceil t\rceil}} \mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil})\right) \\ &\cong \varprojlim_{\substack{m,n \\ n\ge\lceil t\rceil}} \mathrm{Art}_K^{-1}(\mathrm{Gal}(K_mL_n/K_mL_{\lceil t\rceil})) \\ &\cong \varprojlim_{\substack{m,n \\ n\ge\lceil t\rceil}} U_K^{(\lceil t\rceil)} \big/ U_K^{(n)} \\ &\cong U_K^{(\lceil t\rceil)} \end{aligned}$$

□

Corollary 7.4.6. *Let L/K be a finite abelian extension of local fields. Then we have an isomorphism*

$$\mathrm{Art}_K : K^\times \big/ \mathbf{N}(L/K) \to \mathrm{Gal}(L/K)$$

Moreover, for $t > -1$ we have

$$G^t(L/K) = \mathrm{Art}_K\left(\frac{U_K^{(\lceil t\rceil)}\,\mathbf{N}(L/K)}{\mathbf{N}(L/K)}\right)$$

Proof. By Herbrand's theorem, the upper numbering on ramification groups is compatible with quotients so we have

$$G^t(L/K) = \frac{G^t(K^{\mathrm{ab}}/K)G(K^{\mathrm{ab}}/L)}{G(K^{\mathrm{ab}}/L)} = \mathrm{Art}_K\left(\frac{U_K^{(\lceil t\rceil)}\,\mathbf{N}(L/K)}{\mathbf{N}(L/K)}\right)$$

□