

Part III Local Fields

Based on lectures by Dr C. Johansson

Michaelmas 2016
University of Cambridge

Contents

1 Basic Theory	1
1.1 The p-adic Numbers	3
1.2 Valued Fields	4
1.3 Newton Polygons	6
1.4 *Witt Vectors*	11
2 Some p-adic Analysis	12
2.1 Mahler's Theorem	13
3 Ramification Theory for Local Fields	16
3.1 More on Finite Extensions	16
3.2 Totally Ramified Extensions	21
3.3 The Unit Group \mathcal{O}_K^\times	22
3.4 The Inertia Group	22
3.5 Higher Ramification Groups	23
3.6 Quotients	25
4 Local Class Field Theory	28
4.1 Infinite Galois Theory	28
4.2 Unramified Extensions and Weil Groups	30

1 Basic Theory

Definition 1 (Absolute value). Let K be a field. An **absolute value** on K is a function $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$ s.t.

- i. $|x| = 0 \iff x = 0$

ii. $|xy| = |x| |y| \quad \forall x, y \in K$

iii. $|x + y| \leq |x| + |y|$

Definition 2 (Valued field). A **valued field** is a field with an absolute value.

Definition 3 (Equivalence of absolute values). Let K be a field and let $|\cdot|, |\cdot|'$ be absolute values on K . We say that $|\cdot|$ and $|\cdot|'$ are **equivalent** if the associated metrics induce the same topology.

Definition 6 (Non-archimedean absolute value). An absolute value $|\cdot|$ on a field K is called **non-archimedean** if $|x + y| \leq \max(|x|, |y|)$ (the **strong triangle inequality**).

Metrics s.t. $d(x, z) \leq \max(d(x, y), d(y, z))$ are called **ultrametrics**.

Assumption: unless otherwise mentioned, all absolute values will be non-archimedean. These metrics are weird!

Proposition 7. Let K be a valued field. Then $\mathcal{O} = \{x \mid |x| \leq 1\}$ is an open subring of K , called the **valuation ring** of K . $\forall r \in (0, 1]$, $\{x \mid |x| < r\}$ and $\{x \mid |x| \leq r\}$ are open ideals of \mathcal{O} .

Moreover, $\mathcal{O}^\times = \{x \mid |x| = 1\}$.

Proposition 8. Let K be a valued field.

i. Let (x_n) be a sequence in K . If $x_n - x_{n+1} \rightarrow 0$ then (x_n) is Cauchy

Assume that K is complete

ii. Let (x_n) be a sequence in K . If $x_n - x_{n+1} \rightarrow 0$ then (x_n) converges

iii. Let $\sum_{n=0}^{\infty} y_n$ be a series in K . If $y_n \rightarrow 0$, then $\sum_{n=0}^{\infty} y_n$ converges

Definition 9. Let $R \subseteq S$ be rings. Then $s \in S$ is **integral over R** if \exists monic $f(x) \in R[x]$ s.t. $f(s) = 0$.

Proposition 10. Let $R \subseteq S$ be rings. Then $s_1, \dots, s_n \in S$ are all integral over $R \iff R[s_1, \dots, s_n] \subseteq S$ is a finitely generated R -module.

Corollary 11. let $R \subseteq S$ be rings. If $s_1, s_2 \in S$ are integral over R , then $s_1 + s_2$ and $s_1 s_2$ are integral over R . In particular, the set $\tilde{R} \subseteq S$ of all elements in S integral over R is a ring, called the **integral closure** of R in S .

Definition 12. Let R be a ring. A topology on R is called a **ring topology** on R if addition and multiplication are continuous maps $R \times R \rightarrow R$. A ring with a ring topology is called a **topological ring**.

Definition 13. Let R be a ring, $I \subseteq R$ an ideal. A subset $U \subseteq R$ is called **I-adically open** if $\forall x \in U \exists n \geq 1$ s.t. $x + I^n \subseteq U$.

Proposition 14. The set of all I -adically open sets form a topology on R , called the **I-adic topology**.

Definition 15. Let R_1, R_2, \dots be topological rings with continuous homomorphisms $f_n : R_{n+1} \rightarrow R_n \forall n \geq 1$. The **inverse limit** of the R_i is the ring

$$\begin{aligned} \varprojlim_n R_n &= \left\{ (x_n) \in \prod_n R_n \mid f_n(x_{n+1}) = x_n \forall n \geq 1 \right\} \\ &\subseteq \prod_n R_n \end{aligned}$$

Proposition 16. The inverse limit topology is a ring topology.

Definition 17. Let R be a ring, I an ideal. The **I-adic completion** of R is the topological ring $\varprojlim_n R/I^n$ (R/I^n has the discrete topology, and $R/I^{n+1} \rightarrow R/I^n$ is the natural map).

There exists a map $\nu : R \rightarrow \varprojlim_n R/I^n$, $r \mapsto (r \bmod I^n)_n$. This map is a continuous ring homomorphism when R is given the I -adic topology. We say that R is **I-adically complete** if ν is a bijection.

If $I = xR$ then we often call the I -adic topology the **x-adic topology**.

1.1 The p-adic Numbers

Let p be a prime number throughout.

If $x \in \mathbb{Q} \setminus \{0\}$ then $\exists!$ representation $x = p^n \frac{a}{b}$, where $n \in \mathbb{Z}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$ and $(a, p) = (b, p) = 1$.

We define the **p-adic absolute value** on \mathbb{Q} to be the function $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$ given by

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

Then $|\cdot|_p$ is an absolute value.

Definition 18. The **p-adic numbers** \mathbb{Q}_p are the completion of \mathbb{Q} w.r.t. $|\cdot|_p$.

The valuation ring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ is called the **p-adic integers**.

Proposition 19. \mathbb{Z}_p is the closure of \mathbb{Z} inside \mathbb{Q}_p .

Proposition 20. The non-zero ideals of \mathbb{Z}_p are $p^n \mathbb{Z}_p$ for $n \geq 0$. Moreover, $\mathbb{Z}/p^n \mathbb{Z} \cong \mathbb{Z}_p/p^n \mathbb{Z}_p$

Corollary 21. \mathbb{Z}_p is a PID with a unique prime element p (up to units).

Proposition 22. The topology on \mathbb{Z} induced by $|\cdot|_p$ is the p -adic topology.

Proposition 23. \mathbb{Z}_p is p -adically complete and is (isomorphic to) the p -adic completion of \mathbb{Z} .

Corollary 24. Every $a \in \mathbb{Z}_p$ has a unique expansion

$$a = \sum_{i=0}^{\infty} a_i p^i$$

with $a_i \in \{0, 1, \dots, p-1\}$

Every $a \in \mathbb{Q}_p^\times$ has a unique expansion

$$a = \sum_{i=n}^{\infty} a_i p^i$$

$n \in \mathbb{Z}$, $n = -\log_p |a|_p$, $a_n \neq 0$.

1.2 Valued Fields

Definition 25. Let K be a field. A **valuation** on K is a function $v : K \rightarrow \mathbb{R} \cup \{\infty\}$ s.t.

- i. $v(x) = \infty \iff x = 0$
- ii. $v(xy) = v(x) + v(y)$
- iii. $v(x + y) \geq \min(v(x), v(y))$

$\forall x, y \in K$.

Here we use the conventions $r + \infty = \infty$, $r \leq \infty \forall r \in \mathbb{R} \cup \{\infty\}$. v a valuation \implies if $|x| = c^{-v(x)}$, $c \in \mathbb{R}_{>1}$, then $|\cdot|$ is an absolute value. Conversely, if $|\cdot|$ is an absolute value then $v(x) = -\log_c |x|$.

Let K be a valued field.

- $\mathcal{O} = \mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ is the **valuation ring**
- $\mathfrak{m} = \mathfrak{m}_K = \{x \in K \mid |x| < 1\}$ is the **maximal ideal**
- $k = k_K = \mathcal{O}/\mathfrak{m}$ is the **residue field**

If K is a valued field and $F(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$ is a polynomial, we say that F is **primitive** if $\max_i |a_i| = 1$ ($\implies F \in \mathcal{O}[x]$).

Theorem 26 (Hensel's Lemma). *Assume that K is complete and that $F \in K[x]$ is primitive. Put $f = F \bmod \mathfrak{m} \in k[x]$. If \exists factorisation $f(x) = g(x)h(x)$ with $(g, h) = 1$, then \exists factorisation $F(x) = G(x)H(x)$ in $\mathcal{O}[x]$ with $g \equiv G, h \equiv H \bmod \mathfrak{m}$ and $\deg g = \deg G$.*

Proof. Put $d = \deg F$, $m = \deg g$, so $\deg h \leq d - m$. Pick lifts $G_0, H_0 \in \mathcal{O}[x]$ of g, h with $\deg G_0 = \deg g$, $\deg H_0 \leq d - m$.

$$(g, h) = 1 \implies \exists A, B \in \mathcal{O}[x] \text{ s.t. } AG_0 + BH_0 \equiv 1 \bmod \mathfrak{m}.$$

$$\text{Pick } \pi \in \mathfrak{m} \text{ s.t. } F - G_0H_0 \equiv AG_0 + BH_0 - 1 \bmod \pi.$$

Want to find $G = G_0 + \pi P_1 + \pi^2 P_2 + \dots$, $H = H_0 + \pi Q_1 + \pi^2 Q_2 + \dots \in \mathcal{O}[x]$ with $P_i, Q_i \in \mathcal{O}[x]$, $\deg P_i < m$, $\deg Q_i \leq d - m$.

