Local Fields

Cambridge Part III, Michaelmas 2022
Taught by Rong Zhou
Notes taken by Leonard Tomczak

Contents

1 Valued Fields

1.1 Absolute Values and Valuations

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

1. $|x| \geq 0$ *for all $x \in K$ with equality iff $x = 0$.*
2. $|xy| = |x| \cdot |y|$ *for all $x, y \in K$.*
3. $|x + y| \leq |x| + |y|$ *for all $x, y \in K$.*

An absolute value $|\cdot|$ is called non-archimedean *if it satisfies the* ultrametric inequality

$$|x + y| \leq \max\{|x|, |y|\}$$

for all $x, y \in K$. Otherwise it is called archimedean.

It is easily seen that if $|\cdot|$ is non-archimedean and $x, y \in K$ with $|x| < |y|$, then $|x + y| = \max(|x|, |y|) = |y|$.

Two absolute values on a field are said to be *equivalent* if they define the same topology.

$|\cdot|$ is called the *trivial absolute value* on K if $|x| = 1$ for all $x \neq 0$.

Example. Let $K = \mathbb{Q}$ and p a prime number. Given $x \in \mathbb{Q}^\times$ write $x = p^n \frac{a}{b}$ with $a, b \in \mathbb{Z}$ not divisible by p. Then let $|x|_p := p^{-n}$ and set $|0|_p = 0$. Then $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$, called the *p-adic absolute value*. The field $\mathbb{Q}_p$ of *p-adic numbers* is defined to be the completion of $\mathbb{Q}$ w.r.t. the p-adic absolute value.

Of course $\mathbb{Q}$ also has the ordinary archimedean absolute value $|\cdot|_\infty$ whose completion is $\mathbb{R}$. We will later see (Theorem 3.6) that every absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_p$ for some prime p or to $|\cdot|_\infty$.

Proposition 1.1. *Let $|\cdot|, |\cdot|'$ non-trivial absolute values on field K. TFAE:*

(i) $|\cdot|, |\cdot|'$ *are equivalent.*

(ii) $|x| < 1 \Leftrightarrow |x|' < 1$ *for all $x \in K$.*

(iii) There exists $c \in \mathbb{R}_{>0}$ such that $|x|^c = |x|'$ for all $x \in K$.

Proof. $(i) \implies (ii)$ is clear from $|x| < 1 \Leftrightarrow x^n \to 0$ w.r.t. $|\cdot|$.

$(ii) \implies (iii)$ Let $a \in K^\times$ such that $|a| > 1$. We need to show that for all $x \in K^\times$, $\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}$. Let $m/n \in \mathbb{Q}$ such that $\frac{\log|x|}{\log|a|} < m/n$, i.e. $|\frac{x^n}{a^m}| < 1$. Then $|\frac{x^n}{a^m}|' < 1$ and hence $\frac{\log|x|'}{\log|a|'} < m/n$. Thus $\frac{\log|x|}{\log|a|} \geq \frac{\log|x|'}{\log|a|'}$ and similarly $\leq$.

$(iii) \implies (i)$ clear. □

The ultra-metric inequalities gives the following lemma:

Lemma 1.2. *If $(x_n)_{n\in\mathbb{N}}$ is a sequence in K such that $|x_n - x_{n+1}| \to 0$ as $n \to \infty$, then $(x_n)_n$ is a Cauchy sequence. In particular $(x_n)_n$ converges if K is complete.*

Example. $p = 5$. We construct a sequence $(x_n)_n$ in $\mathbb{Q}$ such that

(*i*) $x_n^2 + 1 \equiv 0 \pmod{5^n}$,

(*ii*) $x_n \equiv x_{n+1} \pmod{5^n}$

as follows: Take $x_1 = 2$. Let $x_n^2 + 1 = a5^n$ and $x_{n+1} = x_n + b5^n$. Then

$$x_{n+1}^2 + 1 \equiv a5^n + 2bx_n5^n \bmod 5^{n+1},$$

i.e. want b such that $a + 2bx_n \equiv 0 \pmod 5$ which is possible as $2, x_n$ are coprime to 5. Now (*ii*) implies that $(x_n)_n$ is Cauchy w.r.t. $|\cdot|_5$. Suppose $x_n \to L \in \mathbb{Q}$. Then $x_n^2 \to L^2$. By (*i*) we have $x_n^2 \to -1$, hence $L^2 = -1$, a contradiction. So $\mathbb{Q}$ is not 5-adically complete.

Now let $(K, |\cdot|)$ be non-archimedean valued field. For $x \in K, r \in \mathbb{R}_{>0}$ we let:

$$B(x,r) := \{y \in K \mid |y - x| < r\},$$
$$\overline{B}(x,r) := \{y \in K \mid |y - x| \leq r\}.$$

(Note that $\overline{B}(x,r)$ need not be the closure of $B(x,r)$.)

Lemma 1.3. *Let $x \in K, r \in \mathbb{R}_{>0}$*

(*i*) *If $z \in B(x,r)$, then $B(z,r) = B(x,r)$.*

(*ii*) *If $z \in \overline{B}(x,r)$, then $\overline{B}(z,r) = \overline{B}(x,r)$.*

(*iii*) *$B(x,r)$ is closed.*

(*iv*) *$\overline{B}(x,r)$ is open.*

Proof. Follows easily from the ultra-metric inequality. □

Definition. *A* valuation *on a field K is a function $v : K \to \mathbb{R}^\times$ such that for all $x, y \in K$ the following holds:*

(*i*) *$v(xy) = v(x) + v(y)$,*

(*ii*) *$v(x + y) \geq \min(v(x), v(y))$.*

Valuations correspond to (equivalence classes of) non-archimedean absolute values on K. Given a valuation v and a fixed $\alpha > 1$, define $|x| := \alpha^{-v(x)}$ for $x \neq 0$. We will thus sometimes switch between (non-archimedean) absolute values and valuations, whichever is more convenient.

Definition. *Let $(K, |\cdot|)$ be a non-archimedean valued field. We let*

$$\mathcal{O}_K = \{x \in K \mid |x| \leq 1\} = \{x \in K \mid v(x) \geq 0\},$$
$$\mathfrak{m} = \{x \in K \mid |x| < 1\} = \{x \in K \mid v(x) > 0\}.$$

$\mathcal{O}_K$ is called the valuation ring *of K. The* residue field *is $\mathcal{O}_K/\mathfrak{m}$.*

Note that $\mathcal{O}_K$ is indeed a subring of K and $\mathfrak{m}$ is its unique maximal ideal.

Definition. *A valuation v on K is* discrete *if $v(K^\times) \cong \mathbb{Z}$. If $\pi \in K^\times$ is such that $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$, then π is called a* uniformizer.

Lemma 1.4. *Let (K, v) be a valued field. TFAE:*

(*i*) *v is discrete.*

(*ii*) *$\mathcal{O}_K$ is a PID.*

(*iii*) *$\mathcal{O}_K$ is noetherian*

(*iv*) *$\mathfrak{m}$ is principal.*

Proof. $(i) \Rightarrow (ii)$: Let $0 \neq I \subseteq \mathcal{O}_K$ be an ideal. Let $x \in I$ with $v(x)$ minimal. Then $I = x\mathcal{O}_K$. Thus, $\mathcal{O}_K$ is a PID.

$(ii) \Rightarrow (iii)$: clear.

$(iii) \Rightarrow (iv)$: Write $\mathfrak{m} = (x_1, \ldots, x_n)$, wlog $v(x_1) \leq \cdots \leq v(x_n)$. Then $\mathfrak{m} = x_1\mathcal{O}_K$.

$(iv) \Rightarrow (i)$: Let $\mathfrak{m} = \pi\mathcal{O}_K$ and $c = v(\pi)$. Then, if $x \in \mathfrak{m}$, then $v(x) \geq c$, hence $v(K^\times) \cap (0, c) = \emptyset$ which easily implies that $v(K^\times) = c\mathbb{Z}$. ☐

Lemma 1.5. *If v is a discrete valuation on K with uniformizer π, then for every $x \in K^\times$ there are unique $n \in \mathbb{Z}, u \in \mathcal{O}_K^\times$ such that $v = \pi^n u$.*

Definition. *A ring R is called a* discrete valuation ring *(DVR) if R is a principal ideal domain with exactly one non-zero prime ideal.*

Lemma 1.6. *Let K be a field. If v is a discrete valuation on K, then $\mathcal{O}_K$ is a DVR. Conversely if R is a DVR with $K = \operatorname{Frac} R$, then there is a discrete valuation on K such that $\mathcal{O}_K = R$.*

Example. The rings $\mathbb{Z}_{(p)}$ with p prime and $k[\![t]\!]$ with k a field are DVRs.

1.2 p-adic numbers

Recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ w.r.t. the p-adic absolute value. The ring of *p-adic integers* is its valuation ring, denoted $\mathbb{Z}_p$.

Proposition 1.7. *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. In particular $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ w.r.t. $|\cdot|_p$.*

Proof. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ and $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is open, $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$. Note that $\mathbb{Z}_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\} = \mathbb{Z}_{(p)}$. Thus it suffices to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. Let $a/b \in \mathbb{Z}_{(p)}$ with $a, b \in \mathbb{Z}, p \nmid b$. For $n \in \mathbb{N}$ choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \pmod{p^n}$. Then $y_n \to \frac{a}{b}$ w.r.t. $|\cdot|_p$. □

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings together with homomorphisms $\varphi_n : A_{n+1} \to A_n$. Recall that the *inverse limit* of the system $((A_n)_n, (\varphi)_n)$ is

$$A := \varprojlim_n A_n = \{(a_n) \in \prod_{n=1}^{\infty} A_n \mid \varphi_n(a_{n+1}) = a_n \text{ for all } n \in \mathbb{N}\}.$$

It is again a set/group/ring and inherits the algebraic structure from $\prod_{n=1}^{\infty} A_n$. Let $\theta_m : A \to A_m$ be the projection onto the m-th coordinate. Then $(A, (\theta_m)_m)$ enjoys the following universal property:

Proposition 1.8. *Let B be a set/group/ring together with homomorphisms $\psi_n : B \to A_n$ such that the diagram*

$$\begin{array}{ccc} B & \xrightarrow{\psi_{n+1}} & A_{n+1} \\ & \searrow^{\psi_n} & \downarrow{\scriptstyle \varphi_n} \\ & & A_n \end{array}$$

commutes. Then there exists a unique homomorphism $\psi : B \to A$ such that $\theta_n \circ \psi = \psi_n$ for all n.

Definition. *Let R be a ring and I an ideal of R. Then*

$$\widehat{R} := \varprojlim_n R/I^n$$

*is called the I-*adic completion *of R. The transition maps are the projections $R/I^{n+1} \to R/I^n$. If the natural map $R \to \widehat{R}$ (induced by the projections $R \to R/I^n$ and the universal property) is an isomorphism, R is called I-*adically complete.

Let $(K, |\cdot|)$ be a non-archimedean valued field and $\pi \in \mathcal{O}_K$ such that $|\pi| < 1$.

Proposition 1.9. *Assume K is complete w.r.t. $|\cdot|$.*

(i) *Then $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n$, i.e. $\mathcal{O}_K$ is π-adically complete*

(ii) *Every* $x \in \mathcal{O}_K$ *can be written uniquely as* $x = \sum_{i=0}^{\infty} a_i \pi^i$, $a_i \in A \subseteq \mathcal{O}_K$ *where* A *is a set of coset representatives for* $\mathcal{O}_K/\pi\mathcal{O}_K$.

Moreover any such series $\sum_{i=0}^{\infty} a_i \pi^i$ *converges.*

Proof.

(i) Note that $\mathcal{O}_K$ is complete. If $x \in \bigcap_{n=0}^{\infty} \pi^n \mathcal{O}_K$, then $v(x) \geq nv(\pi)$ for all n, so $x = 0$, hence $\mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi^n$ is injective. Let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n$. For each n let $y_n \in \mathcal{O}_K$ be a lift of x_n. Then $y_n - y_{n+1} \in \pi^n \mathcal{O}_K$ so that $v(y_n - y_{n+1}) \geq nv(\pi)$. Thus $(y_n)_{n=1}^{\infty}$ is a Cauchy sequence in $\mathcal{O}_K$, so it converges to an element $y \in \mathcal{O}_K$ which maps to $(x_n)_{n=1}^{\infty}$ in $\varprojlim_n \mathcal{O}_K/\pi^n$.

(ii) is an exercise. □

Warning: If $(K, |\cdot|)$ is not discretely valued, $\mathcal{O}_K$ is not necessarily $\mathfrak{m}$-adically complete.

Corollary 1.10.

(i) $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

(ii) Every $x \in \mathbb{Q}_p$ *can be written uniquely as* $\sum_{i=n}^{\infty} a_i p^i$ *where* $a_i \in \{0, \ldots, p-1\}$.

Proof. It suffices to show that $\mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p/p^n\mathbb{Z}_p$. Let $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map. Clearly, $\ker(f_n) = \{x \in \mathbb{Z} \mid v_p(x) \geq n\} = p^n\mathbb{Z}$. Let $y \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ and $c \in \mathbb{Z}_p$ be a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there is $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$, i.e. $f_n(x) = y$. □

2 Complete Valued Fields

2.1 Hensel's Lemma

Theorem 2.1 (Hensel's Lemma version 1)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(t) \in \mathcal{O}_K[t]$ and assume there is $a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$. Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $|x - a| < |f'(a)|$.*

Proof. Let $\pi \in \mathcal{O}_K$ be a uniformizer and let $r = v(f'(a))$. We construct a sequence $(x_n)_n$ in $\mathcal{O}_K$ such that (i) $f(x_n) \equiv 0 \pmod{\pi^{n+2r}}$ and (ii) $x_n \equiv x_{n+1} \pmod{\pi^{n+r}}$.

Take $x_1 = a$, then $f(x_1) \equiv 0 \pmod{\pi^{1+2r}}$ by assumption. Suppose we have constructed $x_1, \dots, x_n$ satisfying (i) and (ii). Define $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$. Since $x_n \equiv x_1 \pmod{\pi^{r+1}}$, $v(f'(x_n)) = r$ and hence $\frac{f(x_n)}{f'(x_n)} \equiv 0 \pmod{\pi^{n+r}}$ by (i).

Thus, $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$, so (ii) holds. Note that $f(x_{n+1}) = f(x_n) + f'(x_n)c + g(x_n)c^2$ where $c = -\frac{f(x_n)}{f'(x_n)}$. Since $c \equiv 0 \pmod{\pi^{n+r}}$, we get $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \pmod{\pi^{n+2r+1}}$.

Property (ii) implies that $(x_n)_n$ is Cauchy. So let $x \in \mathcal{O}_K$ such that $x_n \to x$. By (i) it follows that $f(x) = \lim_{n\to\infty} f(x_n) = 0$. Moreover (ii) implies that $a = x_1 \equiv x_n \pmod{\pi^{r+1}}$ for all n, hence $|x - a| < |f'(a)|$.

Uniqueness: Suppose x' also satisfies $f(x') = 0$ and $|x' - a| < |f'(a)|$. Let $\delta = x' - x$. Then $|\delta| = |x' - x| < |f'(a)|$. Also $0 = f(x') = f(x + \delta) = f(x) + f'(x)\delta + (\dots)\delta^2$. Hence $|f'(x)\delta| \leq |\delta|^2$. Since $a \equiv x \pmod{\pi^{1+r}}$, we have $f'(x) \equiv f'(a) \not\equiv 0 \pmod{\pi^{1+r}}$, so $|f'(x)| = |f'(a)|$. Thus, if $\delta \neq 0$, we would get $|f'(a)| \leq |\delta|$, a contradiction. □

Corollary 2.2.

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \textit{if } p > 2, \\ (\mathbb{Z}/2\mathbb{Z})^3 & \textit{if } p = 2. \end{cases}$$

Proof. Case $p > 2$. Let $b \in \mathbb{Z}_p^\times$. Applying Hensel's Lemma to $x^2 - b$, we find that $b \in (\mathbb{Z}_p^\times)^2$ iff $\bar{b} \in (\mathbb{F}_p^\times)^2$. Thus $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$. We have an isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \cong \mathbb{Q}_p^\times$, then done.

Case $p = 2$. Let $b \in \mathbb{Z}_p^\times$ and $f(x) = x^2 - b$. Let $b \equiv 1 \pmod 8$. $|f(1)|_2 \leq 2^{-3} < 2^{-2} = |f'(1)|^2$. Thus, f has a unique root a with $a \equiv b \pmod 4$.

Hence, $b \in (\mathbb{Z}_p^\times)^2$ iff $b \equiv 1 \pmod 8$. Thus, $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We conclude as in the case $p > 2$. □

Theorem 2.3 (Hensel's Lemma version 2)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(x) \in \mathcal{O}_K[x]$. Suppose that $\bar{f}(x) \in k[x]$ factorises as $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ in $k[x]$ with $\bar{g}(x), \bar{h}(x)$ coprime. Then there is a factorization $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$ with $\bar{g}(x) \equiv g(x) \pmod{\mathfrak{m}}$, $\bar{h} \equiv h \pmod{\mathfrak{m}}$ and $\deg g = \deg \bar{g}$.*

Proof. Example Sheet 1. □

Corollary 2.4. *Let $f(x) = a_n x^n + \cdots + a_0 \in K[x]$ where $(K, |\cdot|)$ is complete discretely valued with $a_0, a_n \neq 0$. If f is irreducible, then $|a_i| \leq \max\{|a_0|, |a_n|\}$ for all i.*

Proof. Upon rescaling we may assume that $f \in \mathcal{O}_K[x]$ with $\max_i |a_i| = 1$, so we need to show that $|a_0| = 1$ or $|a_n| = 1$. Suppose this is not the case. Let r be minimal such that $|a_r| = 1$. Then $0 < r < n$. Thus we have $f(x) \equiv x^r(a_r + \cdots + a_n x^{n-r}) \pmod{\mathfrak{m}}$. By Hensel's Lemma version 2 we can lift this factorization to a non-trivial factorization over $\mathcal{O}_K$, contradicting the irreducibility. □