Define

$$G_{n-1} = G_0 + \pi P_1 + \dots + \pi^{n-1} P_{n-1}$$

$$H_{n-1} = H_0 + \pi Q_1 + \dots + \pi^{n-1} Q_{n-1}$$

We want $F \equiv G_{n-1}H_{n-1} \bmod \pi^n$, then take the limit.

Induction on n : $n = 1$ ✓

Assume we have G_{n-1}, H_{n-1} , $G_n = G_{n-1} + \pi^n P_n$, $H_n = H_{n-1} + \pi^n Q_n$.

Expanding $F - H_n G_n$, we want

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

and divide by π^n

$$G_{n-1}Q_n + H_{n-1}P_n = \frac{1}{\pi^n} (F - G_{n-1}H_{n-1}) \bmod \pi$$

Let $F_n := F - G_{n-1}H_{n-1}$. $AG_0 + BH_0 \equiv 1 \bmod \pi \implies F_n \equiv AG_0F_n + BH_0F_n \bmod \pi$.

Write $BF_n = QG_0 + P_n$ with $\deg P_n < \deg G_0$, $P_n \in \mathcal{O}[x]$

$$\implies G_0(AF_n + H_0Q) + H_0P_n \equiv F_n \bmod \pi$$

Now omit all coefficients from $AF_n + H_0Q$ divisible by π to get Q_n . □

Corollary 27. *Let $F(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$, K complete, $a_0a_n \neq 0$. If F is irreducible, then $|a_i| \leq \max(|a_0|, |a_n|) \forall i$.*

Corollary 28. *$F \in \mathcal{O}[x]$ monic, K complete. If $F \bmod \mathfrak{m}$ has a simple root $\bar{\alpha} \in k$, then F has a (unique) simple root $\alpha \in \mathcal{O}$ lifting $\bar{\alpha}$.*

Useful fact: let K be a valued field, $x, y \in K$. $|x| > |y| \implies |x + y| = |x|$.
More generally, if we have a convergent series $\sum_{i=0}^{\infty} x_i$ and the non-zero $|x_i|$ are distinct, then $|x| = \max |x_i|$.

Theorem 29. *Let K be a complete valued field and let L/K be a finite extension. Then the absolute value $|\cdot|$ on K has a unique extension to an absolute value $|\cdot|_L$ on L , given by*

$$|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|}, \quad n = [L : K]$$

and L is complete w.r.t. $|\cdot|_L$.

Corollary 30. *Let K be a complete valued field. If M/K is an algebraic extension of K , then $|\cdot|$ extends uniquely to an absolute value on M .*

Corollary 31. *In the setting of Theorem 16, if $\sigma \in \text{Aut}(L/K)$ then $|\sigma(\alpha)|_L = |\alpha|_L \quad \forall \alpha \in L$*

Definition 32. Let K be a valued field and V a vector space over K . A **norm** on V is a function $\|\cdot\| : V \rightarrow \mathbb{R}_{\geq 0}$ such that

- i. $\|x\| = 0 \iff x = 0$
- ii. $\|\lambda x\| = |\lambda| \|x\| \quad \forall \lambda \in K, x \in V$
- iii. $\|x + y\| \leq \max(\|x\|, \|y\|) \quad \forall x, y \in V$

Two norms $\|\cdot\|, \|\cdot\|'$ are **equivalent** if they induce the same topology on V
 $\iff \exists C, D > 0$ s.t. $C \|x\| \leq \|x\|' \leq D \|x\| \quad \forall x \in V$.

Proposition 33. *Let K be a complete valued field and V a finite dimensional K -vector space. Let x_1, \dots, x_n be a basis of V , then if $x = \sum a_i x_i \in V$,*

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

defines a norm on V , and V is complete w.r.t $\|\cdot\|_{\max}$.

Moreover, if $\|\cdot\|$ is any norm on V , then $\|\cdot\|$ is equivalent to $\|\cdot\|_{\max}$ and hence V is complete w.r.t $\|\cdot\|$.

Lemma 34. *Let K be a valued field. Then \mathcal{O}_K is integrally closed in K .*

Corollary 35. *Let K be a complete valued field, L/K finite. Equip L with $|\cdot|_L$ extending $|\cdot|$ on K . Then \mathcal{O}_L is the integral closure of \mathcal{O}_K inside L .*

1.3 Newton Polygons

Definition. $S \subset \mathbb{R}^2$ is **lower convex** if

- i. $(x, y) \in S \implies (x, z) \in S \quad \forall z \geq y$
- ii. S is convex

Given any $T \subset \mathbb{R}^2$, there exists a minimal lower convex $LCH(T) \supseteq T$ ($LCH(T) = \bigcap_{T \subset S', S' \text{ lower convex}} S'$).

Definition. Let $f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$ where K is a valued field, v a valuation on K .

Define the **Newton polygon** of f as $LCH \left(\left\{ (i, v(a_i)) \mid \begin{array}{l} i = 0, 1, \dots, n \\ a_i \neq 0 \end{array} \right\} \right)$.

Definition. The horizontal length of a line segment is called the **multiplicity**. Line segments have a **slope**.

Theorem 36. Let K be a complete valued field, v a valuation on K , $f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$. Let L be the splitting field of f over K , equipped with the unique extension w of v .

If $(r, v(a_r)) \rightarrow (s, v(a_s))$ is a line segment of the Newton polygon of f with slope $-m \in \mathbb{R}$, then f has precisely $s - r$ roots of valuation m .

Proof. Dividing by a_n only shifts the NP vertically, so wlog $a_n = 1$.

Number the roots of f s.t.

$$\begin{array}{ccccccc} v(\alpha_1) & = & \dots & = & v(\alpha_{s_1}) & = & m_1 \\ v(\alpha_{s_1+1}) & = & \dots & = & v(\alpha_{s_2}) & = & m_2 \\ \vdots & & & & \vdots & & \vdots \\ v(\alpha_{s_t+1}) & = & \dots & = & v(\alpha_{s_{t+1}}) & = & m_{t+1} \end{array}$$

where $m_1 < m_2 < \dots < m_{t+1}$, and the α_i are the roots of f with multiplicity.

$$v(a_n) = v(1) = 0$$

$$v(a_{n-1}) = v(\sum_i a_i) \geq \min_i v(\alpha_i) = m_1$$

$$v(a_{n-2}) \geq \min_{i \neq j} v(\alpha_i \alpha_j) = 2m_1$$

$$v(a_{n-s_1}) = v(\sum_{i_1, \dots, i_{s_1} \text{ distinct}} \alpha_{i_1} \dots \alpha_{i_{s_1}}) = s_1 m_1$$

$$v(a_{n-s_1-1}) \geq \min v(\alpha_{i_1} \dots \alpha_{i_{s_1+1}}) = s_1 m_1 + m_2$$

$$\vdots$$

$$v(a_{n-s_2}) = \min v(\alpha_{i_1} \dots \alpha_{i_{s_2}}) = s_1 m_1 + (s_2 - s_1) m_2$$

etc. Drawing the lines between the points $(n, 0)$, $(n - s_1, s_1 m_1)$, \dots gives

the NP of f .

The first line segment has length $n - (n - s_1) = s_1$ and slope $\frac{0 - s_1 m_1}{n - (n - s_1)} = -m_1$. For $k \geq 2$, the k th line segment has length $(n - s_{k-1}) - (n - s_k) = s_k - s_{k-1}$ and slope

$$\begin{aligned} & \frac{(s_1 m_1 + \sum_{i=1}^{k-2} (s_{i+1} - s_i) m_{i+1}) - (s_1 m_1 + \sum_{i=1}^{k-1} (s_{i+1} - s_i) m_{i+1})}{(n - s_{k-1}) - (n - s_k)} \\ &= \frac{-(s_k - s_{k-1}) m_k}{s_k - s_{k-1}} = -m_k \end{aligned}$$

□

Corollary 37. *If f is irreducible, then the NP has a single line segment.*

Proof. we need to show that all roots have the same valuation. Let α, β be roots in the splitting field L . Then $\exists \sigma \in \text{Aut}(L/K)$ s.t. $\sigma(\alpha) = \beta$. So $v(\alpha) = v(\sigma(\alpha)) = v(\beta)$ by Corollary 30. □

Definition 38. Let K be a valued field with valuation v . K is a **discretely valued field** (DVF) if $v(K^\times) \subset \mathbb{R}$ is a discrete subgroup of \mathbb{R} ($\iff v(K^\times)$ is infinite cyclic).

Definition 39. A complete DVF with finite residue field is called a **local field**.

Let K be a DVF. $\pi \in K$ is called a **uniformiser** if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$ ($\iff v(\pi)$ has minimal positive valuation).

Proposition 40. *Let K be a DVF, uniformiser π . Let $S \subset \mathcal{O}_K$ be a set of coset representatives of $\mathcal{O}_K/\mathfrak{m}_K = k_K$ containing 0. Then*

1. *The non-zero ideals of \mathcal{O}_K are $\pi^n \mathcal{O}_K$, $n \geq 0$*
2. *\mathcal{O}_K is a PID with unique prime π (up to units), $\mathfrak{m}_K = \pi \mathcal{O}_K$*
3. *The topology on \mathcal{O}_K induced by $|\cdot|$ 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 $x \in K$ can be written uniquely as*

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

with $a_n \in S$ and $|x| = |p|^{-\inf\{n \mid a_n \neq 0\}}$

6. *The completion \hat{K} of K is a DVF, π is a uniformiser and*

$$\mathcal{O}_K/\pi^n \mathcal{O}_K \xrightarrow{\sim} \mathcal{O}_{\hat{K}}/\pi^n \mathcal{O}_{\hat{K}}$$

via the natural map.