2.2 Teichmüller Lifts

Definition. *A ring R of characteristic $p > 0$ is called* perfect *if the Frobenius $x \mapsto x^p$ is a bijection.*

Theorem 2.5. *Let $(K, |\cdot|)$ be a complete discretely valued field such that $k = \mathcal{O}_K/\mathfrak{m}$ is a perfect field of characteristic p. Then there exists a unique map $[\cdot] : k \to \mathcal{O}_K$ such that*

(i) $a = [a] \bmod \mathfrak{m}$

(ii) $[ab] = [a][b]$

Moreover if $\operatorname{char} K = p$*, this lifting $[\cdot]$ is a ring homomorphism.*

The element $[a] \in \mathcal{O}_K$ is called the Teichmüller lift of *a.*

Lemma 2.6. *Let $(K, |\cdot|)$ be as in the theorem and $\pi \in \mathcal{O}_K$ a uniformizer. Let $x, y \in \mathcal{O}_K$ such that $x \equiv y \pmod{\pi^k}$ for some $k \geq 1$. Then $x^p \equiv y^p \pmod{\pi^{k+1}}$.*

Proof. Let $x = y + u\pi^k$ with $u \in \mathcal{O}_K$. Then

$$x^p = \sum_{i=0}^{p} \binom{p}{i} y^{p-i}(u\pi^k)^i = y^p + p\pi^k(\dots) + u^p\pi^{pk} \equiv y^p \pmod{\pi^{k+1}}.$$

□

Proof of the theorem. Let $a \in k$. For each $i \geq 0$ we choose a lift $y_i \in \mathcal{O}_K$ of a^{1/p^i} and we define $x_i = y_i^{p^i}$. We claim that $(x_i)_i$ is a Cauchy sequence and its limit x is independent of the choice of y_i. By construction $y_i \equiv y_{i+1}^p \pmod{\pi}$. By the lemma and induction we obtain $y_i^{p^r} \equiv y_{i+1}^{p^{r+1}} \pmod{\pi^{r+1}}$, so $x_i \equiv x_{i+1} \pmod{\pi^{i+1}}$ (take $r = i$). Then $(x_i)_i$ is Cauchy, so $x_i \to x \in \mathcal{O}_K$. Suppose $(x_i')_i$ arises from another choice of y_i' lifting a^{1/p_i}. Then $(x_i')_i$ is Cauchy and $x_i' \to x' \in \mathcal{O}_K$. Let $x_i'' = x_i$ for i even and $x_i'' = x_i$ for i odd. Then x_i'' arises in a similar way and we get that x_i'' is Cauchy. But then the subsequences x_i, x_i' must converge to the same limit, i.e. $x = x'$.

We define $[a] = x$. Then $x_i = y_i^{p^i} \equiv (a^{1/p^i})^{p^i} = a \pmod{\pi}$, so $[a]$ is indeed a lift of a, i.e. (i) is satisfied.

Let $b \in k$ and we choose $u_i \in \mathcal{O}_K$ a lift of b^{1/p^i}. Let $z_i = u_i^{p^i}$. Then $\lim_i z_i = [b]$. Now $u_i y_i$ is a lift of $(ab)^{1/p^i}$, hence $[ab] = \lim_{i\to\infty} x_i z_i = \lim_i x_i \lim_i z_i = [a][b]$. This shows that (ii) is satisfied.

Suppose that $\operatorname{char} K = p$. $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$, so $[a+b] = \lim_{i\to\infty}(y_i + u_i)^{p^i} = \lim_{i\to\infty} y_i^{p^i} + u_i^{p^i} = \lim_i x_i + \lim_i z_i = [a] + [b]$.

Uniqueness: Let $\phi : k \to \mathcal{O}_K$ be another such map. Then for $a \in k$, $\phi(a^{1/p^i})$ lifts a^{1/p^i}. It follows that $[a] = \lim_{i\to\infty} \phi(a^{1/p^i})^{p^i} = \phi(a)$. □

E.g. $K = \mathbb{Q}_p$, $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$. $a \in \mathbb{F}_p^\times$, $[a]^{p-1} = [a^{p-1}] = [1] = 1$, so $[a]$ is a $(p-1)$-th root of unity.

More generally:

Lemma 2.7. *$(K, |\cdot|)$ complete discretely valued field. If $k = \mathcal{O}_K/\mathfrak{m} \subseteq \mathbb{F}_p^{\mathrm{alg}}$, then $[a] \in \mathcal{O}_K$ is a root of unity.*

Theorem 2.8. *Let $(K, |\cdot|)$ be a complete discretely valued field with $\operatorname{char} K = p > 0$. Assume k is perfect. Then $K \cong k(\!(t)\!)$.*

Proof. It suffices to show that $\mathcal{O}_K \cong k[\![t]\!]$. Fix $\pi \in \mathcal{O}_K$ a uniformizer, let $[\cdot] : k \to \mathcal{O}_K$ be the Teichmüller lift. Define $\varphi : k[\![t]\!] \to \mathcal{O}_K$ by $\varphi(\sum_{i=0}^\infty a_i t^i) = \sum_{i=0}^\infty [a_i]\pi^i$. Then φ is a ring homomorphism since $[\cdot]$ is and it is a bijection since every element in $\mathcal{O}_K$ has a unique π-adic expansion. □

2.3 Extensions of complete valued fields

Theorem 2.9. *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field and L/K a finite extension of degree n. Then*

(1) $|\cdot|$ extends uniquely to an absolute value $|\cdot|_L$ on L defined by

$$|y|_L = |N_{L/K}(y)|^{1/n}.$$

(2) L is complete w.r.t. $|\cdot|_L$.

Definition. *Let Let $(K, |\cdot|)$ be a non-archimedean valued field, V a vector space over K. A* norm *on V is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ satisfying*

(i) $\|x\| = 0$ *iff* $x = 0$,

(ii) $\|\lambda x\| = |\lambda| \, \|x\|$ *for* $\lambda \in K, x \in V$,

(iii) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$ *for* $x, y \in V$.

Example. Let V be finite-dimensional over K and $e_1, \ldots, e_n$ a basis for V. The sup-norm on V (relative to this basis) is defined by

$$\|x\|_{\sup} = \sup_i |x_i|$$

where $x = \sum_i x_i e_i$.

Definition. *Two norms $\|\cdot\|_1, \|\cdot\|_2$ on V are equivalent if there are $C, D > 0$ such that $C \|x\|_1 \leq \|x\|_2 \leq D \|x\|_1$ for all $x \in V$.*

Note that two norms are equivalent iff they induce the same topology.

Proposition 2.10. *Let $(K, |\cdot|)$ be a complete non-archimedean valued field and V a finite dimensional vector space over K. Then V is complete w.r.t. any* sup-*norm.*

Proof. Easy, as in the real case. □

Theorem 2.11. *Let $(K, |\cdot|)$ be complete non-archimedean valued field and V a finite dimensional vector space over K. Then any two norms on V are equivalent, in particular V is complete w.r.t. any norm.*

Proof. Since equivalence of norms is an equivalence relation, we may assume that every norm $\|\cdot\|$ is equivalent to the sup-norm w.r.t. to some chosen basis $e_1, \ldots, e_n$. Set $D := \max_i\{\|e_i\|\}$. Then clearly, $\|x\| \leq D \|x\|_{\sup}$ for all $x \in V$. To find the constant C in the other direction ($C \|x\|_{\sup} \leq \|x\|$) we induct on n. For $n = 1$ the existence of C is clear since every element of V is a multiple of e_1. Let $n > 1$. Set $V_i = \langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n \rangle$. By induction hypothesis V_i is complete, hence closed in V. Then $e_i + V_i$ is also closed for all i, thus so is $S = \bigcup_{i=1}^n (e_i + V_i)$. S is a closed subset that does not contain 0, hence there exists $C > 0$ such that $B(0, C) \cap S = \emptyset$. Let $0 \neq x = \sum_i x_i e_i$ and suppose that $|x_i| = \|x\|_{\sup}$. Then $\frac{1}{x_i} x \in S$, so $\|\frac{1}{x_i} x\| \geq C$, i.e. $\|x\| \geq C \|x\|_{\sup}$. □

Lemma 2.12. *Let $(K, |\cdot|)$ be a valued field. Then $\mathcal{O}_K$ is integrally closed in K.*

Proof of Theorem 2.9. We show that $|\cdot|_L = |N_{L/K}(\cdot)|^{1/n}$ defines an absolute value on L. The only non-trivial property is that $|x+y|_L \leq \max\{|x|_L, |y|_L\}$. Let $\mathcal{O}_L = \{y \in L \mid |y|_L \leq 1\}$. We claim that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L and hence in particular a subring.

Assuming this we prove the ultrametric inequality. Wlog we may assume that $|x|_L \leq |y|_L$. Then $|x/y|_L \leq 1$, so $x/y \in \mathcal{O}_L$. But then also $x/y + 1 \in \mathcal{O}_L$ and so $|x+y|_L \leq |y|_L$.

Proof of the claim: Suppose $y \in L$ is integral over $\mathcal{O}_K$, let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in K[x]$ be its minimal polynomial. Since the coefficients are integral over $\mathcal{O}_K$ and $\mathcal{O}_K$ is integrally closed, we have $f(x) \in \mathcal{O}_K[x]$. Then $|N_{L/K}(y)| = \left|\pm a_0^k\right| \leq 1$, so $y \in \mathcal{O}_L$. Conversely, suppose $y \in \mathcal{O}_L$ and let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in K[x]$ be its minimal polynomial over K. By 2.4 we have $|a_{m-1}|, \ldots, |a_1| \leq \max\{1, |a_0|\} = 1$, so $f \in \mathcal{O}_K[x]$ and thus y is integral over K.

This shows that $|\cdot|_L$ is an absolute value. It clearly extends the absolute value on K. If $|\cdot|'_L$ is another absolute value on L extending $|\cdot|$, then $|\cdot|_L, |\cdot|'_L$ are norms on L. So by Theorem 2.11 they are equivalent. Thus $|\cdot|'_L = |\cdot|^c_L$ for some $c \in \mathbb{R}_{>0}$. Since both absolute values agree on K, we must have $c = 1$. □

Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field.

Corollary 2.13. *Let L/K be a finite extension.*

(i) L is discretely valued w.r.t. $|\cdot|_L$.

(ii) $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Proof. (ii) had been proven during the proof of the theorem.

For (i) let v be the valuation on K and v_L its extension to L (via the extension of the absolute value). Then $v_L(y) = \frac{1}{n}v(N_{L/K}(y))$, so $v_L(L^\times) \subseteq \frac{1}{n}v(K^\times)$ is also discrete. □

Corollary 2.14. *Let K^{alg}/K be an algebraic closure. Then the absolute value on K extends uniquely to a unique absolute value on K^{alg}.*

Remark: $|\cdot|_{K^{\mathrm{alg}}}$ is never discrete. E.g. $K = \mathbb{Q}_p$, $\sqrt[n]{p} \in \mathbb{Q}_p^{\mathrm{alg}}$ for all $n \in \mathbb{Z}_{\geq 0}$. Then $v(\sqrt[n]{p}) = \frac{1}{n}v(p) = \frac{1}{n}$.

Proposition 2.15. *Let L/K be a finite extension. Assume that*

(i) $\mathcal{O}_K$ is compact.

(ii) The extension k_L/k of residue fields is finite and separable.

Then there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

(Later we will see that condition (i) already implies (ii))

Proof. Since k_L/k is separable there exists $\bar{\alpha} \in k_L$ such that $k_L = k(\bar{\alpha})$. Let $\alpha \in \mathcal{O}_K$ be a lift of $\bar{\alpha}$ and let $g(x) \in \mathcal{O}_K[x]$ be a monic lift of the minimal polynomial of $\bar{\alpha}$. Fix a uniformizer $\pi_L \in \mathcal{O}_L$. As $\bar{g}(x) \in k[x]$ is separable, we have $g(\alpha) \equiv 0 \pmod{\pi_L}$, but $g'(\alpha) \not\equiv \pmod{\pi_L}$. Thus, by replacing α by $\alpha + \pi_L$ if necessary we may assume that $v(g(\alpha)) = 1$ (where v is the normalized valuation on L). As $\mathcal{O}_K$ is compact, so is

$\mathcal{O}_K[\alpha]$, hence it is closed in $\mathcal{O}_L$. Since $k_L = k(\bar{\alpha})$, $\mathcal{O}_K[\alpha]$ contains a set $\{\lambda_i\}$ of coset representatives of $k_L = \mathcal{O}_L/\beta\mathcal{O}_L$ where $\beta = g(\alpha) \in \mathcal{O}_K[\alpha]$. So every $y \in \mathcal{O}_L$ can be written as $\sum_{i=0}^{\infty} \lambda_i \beta^i$ with $\lambda_i \in \mathcal{O}_K[\alpha]$. By truncating we see that y is in the closure of $\mathcal{O}_K[\alpha]$, hence $\mathcal{O}_K[\alpha] = \mathcal{O}_L$. $\square$

Remark: Assumption (i) is actually not necessary.

3 Local Fields

Definition. *Let $(K, |\cdot|)$ be a valued field. K is a* local field *if it is complete and locally compact.*

Proposition 3.1. *Let $(K, |\cdot|)$ be a non-archimedean complete valued field. Then TFAE:*

(i) K is locally compact.

(ii) $\mathcal{O}_K$ is compact.

(iii) v is discrete and $k = \mathcal{O}_K/\mathfrak{m}$ is finite.

Proof. (i) $\implies$ (ii). Let U be a compact neighborhood of 0. Then there exists $0 \neq x \in \mathcal{O}_K$ such that $x\mathcal{O}_K \subseteq U$. Since $x\mathcal{O}_K$ is closed, $x\mathcal{O}_K$ is compact. From this it follows that $\mathcal{O}_K$ is compact as multiplication by x defines a homeomorphism $\mathcal{O}_K \to x\mathcal{O}_K$.

(ii) $\implies$ (i). Immediate.

(ii) $\implies$ (iii). Let $x \in \mathfrak{m}$ and $A_x \subseteq \mathcal{O}_K$ be a set of coset representatives for $\mathcal{O}_K/x\mathcal{O}_K$. Then $\mathcal{O}_K = \bigcup_{y \in A_x} y + x\mathcal{O}_K$ a disjoint open cover. As $\mathcal{O}_K$ is compact, A_x and so $\mathcal{O}_K/x\mathcal{O}_K$ is finite, hence $\mathcal{O}_K/\mathfrak{m}$ is finite. Suppose v is not discrete. Let $x = x_1, x_2, \ldots$ such that $v(x_1) > v(x_2) > \cdots > 0$. Then $x_1\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq \cdots \subsetneq \mathcal{O}_K$. This is not possible as $\mathcal{O}_K/x_1\mathcal{O}_K$ is finite.

(iii) $\implies$ (ii). Let $(x_n)_n$ be a sequence in $\mathcal{O}_K$ and fix a uniformizer $\pi \in \mathcal{O}_K$. Since $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong k$, we have $\mathcal{O}_K/\pi^i\mathcal{O}_K$ is finite for all i. Since $\mathcal{O}_K/\pi\mathcal{O}_K$ is finite, there exists $a \in \mathcal{O}_K/\pi\mathcal{O}_K$ and a subsequence $(x_{1_n})_{n=1}^{\infty}$ such that $x_{1_n} \equiv a \pmod{\pi}$ for all n. Since $\mathcal{O}_K/\pi^2\mathcal{O}_K$ is finite, there exists a_2 and a subsequence $(x_{2_n})_n$ of (x_{1n}) such that $x_{2n} \equiv a_2 \pmod{\pi^2\mathcal{O}_K}$. Continue like this and get a sequence $(x_{in})_n$ for $i = 1, 2\ldots$ such that (1) $(x_{(i+1)n})_n$ is a subsequence of $(x_{in})_n$ and (2) for any i there exists $a_i \in \mathcal{O}_K/\pi^i\mathcal{O}_K$ such that $x_{in} \equiv a \pmod{\pi^i\mathcal{O}_K}$ for all n. Then necessarily $a_i \equiv a_{i+1} \pmod{\pi^i}$ for all i.

Now let $y_i = x_{ii}$, this defines a subsequence of $(x_n)_n$. Moreover $y_i \equiv y_{i+1} \pmod{\pi^i\mathcal{O}_K}$, so $(y_i)_i$ is Cauchy, hence converges by completeness. □

Examples.

(i) $\mathbb{Q}_p$ is a local field.

(ii) $\mathbb{F}_q(\!(t)\!)$ is a local field.

Proposition 3.2. *Let K be a non-archimedean local field. Under the isomorphism $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ the topology on $\mathcal{O}_K$ coincides with the profinite topology.*

Proof. One checks that the sets $B = \{a + \pi^n\mathcal{O}_K \mid n \in \mathbb{Z}_{\geq 1}, a \in \mathcal{O}_K\}$ is a basis of open sets in both topologies. $\square$

Lemma 3.3. *Let K be a non-archimedean local field and L/K a finite extension. Then L is a local field.*

Proof. We know that L is complete and discretely valued. It suffices to show that $k_L = \mathcal{O}_L/\mathfrak{m}_L$ is finite. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L as a K-vector space. Then the corresponding sup-norm is equivalent to $|\cdot|_L$, so there exists $r > 0$ such that $\mathcal{O}_L \subseteq \{x \in L \mid \|x\|_{\text{sup}} \leq r\}$. Take $a \in K$ such that $|a| \geq r$. Then $\mathcal{O}_L \subseteq \oplus_{i=1}^n a\alpha_i\mathcal{O}_K$. Thus, $\mathcal{O}_L$ is finitely generated as a $\mathcal{O}_K$-module, so k_L is finitely generated as a k-module, so k_L is finite. $\square$

Definition. *A non-archimedean valued field $(K, |\cdot|)$ has* equal characteristic *if* $\operatorname{char} K = \operatorname{char} k$*, otherwise* mixed characteristic*.*

Theorem 3.4. *Let K be a non-archimedean local field of equal characteristic $p > 0$. Then $K \cong \mathbb{F}_{p^n}(\!(t)\!)$.*

Proof. We know that the residue field is finite, say $\mathbb{F}_{p^n}$. Then it is perfect, so we know from the Teichmüller lifts that $K \cong \mathbb{F}_{p^n}(\!(t)\!)$. $\square$

Lemma 3.5. *An absolute value on a field K is non-archimedean iff it is bounded on $\mathbb{Z}$.*

Proof. "$\Rightarrow$" obvious from the ultrametric inequality.