Proof. The same as for \mathbb{Q}_p and \mathbb{Z}_p (use π instead of p). Note that $|\hat{K}| = |K|$ by Ex 9, sheet 1 ($\implies \hat{K}$ is a DVF). □

Proposition 41. *Let K be a DVF. Then K is a local field $\iff \mathcal{O}_K$ is compact*

Proof. \mathcal{O}_K compact $\implies \pi^{-n}\mathcal{O}_K$ is compact $\forall n \geq 0$ (π uniformiser).

$\mathcal{O}_K \cong \pi^{-n}\mathcal{O}_K \implies K = \bigcup_{n \geq 0} \pi^{-n}\mathcal{O}_K$ is complete.

Also $\mathcal{O}_K \rightarrow k_K$ and this map is continuous when k_K is given the discrete topology. So k_K is compact and discrete $\implies k_K$ finite.

Conversely, we seek to prove that K local $\implies \mathcal{O}_K$ is sequentially compact (\iff compact). Note that $\mathcal{O}_K/\pi^n\mathcal{O}_K$ is finite $\forall n \geq 0$ (induction and $\pi^{n-1}\mathcal{O}_K/\pi^n\mathcal{O}_K \cong \mathcal{O}_K/\pi\mathcal{O}_K$).

Let (x_i) be a sequence in \mathcal{O}_K . \exists a subsequence (x_{1i}) which is constant modulo π . Keep going: choose a subsequence $(x_{n+1,i})$ of (x_{ni}) s.t. $(x_{n+1,i})$ is constant mod π^{n+1} .

Then $(x_{ii})_{i=1}^\infty$ converges: it's Cauchy since $|x_{ii} - x_{jj}| \leq |\pi|^j \forall j \leq i$, and K is complete. \square

Definition 42. A ring R is called a **discrete valuation ring** (DVR) if it is a PID with a unique prime element (up to units).

Proposition 43. R is a DVR $\iff R \cong \mathcal{O}_K$ for some DVF K .

Proof. The reverse implication is contained in Proposition 42.

Suppose R is a DVR, π prime. $\forall x \in R \setminus \{0\}$, $\exists! u \in R^\times$, $n \in \mathbb{Z}_{\geq 0}$ such that $x = \pi^n u$ by uniqueness of prime factorisation.

Define $v(x) = \begin{cases} n & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

v defines a discrete valuation of $R \implies v$ extends uniquely to $K = \text{Frac}(R)$.

It remains to show that $R = \mathcal{O}_K$. First, note that $K = R[\frac{1}{\pi}]$. Any non-zero element looks like $\pi^n u$, $u \in R^\times$, $n \in \mathbb{Z}$, so it is invertible.

Then $v(\pi^n u) = n \in \mathbb{Z}_{\geq 0} \iff \pi^n u \in R$

$\therefore R = \mathcal{O}_K$. \square

Definition 44. Let K be a valued field with residue field k_K . K has **equal characteristic** if $\text{char } K = \text{char } k_K$, **mixed characteristic** otherwise ($\implies \text{char } K = 0, \text{char } k_K > 0$).

Definition 45. Let R be a ring of characteristic p . R is **perfect** if the Frobenius map $x \mapsto x^p$ is an automorphism of R .

Theorem 46. Let K be a complete DVF of equal characteristic p and assume that k_K is perfect. Then $K \cong k_K[[T]]$ (as DVFs).

Corollary 47. Let K be a local field of equal characteristic p . Have $k_K \cong \mathbb{F}_q$ for some q a power of p , and $K \cong \mathbb{F}_q((T))$.

Definition 48. Let K be a DVF. The **normalised valuation** v_K on K is the unique valuation on K in the given equivalence class s.t. $v_K(\pi) = 1$ for any uniformiser π .

Lemma 49. Let R be a ring and let $x \in R$. Assume that R is x -adically complete and that R/xR is perfect of characteristic p .

Then $\exists!$ map $[-] : R/xR \rightarrow R$ such that

$$\begin{aligned} [a] &\equiv a \pmod{x} \\ [ab] &= [a][b] \quad \forall a, b \in R/xR \end{aligned}$$

Moreover if R has characteristic p , then $[-]$ is a ring homomorphism.

Proof. Let $a \in R/xR$. $\exists! a^{p^{-n}} \in R/xR \quad \forall n \geq 0$ since R/xR is perfect. Now lift arbitrarily: take $\alpha_n \in R$ such that $\alpha_n \equiv a^{p^{-n}} \pmod{x}$.

Put $\beta_n = \alpha_n^{p^n}$.

Claim: $\lim_{n \rightarrow \infty} \beta_n$ exists and is independent of choices. Call this $[a]$.

Note that if the limit exists no matter how the α_n are chosen, then it is independent of the choices.

Want to prove $\beta_{n+1} - \beta_n \rightarrow 0$ x -adically.

$$\begin{aligned} \beta_{n+1} - \beta_n &= (\alpha_{n+1}^p)^{p^n} - (\alpha_n)^{p^n} \\ \alpha_{n+1}^p &\equiv (a^{p^{-n-1}})^p \equiv a^{p^{-n}} \equiv \alpha_n \pmod{x} \end{aligned}$$

The binomial theorem, R/xR characteristic p and induction \implies

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

i.e. $\beta_{n+1} - \beta_n \equiv 0 \pmod{x^{n+1}}$ so $\lim_{n \rightarrow \infty} \beta_n$ exists.

Multiplicativity: if $b \in R/xR$, with $\gamma_n \in R$ lifting $b^{p^{-n}} \quad \forall n \geq 0$, then $\alpha_n \gamma_n$ lifts $(ab)^{p^{-n}} = a^{p^{-n}} b^{p^{-n}}$

$$\implies [ab] = \lim_{n \rightarrow \infty} \alpha_n^{p^n} \lim_{n \rightarrow \infty} \gamma_n^{p^n} = [a][b]$$

$[a] \equiv a \pmod{x}$:

$$\lim_{n \rightarrow \infty} \alpha_n^{p^n} \equiv \lim_{n \rightarrow \infty} (a^{p^{-n}})^{p^n} \equiv \lim_{n \rightarrow \infty} a \equiv a \pmod{x}$$

Uniqueness: let $\phi : R/xR \rightarrow R$ be another map with these properties.

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

since $\phi(a^{p^{-n}}) \equiv a^{p^{-n}} \pmod{x}$ and ϕ is multiplicative.

Finally, if R has characteristic p , then $\alpha_n + \gamma_n$ lifts $a^{p^{-n}} + b^{p^{-n}} - (a+b)p^{-n}$, so

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

So $[-]$ is additive and multiplicative and (check!) $[1] = 1$, so it's a homomorphism. \square

Definition 50. $[-] : R/xR \rightarrow R$ is called the **Teichmüller map/lift** and $[x]$ is called the **Teichmüller lift/representative** of x .

Proof of Theorem 48. K is a complete DVF. We want to prove that $\mathcal{O}_K \cong k_K[[T]]$.

$\mathcal{O}_K \text{ char } p \implies [-] : k_K \hookrightarrow \mathcal{O}_K$ is an injective ring homomorphism.

Choose a uniformiser $\pi \in \mathcal{O}_K$. Then $k_K = \mathcal{O}_K/\pi\mathcal{O}_K$, \mathcal{O}_K π -adically complete. Now define

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

It's a bijection by one of the basic properties of complete DVFs, check it's a homomorphism. \square

Fact: let F be a field of characteristic p . Then F is perfect \iff every finite extension of F is separable.

\mathbb{F}_q is perfect for every $q = p^n$.

1.4 *Wiff Vectors*

Definition 51. Let A be a ring. A is called a **strict p -ring** if A is p -torsionfree, p -adically complete and A/pA is perfect.

Proposition 52. Let $X = \{x_i \mid i \in I\}$ be a set. Let

$$\begin{aligned} B &= \mathbb{Z}[x_i^{p^{-\infty}} \mid i \in I] \\ &= \bigcup_{n=0}^{\infty} \mathbb{Z}[x_i^{p^{-n}} \mid i \in I] \end{aligned}$$

(Note that $\mathbb{Z}[x_i \mid i \in I] \subseteq \mathbb{Z}[x_i^{p^{-1}} \mid i \in I] \subseteq \dots$) and let A be the p -adic completion of B . Then A is a strict p -ring, and $A/pA \cong \mathbb{F}_p[x_i^{p^{-\infty}} \mid i \in I]$ (think of as 'universal perfect rings').

Lemma 53. Let A and B be strict p -rings and let $f : A/pA \rightarrow B/pB$ be a ring homomorphism. Then $\exists!$ homomorphism $F : A \rightarrow B$ such that $f \equiv F \pmod{p}$.

F is explicitly given by $F(\sum_{n=0}^{\infty} [a_n] p^n) = \sum_{n=0}^{\infty} [f(a_n)] p^n$.

Theorem 54. *Let R be a perfect ring. Then $\exists!$ (up to isomorphism) strict p -ring $W(R)$ (called the **Wiff vectors** of R) such that $W(R)/pW(R) \cong R$. Moreover, if R' is another perfect ring the reduction mod p map gives a bijection*

$$\text{Hom}_{\text{Ring}}(W(R), W(R')) \xrightarrow{\sim} \text{Hom}_{\text{Ring}}(R, R')$$

Proposition 55. *A complete DVR A of mixed characteristic with perfect residue field and such that p is a uniformiser is the same as a strict p -ring A such that A/pA is a field.*

Definition 56. Let R be a mixed characteristic DVR with normalised valuation v_R . The integer $v_R(p)$ where p is the characteristic of the residue field of R is called the **absolute ramification index** of R .

Corollary 57. *Let R be a CDVR of mixed characteristic with absolute ramification index 1 and perfect residue field k . Then $R \cong W(k)$.*

Lemma 53'. *Let A be a strict p -ring and let B be a p -adically complete ring. If $f : A/pA \rightarrow B/pB$ is a ring homomorphism, then $\exists!$ ring homomorphism $F : A \rightarrow B$ with $f \equiv F \pmod{p}$.*

Theorem 58. *Let R be a CDVR of mixed characteristic with perfect residue field k and uniformiser π . Then R is finite over $W(k)$.*

Corollary 59. *Let K be a mixed characteristic local field. Then K is a finite extension of \mathbb{Q}_p .*

2 Some p -adic Analysis

Recall the power series

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

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

Proposition 60. *Let K be a complete valued field with absolute value $|\cdot|$, and assume that $K \supseteq \mathbb{Q}_p$, $|\cdot|_{\mathbb{Q}_p} = |\cdot|_p$. Then $\exp(x)$ converges for $|x| < p^{-\frac{1}{p-1}}$ and $\log(1+x)$ converges for $|x| < 1$, and they define continuous maps*

$$\exp : \left\{ x \in K \mid |x| < p^{-\frac{1}{p-1}} \right\} \rightarrow \mathcal{O}_K$$

$$\log : \{ x \in K \mid |x| < 1 \} \rightarrow K$$

Proof. $v = -\log_p |\cdot|$, this extends v_p .

$$\log: v(n) \leq \log_p n \implies$$

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

if $v(x) > 0$.

$$\text{exp: } v(n!) = \frac{n - s_p(n)}{p-1}. \text{ Then}$$

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

and $\rightarrow \infty$ as $n \rightarrow \infty$ if $v(x) > \frac{1}{p-1}$.

For continuity, we use uniform convergence as in the real case. \square

Lemma 53". *Let A be a strict p -ring, B a ring with element $x \in B$ such that B is x -adically complete and B/xB is perfect of characteristic p . If $f : A/pA \rightarrow B/pB$ is a ring homomorphism, then $\exists!$ ring homomorphism $F : A \rightarrow B$ with $f \equiv F \pmod{p}$.*

Let $n \geq 1$.

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

is a polynomial in x , and so defines a continuous function $\mathbb{Z}_p \rightarrow \mathbb{Q}_p$, $x \mapsto \binom{x}{n}$.

Since $\binom{x}{n} \in \mathbb{Z}$ if $x \in \mathbb{Z}_{\geq 0}$, by the density of $\mathbb{Z}_{\geq 0} \subset \mathbb{Z}_p$ we must have $\binom{x}{n} \in \mathbb{Z}_p \forall x \in \mathbb{Z}_p$.

When $n = 0$, set $\binom{x}{0} = 1 \forall x \in \mathbb{Z}_p$.

2.1 Mahler's Theorem

Theorem 61 (Mahler). *Let $f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ be a continuous function. Then \exists a unique sequence $(a_n)_{n \geq 0}$ with $a_n \in \mathbb{Q}_p$, $a_n \rightarrow 0$ such that*

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n} \quad \forall x \in \mathbb{Z}_p$$

and $\sup_{x \in \mathbb{Z}_p} |f(x)|_p = \max_{n=0,1,\dots} |a_n|_p$.

Let $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) = \{f : \mathbb{Z}_p \rightarrow \mathbb{Q}_p \text{ cts}\}$. This is a \mathbb{Q}_p -vector space.

If $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$, set $\|f\| = \sup_{x \in \mathbb{Z}_p} |f(x)|_p$. \mathbb{Z}_p compact $\implies f$ is bounded, so the supremum exists and is attained.

Let c_0 denote the set of sequences $(a_n)_{n=0}^{\infty}$ in \mathbb{Q}_p such that $a_n \rightarrow 0$. This is a \mathbb{Q}_p -vector space, with a norm $\|(a_n)\| = \max_{n=0,1,\dots} |a_n|_p$, and c_0 is complete w.r.t $\|\cdot\|$.

Define $\Delta : \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) \rightarrow \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ by $\Delta f(x) = f(x+1) - f(x)$. By induction,

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

Note that Δ defines a linear operator on $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$, and

$$|\Delta f(x)|_p = |f(x+1) - f(x)|_p \leq \|f\| \implies \|\Delta f\| \leq \|f\| \text{ or } \|\Delta\| \leq 1$$

Definition 62. Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. The **n th Mahler coefficient** $a_n(f) \in \mathbb{Q}_p$ is defined by

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

Lemma 63. Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. Then $\exists k \geq 1$ such that $\left\| \Delta^{p^k} f \right\| \leq \frac{1}{p} \|f\|$.

Proof. If $f = 0$ there's nothing to prove, so wlog $\|f\| = 1$ (by scaling). Then we want to show that $\Delta^{p^k} f(x) \equiv 0 \pmod{p} \forall x \in \mathbb{Z}_p$, some $k \geq 1$.

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

because $\binom{p^k}{i} \equiv 0 \pmod{p}$ for $i = 1, 2, \dots, p^k - 1$ and $(-1)^{p^k} \equiv -1 \pmod{p}$.

Now \mathbb{Z}_p compact $\implies f$ is uniformly continuous, so $\exists k$ such that $|x - y|_p \leq p^{-k} \implies |f(x) - f(y)|_p \leq \frac{1}{p} \forall x, y \in \mathbb{Z}_p$. Take this k , and we're done. \square

Proposition 64. The map $f \mapsto (a_n(f))_{n=0}^\infty$ defines an injective norm-decreasing linear map $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) \rightarrow c_0$.

Proof. First we prove that $a_n(f) \rightarrow 0$. We have $|a_n(f)|_p \leq \|\Delta^n f\|$, so it suffices to prove that $\|\Delta^n f\| \rightarrow 0$. Since $\|\Delta\| \leq 1$, $\|\Delta^n f\|$ is monotonically decreasing, so it suffices to find a subsequence $\rightarrow 0$.

Apply Lemma 63 repeatedly to get k_1, k_2, \dots such that

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

This gives the desired subsequence.

Note that $|a_n(f)|_p \leq \|\Delta^n f\| \leq \|\Delta\|^n \|f\|$, so $\|(a_n(f))_n\| = \max_{n=0,1,\dots} |a_n(f)|_p \leq \|f\|$, so the map is norm-decreasing. Linearity follows from the linearity of Δ .

Injectivity: assume $a_n(f) = 0 \forall n \geq 0$. Then $a_0(f) = f(0) = 0$, and by induction $f(n) = \Delta^n f(0) = a_n(f) = 0 \forall n \geq 0$. So $f = 0$ by continuity since $\mathbb{Z}_{\geq 0} \subseteq \mathbb{Z}_p$ is dense. \square

We will prove that the linear maps

$$\begin{aligned} f &\mapsto (a_n(f)) \\ \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) &\rightleftarrows c_0 \\ f_a(x) &= \sum_{n=0}^{\infty} a_n \binom{x}{n} \leftrightarrow (a_n) = a \end{aligned}$$

are mutual inverses and norm-preserving.

Lemma 65. *We have $\binom{x}{n} + \binom{x}{n-1} = \binom{x+1}{n} \forall n \in \mathbb{Z}_{\geq 1}$ and $x \in \mathbb{Z}_p$.*

Proof 1. True when $x \in \mathbb{Z}_{\geq n}$, and then the lemma follows by the density of $\mathbb{Z}_{\geq n} \subset \mathbb{Z}_p$ and continuity. \square

Proof 2. True when $x \in \mathbb{Z}_{\geq n}$, and both sides are polynomials which agree on an infinite set of points \implies equal as elements of $\mathbb{Q}[x]$. Now evaluate. \square

Now let $a = (a_n)_{n=0}^{\infty} \in c_0$. Define $f_a : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$,

$$f_a(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$$

This is a uniformly convergent series, so $f_a \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$.

Proposition 66. *$a \mapsto f_a$ defines a norm-decreasing linear map $c_0 \rightarrow \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$.*

Moreover, $a_n(f_a) = a_n \forall n \geq 0$.

Proof. Linearity is clear.

Norm decreasing:

$$\begin{aligned} |f_a(x)|_p &= \left| \sum_{n=0}^{\infty} a_n \binom{x}{n} \right| \\ &\leq \sup_n |a_n|_p \left| \binom{x}{n} \right|_p \\ &\leq \sup_n |a_n|_p = \|a\| \quad \forall x \in \mathbb{Z}_p \end{aligned}$$

$$\implies \|f_a\| \leq \|a\|.$$

Inverses: $\forall k \in \mathbb{Z}_{\geq 0}$ define $a^{(k)} = (a_k, a_{k+1}, a_{k+2}, \dots)$

$$\begin{aligned} \triangle f_a(x) &= f_a(x+1) - f_a(x) \\ &= \sum_{n=1}^{\infty} a_n \left(\binom{x+1}{n} - \binom{x}{n} \right) \\ &= \sum_{n=1}^{\infty} a_n \binom{x}{n-1} \text{ by Lemma 65} \\ &= \sum_{n=0}^{\infty} a_{n+1} \binom{x}{n} = f_{a^{(1)}}(x) \end{aligned}$$

Iterating, $\Delta^k f_a = f_{a^{(k)}} \implies$

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

□

Summing up:

$$\begin{aligned} F(f) &= (a_n(f)) \\ V = \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) &\xrightleftharpoons[G]{F} c_0 = W \\ G(a) &= f_a \end{aligned}$$

We know: F is injective and norm-decreasing, $FG = id_W$ and G is norm-decreasing.

Lemma 67. *In this situation, $GF = id_V$ and F and G are norm-preserving.*

Proof. Let $v \in V$. Then $F(v - GFv) = Fv - Fv = 0 \implies v = GFv$ since F is injective. So $GF = id_V$.