"$\Leftarrow$" Suppose $|n| \leq B$ for all $n \in \mathbb{Z}$. Let $x, y \in K$ such that $|x| \leq |y|$. Then

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

Then $|x + y| \leq [(m + 1)B]^{1/m}|y|$. Letting $m \to \infty$ we get $|x + y| \leq |y|$, so the absolute value is non-archimedean. $\square$

Theorem 3.6 (Ostrowski's Theorem)**.** *Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the usual absolute value $|\cdot|_\infty$ or a p-adic absolute value $|\cdot|_p$ for some prime p.*

Proof. Case 1. $|\cdot|$ is archimedean. We fix an integer $b > 1$ such that $|b| > 1$ (exists by previous lemma). Let $a > 1$ be an integer and write b^n in base a:

$$b^n = c_m a^m + c_{m-1}a^{m-1} + \cdots + c_0$$

where $0 \leq c_i < a$ and $c_m \neq 0$. Let $B = \max_{0 \leq c < a} |c|$. Then we have

$$|b|^n \leq (m+1) B \max(|a|^m, 1)$$

Then $|b| \leq [(n(\log_a b) + 1)B]^{1/n} \max(|a|^{\log_a b}, 1)$ (Note that $m \leq n \log_a b$) This goes to 1 as $n \to \infty$. Therefore $|b| \leq \max(|a|^{\log_a b}, 1)$ Then $|a| > 1$, and $|b| \leq |a|^{\log_a b}$. Switching the roles of a and b, we obtain $|a| \leq |b|^{\log_b a}$. Then these two inequalities we get

$$\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} =: \lambda$$

Then $|a| = a^\lambda$ for all $a \in \mathbb{Z}_{>1}$. Then $|x| = |x|_\infty^\lambda$ for all $x \in \mathbb{Q}$. Hence $| \cdot |$ is equivalent to $| \cdot |_\infty$.

Case 2. $| \cdot |$ is non-archimedean. Then we have $|n| \leq 1$ for all $n \in \mathbb{Z}$. As $| \cdot |$ is non-trivial, there exists $n \in \mathbb{Z}_{>0}$ such that $|n| < 1$. Then there is a prime factor p of n such that $|p| < 1$. Suppose that there exists another prime $q \neq p$ with $|q| < 1$. Then $rp + sq = 1$ for some integers $r, s \in \mathbb{Z}$. Then $1 = |1| = |rp + rs| < 1$ by the ultrametric inequality, a contradiction. Then $\alpha := |p| < 1$ and $|q| = 1$ for all primes $q \neq p$. By decomposition into prime factors we see that this uniquely determines $| \cdot |$ and shows that it is equivalent to $| \cdot |_p$. □

Theorem 3.7. *Let $(K, |\cdot|)$ be a non-archimedean local field of mixed characteristic. Then K is a finite extension of $\mathbb{Q}_p$ for some prime p.*

Proof. As K has mixed characterstic, $\operatorname{char} K = 0$, so $\mathbb{Q} \subseteq K$. K is non-archimedean, so $| \cdot ||_{\mathbb{Q}}$ is equivalent to $| \cdot |_p$ for some prime p[1]. As K is complete we get $\mathbb{Q}_p \subseteq K$. Let $\pi \in \mathcal{O}_K$ be a uniformizer, v normalized valuation on K and set $v(p) = e$. Then $\mathcal{O}_K / p\mathcal{O}_K \cong \mathcal{O}_K / \pi^e \mathcal{O}_K$ is finite. Let $x_1, \ldots, x_n \in \mathcal{O}_K$ be coset representatives for a basis of $\mathcal{O}_K/p\mathcal{O}_K$ as a $\mathbb{F}_p$-vector space. Then $\{\sum_{i=1}^n a_i x_i \mid a_i \in \{0, 1, \ldots, p-1\}\}$ is a set of coset representatives for $\mathcal{O}_K/p\mathcal{O}_K$. Let $y \in \mathcal{O}_K$. We then get

$$y = \sum_{i=0}^{\infty} \left(\sum_{i=1}^{n} a_{ij} x_i \right) p^i = \sum_{j=1}^{n} \left(\sum_{i=0}^{\infty} a_{ij} p^i \right) x_j.$$

Note that $\sum_{i=0}^\infty a_{ij} p^i$ converges in $\mathbb{Z}_p$, so the x_j give a generating set of $\mathcal{O}_K$ over $\mathbb{Z}_p$. Then K is finite over $\mathbb{Q}_p$. □

Theorem 3.8. *Let $(K, | \cdot |)$ be an archimedean local field. Then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.*

Proof. See example sheet. □

[1] Addendum: We also need that $| \cdot ||_{\mathbb{Q}}$ is non-trivial. This follows from the fact that $\mathcal{O}_K/\mathfrak{m}$ is finite, so that there exists $n \in \mathbb{Z}$ with $n \in \mathfrak{m}$, i.e. $|n| < 1$.

4 Global Fields

Definition. *A* global field *is a field which is either*

(i) an algebraic number field (i.e. a finite extension of $\mathbb{Q}$) or

(ii) a global function field (i.e. a finite extension of $\mathbb{F}_p(t)$).

Lemma 4.1. *Let $(K, |\cdot|)$ be a complete discretely valued field, L/K a finite Galois extension with absolute value $|\cdot|_L$ extending the one on K. Then for any $x \in L$ and $\sigma \in \mathrm{Gal}(L/K)$ we have $|\sigma x|_L = |x|_L$.*

Proof. Follows from the uniqueness of extensions of absolute values on complete fields. □

Lemma 4.2 (Krasner's Lemma)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) \in K[x]$ be a separable irreducible polynomial with roots $\alpha_1, \ldots, \alpha_n \in K^{\mathrm{alg}}$. Suppose $\beta \in K^{\mathrm{alg}}$ is such that $|\beta - \alpha_1| < |\beta - \alpha_i|$ for $i = 2, \ldots, n$. Then $K(\alpha_1) \subseteq K(\beta)$.*

Proof. Let $L = K(\beta)$, $L' = L(\alpha_1, \ldots, \alpha_n)$. L'/L is Galois. Let $\sigma \in \mathrm{Gal}(L'/L)$. We have $|\beta - \sigma\alpha_1| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1| < |\beta - \alpha_i|$ for $i \neq 1$. Therefore $\sigma\alpha_1 = \alpha_1$. Hence $\alpha_1 \in L = K(\beta)$. □

Proposition 4.3. *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{O}_K[x]$ be a separable irreducible monic polynomial. Let $\alpha \in K^{\mathrm{alg}}$ be a root of f. Then there exists $\varepsilon > 0$ such that for any $g(x) = \sum_{i=0}^{n} b_i x^i \in \mathcal{O}_K[x]$ monic with $|a_i - b_i| < \varepsilon$, there exists a root β of $g(x)$ such that $K(\alpha) = K(\beta)$.*

Proof. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of f (which are necessarily distinct). Then $f'(\alpha_1) \neq 0$. We choose ε sufficiently small such that $|g(\alpha_1)| < |f'(\alpha)|^2$ and $|f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha)|$. Then we have $|g(\alpha_1)| < |f'(\alpha_1)|^2 = |g'(\alpha_1)|^2$. By Hensel's Lemma applied to g (in the field $K(\alpha_1)$) there exists $\beta \in K(\alpha_1)$ such that $g(\beta) = 0$ and $|\beta - \alpha_1| < |g'(\alpha_1)| = |f'(\alpha_1)| = \prod_{i=2}^{n} |\alpha_1 - \alpha_i| \leq |\alpha_1 - \alpha_i|$ for $i = 2, \ldots, n$ (by integrality). Since $|\beta - \alpha_1| < |\alpha_1 - \alpha_i| = |\beta - \alpha_i|$, by Krasner's lemma $\alpha_1 \in K(\beta)$ and hence $K(\alpha_1) = K(\beta)$. □

Theorem 4.4. *Let K be a local field, then K is the completion of a global field.*

Proof. Case 1: $|\cdot|$ is archimedean. Then K is $\mathbb{R}$ or $\mathbb{C}$ and thus the completion of $\mathbb{Q}$ or $\mathbb{Q}(i)$ with $|\cdot|_\infty$.

Case 2: $|\cdot|$ non-archimedean, equal characteristic, so $K \cong \mathbb{F}_q((t))$, then K is the completion of $\mathbb{F}_q(t)$ with the t-adic absolute value.