Norm-preserving: $v \in V$, have $\|Fv\| \leq \|v\|$, but also $\|Fv\| \geq \|GFv\| = \|v\|$, so F is norm preserving. Same proof for G . □

This finishes the proof of Mahler's Theorem.

3 Ramification Theory for Local Fields

The characteristic of the residue field of any local field from now on will be p (unless stated otherwise).

3.1 More on Finite Extensions

Recall: let R be a PID and let M be a f.g. R -module. Assume that M is torsion free. Then $\exists! n \geq 0$ such that $M \cong R^n$. Moreover, if $N \subseteq M$ is a submodule, then N is finitely generated and $N \cong R^m$, with $m \leq n$.

Proposition 68. *Let K be a local field, L/K finite of degree n . Then \mathcal{O}_L is a finite, free \mathcal{O}_K -module of rank n (i.e. $\mathcal{O}_L \cong \mathcal{O}_K^n$ as \mathcal{O}_K -modules), and k_L/k_K is an extension of degree $\leq n$. Moreover, L is a local field.*

Proof. Choose a K -basis $\alpha_1, \dots, \alpha_n$ of L . Let $\|\cdot\|$ denote the maximum norm $\|\sum_{i=1}^n x_i \alpha_i\| = \max_{i=1, \dots, n} |x_i|$ on L as in Proposition 33. $\|\cdot\|$ is equivalent to $|\cdot|$ (the extended absolute value on L) as K -norms, so $\exists r > s > 0$ such that

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

Increasing r and decreasing s as necessary wlog $r = |a|$, $s = |b|$ for some $a, b \in K^\times$. Then

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

$\implies \mathcal{O}_L$ is f.g. and free of rank n over \mathcal{O}_K .

Since $\mathfrak{m}_K = \mathfrak{m}_L \cap \mathcal{O}_K$, we have a natural injection

$$k_K = \mathcal{O}_K / \mathfrak{m}_K \hookrightarrow \mathcal{O}_L / \mathfrak{m}_L = k_L$$

Since \mathcal{O}_L is generated over \mathcal{O}_K by n elements, k_L is generated by n elements over k_K , i.e. $[k_L : k_K] \leq n$.

L a local field: k_L/k_K is finite and k_K finite $\implies k_L$ is a finite field. L is complete by Theorem 29.

Let v_K be the normalised valuation on K , w the extension of v_K to L . Then $w(\alpha) = \frac{1}{n}v_K(N_{L/K}(\alpha))$, so

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

\implies it's discrete. □

Definition 69. Let L/K be a finite extension of local fields. The **inertia degree** of L/K is

$$f_{L/K} = [k_L : k_K]$$

Let v_L be the normalised valuation on L and π_K a uniformiser of K . The integer

$$e_{L/K} = v_L(\pi_K)$$

is called the **ramification index** of L/K .

Theorem 70. Let L/K be a finite extension of local fields. Then $[L : K] = e_{L/K}f_{L/K}$ and $\exists \alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Proof. Write $e = e_{L/K}$, $f = f_{L/K}$.

k_L/k_K is separable, so $\exists \bar{\alpha} \in k_L$ such that $k_L = k_K(\bar{\alpha})$. Let $\bar{f}(x) \in k_K[x]$ be the minimal polynomial of $\bar{\alpha}$ over k_K , and let $f \in \mathcal{O}_K[x]$ be a monic lift of \bar{f} with $\deg f = \deg \bar{f}$.

Claim: $\exists \alpha \in \mathcal{O}_L$ lifting $\bar{\alpha}$ and such that $v_L(f(\alpha)) = 1$ (always ≥ 1).

Let $\beta \in \mathcal{O}_L$ be any lift of $\bar{\alpha}$. If $v(f(\beta)) = 1$, then set $\alpha = \beta$. If not, set $\alpha = \beta + \pi_L$ (π_L uniformiser of L).

$f(\alpha) = f(\beta + \pi_L) = f(\beta) + f'(\beta)\pi_L + b\pi_L^2$ for some $b \in \mathcal{O}_L$ (Taylor expanding around β).

Since $v_L(f(\beta)) \geq 2$ and $v_L(f'(\beta)) = 0$, we have $v_L(f(\alpha)) = 1$. Put $\pi = f(\alpha)$ (uniformiser of L).

We claim that $\alpha^i \pi^j$, $i = 0, \dots, f-1$, $j = 0, \dots, e-1$ are an \mathcal{O}_K -basis of \mathcal{O}_L .

Linear independence: assume $\sum_{i,j} a_{ij} \alpha^i \pi^j = 0$ for some $a_{ij} \in K$, not all 0. Put $s_j = \sum_{i=0}^{f-1} a_{ij} \alpha^i \forall j$. $1, \alpha, \dots, \alpha^{f-1}$ are linearly independent over K since there reductions are linearly independent over k_K . So $\exists j$ such that $s_j \neq 0$.

Claim: $e | v_L(s_j)$ if $s_j \neq 0$.

Let k be such that $|a_{kj}|$ is maximal, then $a_{kj}^{-1} s_j = \sum_{i=0}^{f-1} a_{kj}^{-1} a_{ij} \alpha^i \implies a_{kj}^{-1} s_k \not\equiv 0 \pmod{\pi_L}$ because $1, \bar{\alpha}, \dots, \bar{\alpha}^{f-1}$ are linearly independent over k_K .

$$\begin{aligned} \implies v_L(a_{kj}^{-1} s_j) = 0 &\implies v_L(s_j) = v_L(a_{kj}) = v_L(a_{kj}^{-1} s_j) \\ &\in v_L(K^\times) \\ &= ev_L(L^\times) = e\mathbb{Z} \end{aligned}$$

Now write $\sum_{i,j} a_{ij} \alpha^i \pi^j = \sum_{j=0}^{e-1} s_j \pi^j = 0$. If $s_j \neq 0$, we have $v_L(s_j \pi^j) = v_L(s_j) + j \in j + e\mathbb{Z}$.

\implies no two non-zero terms in $\sum_{j=0}^{e-1} s_j \pi^j$ have the same valuation.

$\implies \sum_{j=0}^{e-1} s_j \pi^j \neq 0$, which is a contradiction.

Claim $\mathcal{O}_L = \oplus_{i,j} \alpha^i \pi^j$.

Set $M = \oplus_{i,j} \alpha^i \pi^j$ and $N = \oplus_{i=0}^{f-1} \mathcal{O}_K \alpha^i$. Then $M = N + \pi N + \pi^2 N + \dots + \pi^{e-1} N$. Since $1, \bar{\alpha}, \dots, \bar{\alpha}^{f-1}$ span k_L over k_K we must have $\mathcal{O}_L = N + \pi \mathcal{O}_L$.

$$\begin{aligned} \text{Iterate: } \mathcal{O}_L &= N + \pi(N + \pi \mathcal{O}_L) \\ &= N + \pi N + \pi^2 \mathcal{O}_L \\ &= \dots \\ &= N + \pi N + \dots + \pi^{e-1} N + \pi^e \mathcal{O}_L \\ &= M + \pi_K \mathcal{O}_L \quad (\pi_K \text{ uniformiser of } K) \end{aligned}$$

Iterate: $\mathcal{O}_L = M + \pi_K^n \mathcal{O}_L \forall n \geq 1 \implies M$ is dense in \mathcal{O}_L . But M is the closed unit ball in $V = \oplus_{i,j} K \alpha^i \pi^j \subseteq L$ w.r.t the maximum norm on V w.r.t the basis $\alpha^i \pi^j$.

Proposition 33 and Theorem 29 $\implies M$ is complete both w.r.t the maximum norm and $|\cdot|$ on L .

$\implies M \subseteq L$ is closed.

$\implies M = \mathcal{O}_L$.

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

Corollary 71. *Let $M/L/K$ be finite extensions of local fields. Then $f_{M/K} = f_{L/K} f_{M/L}$ and $e_{M/K} = e_{L/K} e_{M/L}$.*

Proof. $[k_M : k_K] = [k_M : k_L][k_L : k_K]$ by multiplicativity of degrees.

$$e_{M/L}e_{L/K} = \frac{[M:L]}{f_{M/L}} \frac{[L:K]}{f_{L/K}} = \frac{[M:K]}{f_{M/K}} = e_{M/K}. \quad \square$$

Definition 72. Let L/K be a finite extension of local fields. L/K is **unramified** if $e_{L/K} = 1$ (or $f_{L/K} = [L : K]$), and **totally ramified** if $f_{L/K} = 1$.

Theorem 73. Let K be a local field. For each finite extension l/k_K there is a **unique** (up to isomorphism) finite unramified extension L/K with $k_L \cong l$ over k_K .

Moreover, L/K is Galois with $\text{Gal}(L/K) \cong \text{Gal}(l/k_K)$.

Proof. Existence: let $\bar{\alpha}$ be a primitive element of l/k_K with minimal polynomial $\bar{f} \in k_K[x]$. Take a monic lift $f \in \mathcal{O}_K[x]$ of \bar{f} ($\deg f = \deg \bar{f}$).

Put $L = K(\alpha)$ where α is a root of f . \bar{f} irreducible $\implies f$ irreducible $\implies [L : K] = [l : k_K]$.

Moreover, k_L contains a root of \bar{f} (the reduction of α). So $l \hookrightarrow k_L$ over $k_K \implies [L : K] \geq [k_L : k_K] = [l : k_K]$.

$\implies L/K$ is unramified and $k_L \cong l$ over k_K . \square

Uniqueness and Galois property follows from:

Lemma 74. 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

$$\text{Hom}_{K\text{-alg}}(L, M) \xrightarrow{\sim} \text{Hom}_{k_K\text{-alg}}(k_L, k_M)$$

($\varphi : L \rightarrow M$ restricts to $\varphi : \mathcal{O}_L \rightarrow \mathcal{O}_M$, then take reductions).

Proof. By uniqueness of extended absolute values (Theorem 29) any K -algebra homomorphism $\phi : L \rightarrow M$ is an isometry for the extended absolute values.

Thus $\varphi(\mathcal{O}_L) \subseteq \mathcal{O}_M$, $\varphi(\mathfrak{m}_L) \subseteq \varphi(\mathfrak{m}_M)$ so we get the induced k_K -algebra homomorphism $\bar{\varphi} : k_L \rightarrow k_M$. This gives

$$\text{Hom}_{K\text{-alg}}(L, M) \rightarrow \text{Hom}_{k_K\text{-alg}}(k_L, k_M)$$

Bijectivity: let $\bar{\alpha} \in k_L$ be a primitive element over k_K , $\bar{f} \in k_K[x]$ its minimal polynomial, $f \in \mathcal{O}_K[x]$ a monic lift of \bar{f} and $\alpha \in \mathcal{O}_L$ the unique root of f which lifts to $\bar{\alpha}$ (Hensel's Lemma).

Then $k_L = k_L(\bar{\alpha})$ and $L = K(\alpha)$.

$$\begin{array}{ccccc} \varphi & & \text{Hom}_{K\text{-alg}}(L, M) & \longrightarrow & \text{Hom}_{k_K}(k_L, k_M) & & \hat{\varphi} \\ \downarrow & & \wr \downarrow & & \wr \downarrow & & \downarrow \\ \varphi(\alpha) & & \{x \in M \mid f(x) = 0\} & \longrightarrow & \{\bar{x} \in k_M \mid \bar{f}(\bar{x}) = 0\} & & \bar{\varphi}(\bar{\alpha}) \end{array}$$

This is a bijection by Hensel's Lemma, since \bar{f} is seperable. \square

Proof of 73 cont. Uniqueness: $k_L \cong k_M$ over k_K , L/K , M/K unramified. Then $\bar{\phi}$ lifts to a K -embedding $\phi : L \hookrightarrow M$ and $[L : K] = [M : K] \implies \phi$ an isomorphism.

Galois: $|\text{Aut}_K(L)| = |\text{Aut}_{k_K}(k_L)| = [k_L : k_K] = [L : K] \implies L/K$ Galois.

Also, $\text{Aut}_K(L) \rightarrow \text{Aut}_{k_K}(k_L)$ is really a homomorphism (so an isomorphism). \square

Proposition 75. *Let K be a local field, L/K finite unramified, M/K finite. Say $L, M \subset$ fixed algebraic closure \bar{K} of K . Then LM/M is unramified. Any subextension of L/K is unramified over K . If M/K is unramified, then LM/K is unramified.*

Proof. Let $\hat{\alpha}$ be a primitive element of k_L/k_K , $\bar{f} \in k_K[x]$ the minimal polynomial of $\hat{\alpha}$, $f \in \mathcal{O}_K[x]$ a monic lift of \bar{f} , $\alpha \in \mathcal{O}_L$ the unique root of f lifting $\hat{\alpha}$. Then $L = K(\alpha)$ so $LM = M(\alpha)$.

Let \bar{g} be the minimal polynomial of $\bar{\alpha}$ over k_M . Then $\bar{g}|\bar{f} \implies f = gh$ in $\mathcal{O}_M[x]$ by Hensel's Lemma. g monic, lifts $\bar{g} \implies g(\alpha) = 0$ and g irreducible in $M[x]$.

So g is the minimal polynomial of α over $M \implies$

$$[LM : M] = \deg g = \deg \bar{g} \leq [k_{LM} : k_M] \leq [LM : M]$$

\implies have equalities, LM/M unramified.

The second claim follows from the multiplicativity of $f_{L/K}$ and $e_{L/K}$ (Corollary 71), as does the third ($[LM : K] = [LM : M][M : K] = f_{LM/M}f_{M/K} = f_{LM/K} \implies LM/K$ unramified). \square

Corollary 76. *Let K be a local field, L/K finite. Then \exists a unique maximal subfield $K \subseteq T \subseteq L$ such that T/K is unramified. Moreover, $[T : K] = f_{L/K}$.*

Proof. Existence: T is the composite of all unramified subextensions of L/K (use Proposition 75).

Have $[T : K] = f_{T/K} \leq f_{L/K}$ by Corollary 71.

Let T'/K be the unique unramified extension with residue field extension k_L/k_K . Then $\text{id} : k_{T'} = k_L \rightarrow k_L$ lifts to a K -embedding $T' \xrightarrow{\varphi} L$, by Lemma 74.

Then $[T : K] \geq [\varphi(T') : K] = f_{L/K} \implies [T : K] = f_{L/K}$. \square

3.2 Totally Ramified Extensions

Recall

Theorem 77 (Eisenstein's Criterion). *Let K be a local field, $f(x) = x^n + \dots + a_0 \in \mathcal{O}_K[x]$, π_K uniformiser of K . If $\pi_K | a_{n-1}, \dots, a_0$ and $\pi_K^2 \nmid a_0$, then f is irreducible.*

Note that if L/K finite, v_K a normalised valuation on K and w the unique extension of v_K to L . Then $e_{L/K}^{-1} = w(\pi_L) = \min_{x \in \mathfrak{m}_L} w(x)$.

A polynomial $f(x) \in \mathcal{O}_K[x]$ satisfying the assumptions of Eisenstein's criterion is called an **Eisenstein polynomial**.

Proposition 78. *Let L/K be a totally ramified extension of local fields. Then $L = K(\pi_L)$ and the minimal polynomial of π_L over K is Eisenstein.*

Conversely, if $L = K(\alpha)$ and the minimal polynomial of α over K is Eisenstein, then L/K is totally ramified and α is a uniformiser of L .

Proof. First part: $n = [L : K]$, v_K a normalised valuation on K and w the unique extension of v_K to L . Then

$$[K(\pi_L) : K]^{-1} \leq e_{K(\pi_L)/K}^{-1} = \min_{x \in \mathfrak{m}_K(\pi_L)} w(x) \leq \frac{1}{n}$$

$$\implies [K(\pi_L) : K] \geq [L : K] \implies L = K(\pi_L).$$

Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathcal{O}_K[x]$ be the minimal polynomial of π_L over K .

$$\pi_L^n = -(a_0 + a_1(\pi_L) + \dots + a_{n-1}\pi_L^{n-1})$$

So $1 = w(\pi_L^n) = w(a_0 + a_1\pi_L + \dots + a_{n-1}\pi_L^{n-1}) = \min_{i=0,1,\dots,n-1} (v_K(a_i) + \frac{i}{n})$
 $\implies v_K(a_i) \geq 1 \ \forall i$ and $v_K(a_0) = 1$, so f is Eisenstein.

Converse: $L = K(\alpha)$, $n = [L : K]$. Let $g(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0 \in \mathcal{O}_K[x]$ be the minimal polynomial of α . g irreducible \implies all roots have the same valuation, so

$$1 = w(b_0) = n \cdot w(\alpha) \implies w(\alpha) = \frac{1}{n}$$

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

$$\implies [L : K] = e_{L/K} = n, \text{ so } L/K \text{ is totally ramified and } \alpha \text{ is a uniformiser.}$$

□

We've show that if L/K is a totally ramified extension of local fields, then $L = K(\pi_L)$. In fact, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ (see proof of Theorem 70).

3.3 The Unit Group \mathcal{O}_K^\times

Let K be a local field. For each $s \in \mathbb{Z}_{\geq 1}$, set

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

where π_K is a uniformiser of K . Put $U_K = U_K^{(0)} = U^{(0)} = \mathcal{O}_K^\times$.

Proposition 79. *We have $U_K/U_K^{(1)} \cong (k_K^\times, \cdot)$ and $U_K^{(s)}/U_K^{(s+1)} \cong (k_K, +)$.*

Proof. We have a surjective homomorphism $\mathcal{O}_K^\times \rightarrow k_K^\times$ which is just reduction mod π_K , and the kernel is $1 + \pi_K \mathcal{O}_K = U_K^{(1)}$.

For the second part, define a surjection

$$\begin{aligned} U_K^{(s)} &\rightarrow k_K \\ 1 + \pi_K^s x &\mapsto x \pmod{\pi_K} \end{aligned}$$

This is a group homomorphism: writing $\pi = \pi_K$,

$$(1 + \pi^s x)(1 + \pi^s y) = 1 + \pi^s(x + y + \pi^s xy) \mapsto x + y + \pi^s xy \equiv x + y \pmod{\pi}$$

The kernel is $1 + \pi^{s+1} \mathcal{O}_K = U_K^{s+1}$. \square

3.4 The Inertia Group

Proposition 80. *If L/K is a finite Galois extension of local fields, then \exists a surjective homomorphism $\text{Gal}(L/K) \rightarrow \text{Gal}(k_L/k_K)$.*

Proof. Lemma 74 gives us a homomorphism

$$\begin{array}{ccc} \text{Aut}_K(L) & \longrightarrow & \text{Aut}_{k_K}(k_L) \\ \parallel & & \parallel \\ \text{Gal}(L/K) & & \text{Gal}(k_L/k_K) \end{array}$$

Let T/K be the maximal unramified subextension of L/K .

$$\begin{array}{ccc} \text{Gal}(L/K) & \longrightarrow & \text{Gal}(k_L/k_K) \\ \downarrow & & \parallel_{(k_T=k_L)} \\ \text{Gal}(T/K) & \xrightarrow{\sim} & \text{Gal}(k_T/k_K) \end{array}$$

\implies surjectivity. \square

Definition 81. In the setting of proposition 80, the kernel $I(L/K) = \text{Gal}(L/T)$ of $\text{Gal}(L/K) \rightarrow \text{Gal}(k_L/k_K)$ is called the **inertia group** of L/K (Trivial $\iff L/K$ unramified).