Case 3: $|\cdot|$ non-archimedean, mixed characteristic, so $K = \mathbb{Q}_p(\alpha)$ where α is a root of a monic irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we can choose $g(x) \in \mathbb{Z}[x]$ that is close enough to $f(x)$ such that $K = \mathbb{Q}_p(\beta)$ where β is a root of $g(x)$. Then $\mathbb{Q}(\beta)$ is an algebraic number field. Since $\mathbb{Q}(\beta)$ is dense in $\mathbb{Q}_p(\beta) = K$, K is the completion of $\mathbb{Q}(\beta)$ w.r.t. the restriction of $|\cdot|$ to $\mathbb{Q}(\beta)$. $\square$

5 Dedekind Domains

Definition. *A* Dedekind domain *is a ring R such that*

(i) R is a noetherian integral domain.

(ii) R is integrally closed.

(iii) Every non-zero prime ideal is maximal.

Theorem 5.1. *A ring R is a DVR iff R is a Dedekind domain with exactly one non-zero prime ideal.*

Lemma 5.2. *Let R be a noetherian ring and $I \subseteq R$ a non-zero ideal, then there exist non-zero prime ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_r \subseteq R$ such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq I$.*

Proof. Suppose not, then there is an ideal I maximal with the property that it contains no product of prime ideals. Then I is not prime, so there are elements $x, y \in R \backslash I$ with $xy \in I$. Then both $I+(x)$ and $I+(y)$ contain products of prime ideals. Then also $(I+(x))(I+(y))$ contains a product of prime ideals, a contradiction as $(I+(x))(I+(y)) \subseteq I$. □

Lemma 5.3. *Let R be an integral domain which is integrally closed. Let $I \subseteq R$ be a non-zero finitely generated ideal and $x \in K = \operatorname{Frac} R$. Then if $xI \subseteq I$, we have $x \in R$.*

Proof. Let $I = (c_1, \ldots, c_n)$. Then $xc_i = \sum_{j=1}^n a_{ij} c_j$ for some $a_{ij} \in R$. Let $A = (a_{ij})_{ij}$. Set $B = xI_n - A$. Then $B \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$, so multiplying by the adjugate matrix of B we get $\det B = 0$. This determinant is a monic polynomial in x with coefficients in R, so $x \in R$ as R is integrally closed. □

Proof of Theorem 5.1. "⇒" is clear.

For "⇐" we need to show that R is a PID. Let $\mathfrak{m}$ be the maximal ideal of R.

Step 1. $\mathfrak{m}$ is principal. Let $x \in \mathfrak{m}$ by non-zero. Then $(x) \supseteq \mathfrak{m}^n$ for some $n \geq 1$ by Lemma 5.2. Let n be minimal with this property. Then we may choose $y \in \mathfrak{m}^{n-1} \backslash (x)$. Let $\pi := \frac{x}{y}$. Then $y\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (x)$, so $\pi^{-1}\mathfrak{m} \subseteq R$. Suppose $\pi^{-1}\mathfrak{m} \neq R$, then $\pi^{-1}\mathfrak{m} \subseteq \mathfrak{m}$ and so $\pi^{-1} \in R$ by the lemma. Hence $y \in (x)$, which is a contradiction. Hence $\pi^{-1}\mathfrak{m} = R$, i.e. $\mathfrak{m} = (\pi)$.

Step 2. R is a PID. Let R be any non-zero ideal. Consider the sequence of fractional ideals $I \subseteq \pi^{-1}I \subseteq \pi^{-2}I \subseteq \dots$. Since $\pi^{-1} \notin R$, we have $\pi^{-k}I \neq \pi^{-(k+1)}I$ for all k. As R is noetherian, we can choose n maximal such that $\pi^{-n}I \subseteq R$. If $\pi^{-n}I \neq R$, then $\pi^{-n}I \subseteq \mathfrak{m} = (\pi)$, but then $\pi^{-(n+1)}I \subseteq R$, contradicting the maximality of n, hence $\pi^{-n}I = R$, so $I = (\pi^n)$ is principal. □

Corollary 5.4. *Let R be a Dedekind domain and $\mathfrak{p} \subseteq R$ a non-zero prime ideal. Then $R_{(\mathfrak{p})}$ is a DVR.*

Definition. *If R is a Dedekind domain, $\mathfrak{p} \subseteq R$ a non-zero prime ideal, then we write $v_\mathfrak{p}$ for the normalized valuation on $\operatorname{Frac} R$ corresponding to the DVR $R_{(\mathfrak{p})}$.*

Theorem 5.5. *Let R be a Dedekind domain. Then every non-zero ideal $I \subseteq R$ can be written uniquely as a product of prime ideals $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ ($\mathfrak{p}_i$ distinct,$e_i > 0$).*

Proof. Let $I \subseteq R$ be a non-zero ideal. By Lemma 5.2 there are distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and $\beta_1, \dots, \beta_r > 0$ such that $\mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_r^{\beta_r} \subseteq I$. Let $0 \neq \mathfrak{p}$ be a prime ideal distinct from the $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. Then we have $\mathfrak{p}_i R_{(\mathfrak{p})} = R_{(\mathfrak{p})}$, so $IR_{(\mathfrak{p})} = R_{(\mathfrak{p})}$. Since $R_{(\mathfrak{p}_i)}$ is a DVR we have $IR_{(\mathfrak{p}_i)} = (\mathfrak{p}_i R_{(\mathfrak{p}_i)})^{\alpha_i} = \mathfrak{p}_i^{\alpha_i} R_{(\mathfrak{p}_i)}$. Then $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$ as this holds locally at each prime. For uniqueness, if $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r} = \mathfrak{p}_1^{\gamma_1} \dots \mathfrak{p}_r^{\gamma_r}$, then $\mathfrak{p}_i^{\alpha_i} R_{(\mathfrak{p}_i)} = \mathfrak{p}_i^{\gamma_i} R_{(\mathfrak{p}_i)}$, so $\alpha_i = \gamma_i$ by unique factorization in DVR's. □

5.1 Dedekind domains and extensions

Lemma 5.6. *Let L/K be a finite separable field extension. Then the symmetric bilinear pairing*

$$\begin{aligned} (\ ,\ ) : L \times L &\longrightarrow K \\ (x, y) &\longmapsto \operatorname{Tr}_{L/K}(xy) \end{aligned}$$

is non-degenerate.

Proof. As L/K is separable, we have $L = K(\alpha)$ for some $\alpha \in L$. Consider the matrix A representing $(\ ,\ )$ in the K-basis for L given by $1, \alpha, \dots, \alpha^{n-1}$. Then $A_{ij} = \operatorname{Tr}_{L/K}(\alpha^{i+j}) = BB^T$ where $B = (\sigma_j(\alpha^i))_{ij}$ where the σ_j are the embeddings of L/K into K^{alg}, so $\det A = (\det B)^2$ and $\det B = \prod_{1 \le i < j \le n} (\sigma_j(\alpha) - \sigma_i(\alpha)) \neq 0$. □

Theorem 5.7. *Let $\mathcal{O}_K$ be a Dedekind domain (where $K = \operatorname{Frac} \mathcal{O}_K$) and L a finite separable extension of K. Then the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L is also a Dedekind domain.*

Proof. $\mathcal{O}_L$ is clearly an integrally closed integral domain.

Let $e_1, \dots, e_n \in L$ be a K-basis for L which we may assume to be contained in $\mathcal{O}_L$. Let $f_1, \dots, f_n \in L$ be the dual basis for $e_1, \dots, e_n$ w.r.t. the trace form, i.e. $\operatorname{Tr}_{L/K}(e_i f_j) = \delta_{ij}$.

Let $x \in \mathcal{O}_L$, write $x = \sum_{i=1}^n \lambda_i f_i$ where $\lambda_i \in K$. Then $\lambda_i = \mathrm{Tr}_{L/K}(xe_i) \in \mathcal{O}_K$. Therefore $\mathcal{O}_L \subseteq \sum_{i=1}^n \mathcal{O}_K f_i$. Since $\mathcal{O}_K$ is noetherian, $\mathcal{O}_L$ is finitely generated (as a module) over $\mathcal{O}_K$. Then $\mathcal{O}_L$ is also noetherian.

Let $\mathfrak{q}$ be a non-zero prime ideal in $\mathcal{O}_L$ and let $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Then $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and it is non-zero, since if $0 \neq x \in \mathfrak{q}$, then $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ for some $a_i \in \mathcal{O}_K$ with wlog $a_n \neq 0$, then $a_n \in \mathfrak{p}$. So $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$, hence maximal. We have an integral extension $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{q}$. Since $\mathcal{O}_K/\mathfrak{p}$ is a field, it follows easily that $\mathcal{O}_L/\mathfrak{q}$ is a field, hence $\mathfrak{q}$ is maximal. □

Corollary 5.8. *The ring of integers in a number field is a Dedekind domain.*

Conventions on normalizations: Let $\mathcal{O}_K$ be the ring of integers of a number field K, $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal. We normalize $|\cdot|_\mathfrak{p}$ by $|x|_\mathfrak{p} = N\mathfrak{p}^{-v_\mathfrak{p}(x)}$ where $N\mathfrak{p} = \#\mathcal{O}_K/\mathfrak{p}$.

Now let $\mathcal{O}_K$ be a Dedekind domain with $K = \mathrm{Frac}\,\mathcal{O}_K$. Let L/K be a finite separable extension and $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L.

It is easy to see that for $0 \neq x \in \mathcal{O}_K$ we have $(x) = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_\mathfrak{p}(x)}$.

Theorem 5.9. *For $\mathfrak{p}$ a non-zero prime ideal of $\mathcal{O}_K$, write $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$ with $e_i > 0$. Then the absolute values on L extending $|\cdot|_\mathfrak{p}$ (up to equialence) are precisely $|\cdot|_{P_1}, \dots, |\cdot|_{P_r}$.*

Proof. For any $0 \neq x \in \mathcal{O}_K$ we have $v_{P_i}(x) = e_i v_\mathfrak{p}(x)$. Hence, up to equivalence, $|\cdot|_{P_i}$ extends $|\cdot|_\mathfrak{p}$. Now suppose $|\cdot|$ is an absolute value on L extending $|\cdot|_\mathfrak{p}$. Note that it is bounded on $\mathbb{Z}$, thus non-archimedean. Let $R = \{x \in L \mid |x| \leq 1\} \subseteq L$ be the valuation ring corresponding to $|\cdot|$. Then $\mathcal{O}_K \subseteq R$, and since R is integrally closed in L we have $\mathcal{O}_L \subseteq R$. Set $P = \{x \in \mathcal{O}_L \mid |x| < 1\} = \mathcal{O}_L \cap \mathfrak{m}_R$. P is a prime ideal of $\mathcal{O}_L$. It is non-zero as it contains $\mathfrak{p}$. Then $\mathcal{O}_{L,P} \subseteq R$. By maximality of DVRs we have $\mathcal{O}_{L,P} = R$. From this it follows that $|\cdot|$ is equivalent to $|\cdot|_P$. Since $|\cdot|$ extends $|\cdot|_\mathfrak{p}$, $P \cap \mathcal{O}_K = \mathfrak{p}$. Therefore $P_1^{e_1} \cdots P_r^{e_r} \subseteq P$, so $P = P_i$ for some i. □

Let K be a number field. If $\sigma : K \to \mathbb{R}, \mathbb{C}$ is a real or complex embedding, then $x \mapsto |\sigma(x)|_\infty$ defines an absolute value on K, denoted by $|\cdot|_\sigma$.

Corollary 5.10. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then any absolute value on K is equivalent to either $|\cdot|_\mathfrak{p}$ for some non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ or $|\cdot|_\sigma$ for some embedding $\sigma : K \to \mathbb{R}$ or $\mathbb{C}$.*

Proof. Case $|\cdot|$ is non-archimedean. Then $|\cdot||_\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p. Thus by the Theorem $|\cdot| \sim |\cdot|_\mathfrak{p}$ for some prime $\mathfrak{p} \mid p$.

The archimedean case is an exercise. □

5.2 Completions

Setup as before: $\mathcal{O}_K$ Dedekind domain, L/K finite separable extension. Let $\mathfrak{p} \subseteq \mathcal{O}_K, P \subseteq \mathcal{O}_L$ non-zero prime ideals with $P \mid \mathfrak{p}$. We write $K_\mathfrak{p}$ and L_P for the completion with respect to the $\mathfrak{p}$- resp. P-adic absolute values.

Lemma 5.11.

(i) The natural map $\pi_P : L \otimes_K K_\mathfrak{p} \to L_P$ is surjective.

(ii) $[L_P : K_\mathfrak{p}] \leq [L : K]$.

Proof. (ii) is immediate from (i). Consider $M = LK_\mathfrak{p} = \operatorname{im} \pi_P$. M is complete as it is a finite extension of $K_\mathfrak{p}$ and $L \subseteq M \subseteq L_P$, thus $M = L_P$. $\square$

Theorem 5.12. *The natural map $L \otimes_K K_\mathfrak{p} \to \prod_{P|\mathfrak{p}} L_P$ is an isomorphism.*

Proof. Write $L = K(\alpha)$ and let $f(x) \in K[x]$ be the minimal polynomial of α. Then we have $f(x) = f_1(x) \ldots f_r(x)$ in $K_\mathfrak{p}[x]$ where $f_i \in K_\mathfrak{p}[X]$ are distinct irreducible. Since $L = K[X]/(f(x))$ we have $L \otimes_K K_\mathfrak{p} = K_\mathfrak{p}[X](f(x)) \cong \prod_{i=1}^r K_\mathfrak{p}[x]/(f_i(x))$. Let $L_i = K_\mathfrak{p}[x]/(f_i(x))$. This is a finite extension of $K_\mathfrak{p}$. Then L_i contains both L and $K_\mathfrak{p}$. Moreover, L is dense inside L_i. Indeed, since K is dense in $K_\mathfrak{p}$, we can approximate coefficients of an element of $K_\mathfrak{p}[x]/(f_i(x))$ by an element in $K[x]/f(x) = L$. The theorem will follow from the following three claims:

(1) $L_i \cong L_P$ for some prime P of $\mathcal{O}_L$ dividing $\mathfrak{p}$ (and the isomorphism fixes L and $K_\mathfrak{p}$)

(2) Each P appears at most once.

(3) Each P appears at least once.

Proof:

(1) Since $[L_i : K_\mathfrak{p}] < \infty$, there is a unique absolute value $|\cdot|_{L_i}$ on L_i extending $|\cdot|_\mathfrak{p}$. We must have that $|\cdot|_{L_i}|_L$ is equivalent to $|\cdot|_P$ for some $P \mid \mathfrak{p}$. Since L is dense in L_i and L_i is complete, we have $L_i \cong L_P$.

(2) Suppose $\varphi : L_i \cong L_j$ is an isomorphism preserving L and $K_\mathfrak{p}$, then $\varphi : K_\mathfrak{p}[x]/(f_i(x)) \to K_\mathfrak{p}[x]/(f_j(x))$ takes x to x and hence $f_i = f_j$, i.e. $i = j$.

(3) By the previous lemma the map $\pi_P : L \otimes_K K_\mathfrak{p} \to L_P$ is surjective for every $P \mid \mathfrak{p}$. Since L_P is a field, π_P factors through L_i for some i and we have $L_i \cong L_P$ by surjectivity. $\square$

Corollary 5.13. *For $x \in L$,*

$$N_{L/K}(x) = \prod_{P|\mathfrak{p}} N_{L_P/K_\mathfrak{p}}(x),$$

$$\mathrm{Tr}_{L/K}(x) = \sum_{P|\mathfrak{p}} \mathrm{Tr}_{L_P/K_\mathfrak{p}}(x).$$

5.3 Decomposition groups

Let $0 \neq \mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Let $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \dots P_r^{e_r}$ where the P_i are distinct prime ideals in $\mathcal{O}_L$, $e_i > 0$.

e_i is called the *ramification index* of P_i over $\mathfrak{p}$. $f_i := [\mathcal{O}_L/P_i : \mathcal{O}_K/\mathfrak{p}]$ is called the *residue class degree* of P_i over $\mathfrak{p}$.

Theorem 5.14. $\sum_{i=1}^r e_i f_i = [L : K]$

Proof. Let $S = \mathcal{O}_K \backslash \mathfrak{p}$. We note that $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K$ in L. Furthermore $\mathfrak{p}S^{-1}\mathcal{O}_L = S^{-1}P_1^{e_1} \dots P_r^{e_r}$ and $S^{-1}\mathcal{O}_L/S^{-1}P_i \cong \mathcal{O}_L/P_i$ and $S^{-1}\mathcal{O}_K/S^{-1}\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$. Thus, we may assume that $\mathcal{O}_K$ is a DVR. By CRT, we have $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^r \mathcal{O}_L/P_i^{e_i}$. We count dimensions of both sides as $k = \mathcal{O}_K/\mathfrak{p}$ vector spaces. For each i we have an increasing sequence of k-subspaces:

$$0 \subseteq P_i^{e_i-1}/P_i^{e_i} \subseteq \dots \subseteq P_i/P_i^{e_i} \subseteq \mathcal{O}_L/P_i^{e_i}$$

Note that P_i^j/P_i^{j+1} is an $\mathcal{O}_L/P_i$-module and $x \in P_i^j \setminus P_i^{j+1}$ is a generator. (E.g. can prove this after localization at P_i). So $\dim_k P_i^j/P_i^{j+1} = f_i$ and we have $\dim_k \mathcal{O}_L/P_i^{e_i} = e_i f_i$. $\mathcal{O}_L$ has rank $[L : K]$ over $\mathcal{O}_K$, so $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ has dimension $[L : K]$ over k. □

Now assume that L/K is Galois. Then for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(P_i) \cap \mathcal{O}_K = \mathfrak{p}$ and hence $\sigma(P_i) \in \{P_1, \dots, P_r\}$.