The field T is (sometimes) called the **inertial field** of L/K .

Lemma 82. *Let L/K be a finite Galois extension of local fields. Let $x \in k_L$ and $\sigma \in \text{Gal}(L/K)$ with image $\bar{\sigma} \in \text{Gal}(k_L/k_K)$. Then*

$$[\bar{\sigma}(x)] = \sigma([x])$$

In particular, $\sigma([x]) = [x] \ \forall x \in k_L \iff \sigma \in I(L/K)$.

Proof. The map

$$\begin{aligned} x &\mapsto \sigma^{-1}([\bar{\sigma}(x)]) \\ k_L &\rightarrow \mathcal{O}_L \end{aligned}$$

is multiplicative and $\sigma^{-1}([\bar{\sigma}(x)]) \equiv x \pmod{\pi_L}$
 $\implies \sigma^{-1}([\bar{\sigma}(x)]) = [x]$ by uniqueness of $[-]$. □

3.5 Higher Ramification Groups

Let L/K be a finite Galois extension of local fields, v_L a normalised valuation on L .

Definition 83. Let $s \in \mathbb{R}_{\geq -1}$. Define the **s-th ramification group** of L/K by

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

We could have defined these only for $s \in \mathbb{Z}_{\geq -1}$. Note that $G_{-1}(L/K) = \text{Gal}(L/K)$, $G_0(L/K) = I(L/K)$.

Proposition 84. *Notation as above, π_L a uniformiser of L . Then $G_{s+1}(L/K)$ is a normal subgroup of $G_s(L/K) \ \forall s \in \mathbb{Z}_{s \geq 0}$ and the map*

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

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

Proof. Define $\phi : G_s(L/K) \rightarrow \frac{U_L^{(s)}}{U_L^{(s+1)}}$ by $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$. $\sigma \in G_s(L/K)$, $\sigma(\pi_L) = \pi_L + \pi_L^{s+1}x$ for some $x \in \mathcal{O}_L \implies$

$$\frac{\sigma(\pi_L)}{\pi_L} = 1 + \pi_L^s x \in U_L^s$$

Now let $u \in \mathcal{O}_L^\times$. Then $\sigma(u) = u + \pi_L^{s+1}y$ for some $y \in \mathcal{O}_L$, so

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

So ϕ is independent of the choice of π_L .

It's a homomorphism:

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

We have

$$\begin{aligned} \text{Ker } \phi &= \{\sigma \in G_s(L/K) \mid v_L(\sigma(\pi_L) - \pi_L) \geq s+2\} \\ &\subseteq \{\sigma \in G_s(L/K) \mid v_L(\sigma(z) - z) \geq s+2 \ \forall z \in \mathcal{O}_L\} \\ &= G_{s+1}(L/K) \end{aligned}$$

Conversely, let $x \in \mathcal{O}_L$ and write $x = \sum_{n=0}^\infty [x_n]\pi_L^n$, $x_n \in k_L$. Write $\sigma(\pi_L) = \pi_L + \pi_L^{s+2}y$, $y \in \mathcal{O}_L$. Let $\sigma \in \text{Ker } \phi \subseteq I(L/K)$.

By Lemma 82,

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

so $v_L(\sigma(x) - x) \geq s+2$, so $\sigma \in G_{s+1}(L/K)$. \square

Corollary 85. $\text{Gal}(L/K)$ is soluble.

Proof. Note that $\bigcap_s G_s(L/K) = \{id\}$, so $(G_s(L/K))_{s \in \mathbb{Z}_{\geq -1}}$ is a subnormal series of $\text{Gal}(L/K)$ and $\frac{G_s(L/K)}{G_{s+1}(L/K)}$ is abelian. \square

Let L/K be a finite Galois extension of local fields. Then $G_1(L/K)$ is a p -group (since $\frac{G_s(L/K)}{G_{s+1}(L/K)} \hookrightarrow k_L \ \forall s \in \mathbb{Z}_{\geq 1}$) and $\frac{G_0(L/K)}{G_1(L/K)} \hookrightarrow k_L^\times$, which has order prime to p .

$\implies G_1(L/K)$ is the unique Sylow p -subgroup of $G_0(L/K)$.

$G_1(L/K)$ is called the **wild inertia group** and $\frac{G_0(L/K)}{G_1(L/K)}$ is called the **tame quotient**.

Proposition 86. *Let $M/L/K$ be finite extensions of local fields, M/K Galois. Then $G_s(M/K) \cap \text{Gal}(M/L) = G_s(M/L)$.*

Proof.

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

□

3.6 Quotients

Let L/K be a finite Galois extension of local fields. Pick $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. set $i_{L/K}(\sigma) = v_L(\sigma(\alpha) - \alpha)$ for $\sigma \in \text{Gal}(L/K)$.

If $g(x) = \sum_{i=0}^m b_i x^i \in \mathcal{O}_K[x]$, then

$$v_L(\sigma(g(\alpha)) - g(\alpha)) = v_L\left(\sum_{i=1}^m b_i(\sigma(\alpha)^i - \alpha^i)\right) \geq v_L(\sigma(\alpha) - \alpha)$$

$\implies i_{L/K}(\sigma)$ is independent of α , and

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

Proposition 87. *Let $M/L/K$ be finite extension of local fields, M/K and L/K Galois. Then*

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

Proof. If $\sigma = 1$, both sides = ∞ . Assume $\sigma \neq 1$. Let $\mathcal{O}_M = \mathcal{O}_K[\alpha]$, $\mathcal{O}_L = \mathcal{O}_K[\beta]$, $\alpha \in \mathcal{O}_M$, $\beta \in \mathcal{O}_L$.

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

$$\tau \in \text{Gal}(M/K) \implies i_{M/K}(\tau) = v_M(\tau(\alpha) - \alpha).$$

Fix τ such that $\tau|_L = \sigma$. Set $H = \text{Gal}(M/L)$. Then

$$(\text{RHS of } *) \cdot e_{M/L} = \sum_{g \in H} (\tau(g(\alpha)) - \alpha) = v_M\left(\prod_{g \in H} (\tau(g(\alpha)) - \alpha)\right)$$

Set $b = \sigma(\beta) - \beta = \tau(\beta) - \beta$ and $a = \prod_{g \in H} (\tau(g(\alpha)) - \alpha)$. We want to prove $v_M(b) = v_M(a)$.

General observation: let $z \in \mathcal{O}_L$, write $z = \sum_{i=0}^h z_i \beta^i$, $z_i \in \mathcal{O}_K$. Then $\tau(z) - z = \sum_{i=1}^h z_i (\tau(\beta)^i - \beta^i)$ 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, $F(x) = \prod_{g \in H} (x - g(\alpha))$.

We have $(\tau F)(x) = \prod_{g \in H} (x - \tau(g(\alpha)))$ [τF is the polynomial obtained from F by applying τ to all coefficients], then all coefficients of $\tau F - F$ are of the form $\tau(z) - z$ for some $z \in \mathcal{O}_L \implies$ they are divisible by b .

$$\implies b | (\tau F - F)(a) = \pm a \implies b | a$$

Conversely, pick $f \in \mathcal{O}_K[x]$ such that $f(\alpha) = \beta$. Since $f(\alpha) - \beta = 0$, $f(x) - \beta = F(x)h(x)$ for some $h(x) \in \mathcal{O}_L[x]$.

Then $(f - \tau(\beta))(x) = (\tau F - \tau(\beta))(x) = (\tau F)(x)(\tau(h))(x)$. Set $x = \alpha$: $-b = \beta - \tau(\beta) = (\pm a)\tau h(\alpha) \implies a | b$. \square

Let L/K be a finite Galois extension of local fields. Define $\eta_{L/K} : [-1, \infty) \rightarrow [-1, \infty)$ by

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

When $-1 \leq x < 0$, our convention is that $\frac{1}{|G_0(L/K) : G_x(L/K)|} = |G_x(L/K) : G_0(L/K)|$ which is just $= 1$ when $-1 < x < 0$.

$$\implies \eta_{L/K}(s) = s \text{ if } -1 \leq s \leq 0.$$

Proposition 88. *Let $G = \text{Gal}(L/K)$. Then $\eta_{L/K}(s) = \left(e_{L/K}^{-1} \sum_{\sigma \in G} \min(i_{L/K}(\sigma), s+1) \right) - 1$, for $s \in [-1, \infty)$.*

Proof. Let $\text{RHS} = \theta(s)$. Look at $s \mapsto \min(i_{L/K}, s+1)$.

$\implies \theta(s)$ is piecewise linear and break points are integers (same for $\eta_{L/K}$).

Have

$$\theta(0) = \frac{\#\{\sigma \in G \mid i_{L/K}(\sigma) \geq 1\}}{e_{L/K}} - 1 = 0 = \eta_{L/K}(0)$$

If $s \in [-1, \infty) \setminus \mathbb{Z}$,

$$\theta'(s) = e_{L/K}^{-1} \#\{\sigma \in G \mid i_{L/K}(\sigma) \geq s+1\} = \frac{1}{|G_0 L/K : G_s L/L|} = \eta'_{L/K}(s)$$

$$\implies \theta(s) = \eta_{L/K}(s). \quad \square$$

Theorem 89 (Herbrand). *Let $M/L/K$ be finite extensions of local fields, M/K and L/K Galois. Set $H = \text{Gal}(M/L)$ and $t = \eta_{L/K}(s)$, $s \in [-1, \infty)$.*

Then $\frac{G_s(M/K)H}{H} = G_t(L/K)$.

Proof. Put $G = \text{Gal}(M/K)$. Choose $\tau \in G$ such that $i_{M/K}(\tau) \geq i_{M/K}(\tau g)$ for all $g \in H$. Put $m = i_{M/K}(\tau)$, $\sigma = \tau|_L$.

Claim: $i_{L/K}(\sigma) - 1 = \eta_{M/L}(m - 1)$.

If $g \in G_{m-1}(M/L) \leq H$, then $i_{M/K}(g) \geq m$, so

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

If $g \in H \setminus G_{m-1}(M/L)$, then $i_{M/K}(g) < m$ and $i_{M/K}(\tau g) = i_{M/K}(g)$. In either case, $i_{M/K}(\tau g) = \min(m, i_{M/K}(g))$. By Proposition 87, $i_{L/K}(\sigma) = e_{M/L}^{-1} \sum_{g \in H} \min(m, i_{M/K}(g))$.

By Proposition 88,

$$\eta_{M/L}(m-1) = \left(e_{M/L}^{-1} \sum_{g \in H} \min(i_{M/K}, m) \right) - 1 = i_{L/K}(\sigma) - 1$$

This proves the claim.

Now

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

□

Let L/K be a Galois extension of local fields. $\eta_{L/K} : [-1, \infty) \rightarrow [-1, \infty)$ is continuous, strictly increasing, $\eta_{L/K}(-1) = -1$ and $\eta_{L/K}(s) \rightarrow \infty$ as $s \rightarrow \infty$, so it is invertible. Set $\chi_{L/K} = \eta_{L/K}^{-1}$.

Definition 90. L/K as before. The **upper numbering** of the ramification groups of L/K is defined by

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

for $t \in [-1, \infty)$. The previous numbering is called the **lower numbering**.

Lemma 91. Let $M/L/K$ be finite extension of local fields, M/K and L/K Galois. Then $\eta_{M/K} = \eta_{L/K} \circ \eta_{M/L}$, hence $\chi_{M/K} = \chi_{M/L} \circ \chi_{L/K}$.

Proof. Let $s \in [-1, \infty)$, set $t = \eta_{M/L}(s)$ and $H = \text{Gal}(M/L)$.

By Theorem 89,

$$\begin{aligned} G_t(L/K) &\cong \frac{G_s(M/K)H}{H} \\ &\cong \frac{G_s(M/K)}{H \cap G_s(M/K)} \\ &= \frac{G_s(M/K)}{G_s(M/L)} \end{aligned}$$

Thus

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

so

$$\begin{aligned} \eta'_{M/K}(s) &= \frac{\#G_s(M/K)}{e_{M/K}} \\ &= \frac{\#G_t(L/K)}{e_{L/K}} \cdot \frac{\#G_s(M/L)}{e_{M/L}} \\ &= \eta'_{L/K}(t) \eta'_{M/L}(s) = (\eta_{L/K} \circ \eta_{M/L})'(s) \end{aligned}$$

whenever these derivatives make sense.

Since $\eta_{L/K}(\eta_{M/L}(0)) = \eta_{L/K}(0) = 0 = \eta_{M/K}(0)$, we get $\eta_{M/K} = \eta_{L/K} \circ \eta_{M/L}$. \square

Corollary 92. *Keep the notation of Lemma 91 and its proof. Let $t \in [-1, \infty)$.*

Then

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

Proof. Put $s = \chi_{L/K}(t)$. Then, by Theorem 89 and Lemma 91,

$$\begin{aligned} \frac{G^t(M/K)H}{H} &\stackrel{\text{def}}{=} \frac{G_{\chi_{M/K}(t)}(M/K)H}{H} \\ &\stackrel{89}{=} G_{\eta_{M/L}(\chi_{M/K}(t))}(L/K) \\ &\stackrel{91}{=} G_s(L/K) \stackrel{\text{def}}{=} G^t(L/K) \end{aligned}$$

\square

4 Local Class Field Theory

This is the study of abelian extensions (i.e. extensions with abelian Galois groups) of local fields.

4.1 Infinite Galois Theory

Definition 93. Let L/K be an algebraic field extension. We say that L/K is **seperable** if, for every $\alpha \in L$, the minimal polynomial $f_\alpha \in K[x]$ is seperable.

We say L/K is **normal** if f_α splits into linear factors in $L[x]$ for every $\alpha \in L$.

L/K is **Galois** if it is normal and seperable. If so, we write $\text{Gal}(L/K) = \text{Aut}_K(L)$.

Definition 94. Let M/K be a Galois extension. $U \subseteq \text{Gal}(M/K)$ is open if for every $\sigma \in U$, $\exists L/K$ a finite subextension of M/K such that $\sigma \text{Gal}(M/K) \subseteq U$.

These sets form the open sets of a topology on $\text{Gal}(M/K)$ called the **Krull topology**. $G = \text{Gal}(M/K)$ is a topological group w.r.t. the Krull topology.

Proposition 95. *Let M/K be a Galois extension. Then $\text{Gal}(M/K)$ is compact and Hausdorff, and if $U \subseteq \text{Gal}(M/K)$ is an open subset such that $1 \in U$, then there exists an open normal subgroup $N \subseteq \text{Gal}(M/K)$ such that $N \subseteq U$.*

Remarks. 1. When M/K is finite, the Krull topology is discrete.

2. Topological groups with the properties in Proposition 95 are called **profinite**.

3. Last part: by definition, $\exists L/K$ a finite subextension of M/K such that $\text{Gal}(M/L) \subseteq U$. Let L' be the Galois closure of L over K , then $\text{Gal}(M/L') \subseteq \text{Gal}(M/L) \subseteq U$, and $\text{Gal}(M/L')$ is open and normal.

Definition 96. Let I be a set with a partial order \leq . We say that I is a **directed system** if $\forall i, j \in I \exists k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 97. Let I be a directed system. An **inverse system** (of topological groups) indexed by I is a collection of topological groups G_i , $i \in I$ and continuous homomorphisms $f_{ij} : G_j \rightarrow G_i \forall i, j \in I$ with $i \leq j$ such that

1. $f_{ii} = \text{id}_{G_i}$
2. $f_{ik} = f_{ij} \circ f_{jk}$ when $i \leq j \leq k$

We define the **inverse limit** of the system (G_i, f_{ij}) to be

$$\varprojlim_{i \in I} G_i = \left\{ (g_i) \in \prod_{i \in I} G_i \mid f_{ij}(g_j) = g_i \forall i \leq j \right\} \subseteq \prod_{i \in I} G_i$$

It's a group under coordinate-wise multiplication and a topological space when given the subspace topology of the product topology on $\prod_{i \in I} G_i$. This makes $\varprojlim_{i \in I} G_i$ into a topological group.

Proposition 98. *Let M/K be a Galois extension. The set I of finite Galois subextensions L/K of M/K is a directed system under inclusion. If $L, L' \in I$ with $L \subseteq L'$, then we have a map $\cdot|_L^{L'} : \text{Gal}(L'/K) \rightarrow \text{Gal}(L/K)$. Then $(\text{Gal}(L/K), \cdot|_L^{L'})_{L \in I, L \subseteq L'}$ is an inverse system, and the map*

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

is an isomorphism of topological groups.

Theorem 99 (Fundamental Theorem of Galois Theory). *Let M/K be Galois. The map $L \mapsto \text{Gal}(M/L)$ defines a bijection between subextensions L/K of M/K and closed subgroups of $\text{Gal}(M/K)$, with inverse $H \mapsto M^H$.*

Moreover, L/K is finite $\iff \text{Gal}(M/L)$ is open, and L/K Galois $\iff \text{Gal}(M/L)$ is normal, and then

$$\sigma \mapsto \sigma|_L$$

$$\frac{\text{Gal}(M/K)}{\text{Gal}(M/L)} \xrightarrow{\sim} \text{Gal}(L/K)$$

and $\text{Gal}(M/L)$ is closed.

4.2 Unramified Extensions and Weil Groups

Definition 100. Let K be a local field, M/K an algebraic extension. M/K is **unramified** (or **totally ramified**) if L/K is unramified (or totally ramified) for every finite subextension L/K of M/K .

In general, an algebraic extension M/K has a maximal unramified subextension $T = T_{M/K}/K$, which is Galois.

If L/K is a finite unramified extension of local fields with $q = \#k_K$, then $\text{Gal}(L/K) \xrightarrow{\sim} \text{Gal}(k_L/k_K) \ni x \mapsto x^q$, so $\text{Gal}(L/K)$ is cyclic with a canonical generator $\text{Frob}_{L/K}$, which is a lift of $x \mapsto x^q$. This is called the (arithmetic) **Frobenius element** of L/K .

Frob is compatible in towers: if $M/L/K$ are finite unramified extensions of local fields, then $\text{Frob}_{M/K}|_L = \text{Frob}_{L/K}$ ($x \mapsto x^q$ on k_M restricts to $x \mapsto x^q$ on k_L , $q = \#k_K$).

\implies for M/K an arbitrary unramified extension, we get

$$\text{Frob}_{L/K} \in \varprojlim_{\substack{L/K \\ \text{finite subexts} \\ \text{of } M/K}} \text{Gal}(L/K) \cong \text{Gal}(M/K)$$

so we get an element $\text{Frob}_{M/K} \in \text{Gal}(M/K)$. It is the unique lift of $x \mapsto x^{\#k_K}$ on k_M/k_K .