Proposition 5.15. *The action of* $\mathrm{Gal}(L/K)$ *on* $\{P_1, \dots, P_r\}$ *is transitive.*

Proof. Suppose not, then there are $i \neq j$ such that $\sigma(P_i) \neq P_j$ for all $\sigma \in \mathrm{Gal}(L/K)$. There is $x \in \mathcal{O}_L$ such that $x \equiv 0 \pmod{P_j}, x \equiv 1 \pmod{\sigma(P_i)}$ for all $\sigma \in \mathrm{Gal}(L/K)$. We have $N_{L/K}(x) = \prod_\sigma \sigma(x) \in \mathcal{O}_K \cap P_j = \mathfrak{p} \subseteq P_i$, so $\sigma(x) \in P_i$ for some σ, i.e. $x \in \sigma^{-1}(P_i)$, a contradiction. □

Corollary 5.16. *Suppose L/K is Galois. Then $e := e_1 = \dots = e_r$ and $f := f_1 = f_2 = \dots = f_r$ and we have $n = efr$.*

Proof. For any $\sigma \in \mathrm{Gal}(L/K)$ we have $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_r)^{e_r}$. By uniqueness of prime ideal factorization we get $e_1 = \dots = e_r$. Furthermore $\mathcal{O}_L/P_i \cong \mathcal{O}_L/\sigma(P_i)$ via σ, so $f_1 = \dots = f_r$. □

If L/K is an extension of complete discretely valued fields with normalized valuation v_L, v_K, and uniformizers π_L, π_K, we have $e := e_{L/K} = v_L(\pi_K)$ (i.e. $\pi_K\mathcal{O}_K = \pi_L^e\mathcal{O}_L$) and $f := f_{L/K} = [k_L : k]$.

Corollary 5.17. *Let L/K be a finite separable extension of complete fields, then $[L : K] = ef$.*

Remark: The corollary holds without assumption L/K separable (since in the case of complete fields, $\mathcal{O}_L$ is automatically finite over $\mathcal{O}_K$).

Definition. *Let $\mathcal{O}_K$ be a Dedekind domain. Let L/K be a finite Galois extension. The* decomposition group *at a prime P of $\mathcal{O}_L$ is the subgroup of* $\mathrm{Gal}(L/K)$ *is defined by*

$$G_P = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(P) = P\}.$$

Note that any two decomposition groups of primes lying over the same prime in K are conjugate.

Proposition 5.18. *Suppose L/K is Galois and $P \mid \mathfrak{p}$. Then*

(i) $L_P/K_\mathfrak{p}$ is Galois

(ii) There is a natural map $\mathrm{res} : \mathrm{Gal}(L_P/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$ *which is injective and has image G_P.*

Proof. (i) L/K is Galois, so L is the splitting field of a separable polynomial $f(x) \in K[x]$. Then $L_P/K_\mathfrak{p}$ is the splitting field of $f(x) \in K_\mathfrak{p}[x]$, so $L_P/K_\mathfrak{p}$ is Galois.

(ii) Let $\sigma \in \mathrm{Gal}(L_P/K_\mathfrak{p})$. Then $\sigma(L) = L$ since L/K is normal, hence we get a map $\mathrm{res} : \mathrm{Gal}(L_P/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$. Since L is dense in L_P, res is injective. We know that $|\sigma x|_P = |x|_P$ for all $\sigma \in \mathrm{Gal}(L_P/K_\mathfrak{p})$ and $x \in L_P$, hence $\sigma(P) = P$ for all $\sigma \in \mathrm{Gal}(L_P/K_P)$, i.e. $\mathrm{res}(\sigma) \in G_P$. To show that the image is all of G_P, it suffices to show that $\#G_P = fe = \#\mathrm{Gal}(L_P/K_\mathfrak{p}) = [L_P : K_\mathfrak{p}]$[1]. The first equality is immediate from $efr = n$ and the transitivity of the action of $\mathrm{Gal}(L/K)$ on the primes above $\mathfrak{p}$. The equality $[L_P : K_\mathfrak{p}] = ef$ follows from Corollary 5.17 and the fact that e and f don't change when we take completions. □

[1]Alternativley, one can directly see that the map is surjective: If $\sigma \in G_P$, then σ is continuous for the P-adic absolute value, hence extends to $L_P/K_\mathfrak{p}$.

6 Ramification Theory

6.1 Different and discriminant

Let L/K be an extension of algebraic number fields, $n = [L : K]$. Let $x_1, \dots, x_n \in L$. We set

$$\Delta(x_1, \dots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j))_{ij} = \det(\sigma_i(x_j))^2 \in K$$

where $\sigma_i : L \to K^{\mathrm{alg}}$ are the distinct embeddings. Note: If $y_i = \sum_{j=1}^n a_{ij} x_j$ where $a_{ij} \in K$, then $\Delta(y_1, \dots, y_n) = \det(A)^2 \Delta(x_1, \dots, x_n)$ where $A = (a_{ij})$. If $x_1, \dots, x_n \in \mathcal{O}_L$, then $\Delta(x_1, \dots, x_n) \in \mathcal{O}_K$.

Lemma 6.1. *Let k be a perfect field, R a finite-dimensional k-algebra. The trace form $(\ ,\ ) : R \times R \to K, (x, y) = \mathrm{Tr}_{R/k}(xy)$ is non-degenerate iff $R \cong k_1 \times \cdots \times k_m$ where $k_1, \dots, k_m$ are finite field extensions of k.*

Proof. Exercise on Sheet 3. □

Theorem 6.2. *Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal.*

(i) If $\mathfrak{p}$ ramifies in L, then for every $x_1, \dots, x_n \in \mathcal{O}_L$ we have $\mathfrak{p} \mid \Delta(x_1, \dots, x_n)$.

(ii) If $\mathfrak{p}$ is unramified, then there are $x_1, \dots, x_n \in \mathcal{O}_L$ such that $\mathfrak{p} \nmid \Delta(x_1, \dots, x_n)$.

Proof. Let $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \dots P_r^{e_r}$, where the P_i are distinct and $e_i > 0$. Then $R := \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^r \mathcal{O}_L/P_i^{e_i}$. If $\mathfrak{p}$ ramifies, then $e_i > 1$ for some i, i.e. R is nilpotent elements, so it cannot be the product of field extensions of $k = \mathcal{O}_K/\mathfrak{p}$. By the previous lemma the trace form $\mathrm{Tr}_{R/k}$ is degenerate. So $\Delta(\bar{x}_1, \dots, \bar{x}_n) = 0$ for all $\bar{x}_i \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. This proves (i). The argument for (ii) is the same. □

Definition. *The* discriminant of L/K *is the ideal $d_{L/K} \leq \mathcal{O}_K$ generated by $\Delta(x_1, \dots, x_n)$ for all choices of $x_1, \dots, x_n \in \mathcal{O}_L$.*

Corollary 6.3. *$\mathfrak{p}$ ramifies in L iff $\mathfrak{p} \mid d_{L/K}$*

Definition. *The* inverse different *is the fractional ideal*

$$D_{L/K}^{-1} := \{y \in L \mid \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K \, \forall x \in \mathcal{O}_L\}.$$

This is an $\mathcal{O}_L$-submodule of L containing $\mathcal{O}_L$.

Lemma 6.4. *$D_{L/K}^{-1}$ is a fractional ideal of $\mathcal{O}_L$.*

Proof. Let $x_1, \dots, x_n \in \mathcal{O}_L$ be a basis for L as a K-vector space. Set $d := \Delta(x_1, \dots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)) \in \mathcal{O}_K$. For $x \in D_{L/K}^{-1}$ write $x = \sum_{j=1}^n \lambda_j x_j$ with $\lambda_j \in K$. Then $\mathrm{Tr}_{L/K}(x x_i) = \sum_{j=1}^n \lambda_j \mathrm{Tr}_{L/K}(x_i x_j)$. Then multiplying with the adjugate matrix we get $d\lambda_j \in \mathcal{O}_K$ for all j, so $dD_{L/K}^{-1} \subseteq \mathcal{O}_L$. □

Definition. *The inverse of $D_{L/K}^{-1}$, denoted $D_{L/K} \subseteq \mathcal{O}_L$, is the* different ideal.

Let I_L, I_K be the groups of fractional ideals in L, K resp. Define $N_{L/K} : I_L \to I_K$ on prime ideals P by $P \mapsto (P \cap \mathcal{O}_K)^{f(P|(P\cap\mathcal{O}_K))}$ and extend multiplicatively.

Fact: $N_{L/K}(a\mathcal{O}_L) = N_{L/K}(a)\mathcal{O}_K$. To see this, use $v_\mathfrak{p}(N_{L_P/K_\mathfrak{p}}(x)) = f_{P/\mathfrak{p}} v_P(x)$ for $x \in L_P^\times$.

Theorem 6.5. $N_{L/K}(D_{L/K}) = d_{L/K}$

Proof. First assume that $\mathcal{O}_K$, $\mathcal{O}_L$ are PID's. Let $x_1, \dots, x_n$ be an $\mathcal{O}_K$-basis for $\mathcal{O}_L$ and $y_1, \dots, y_n$ be the dual basis with respect to the trace form. Then $y_1, \dots, y_n$ form a basis for $D_{L/K}^{-1}$. Let $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ be the distinct embeddings. Then $\sum_{i=1}^n \sigma_i(x_j)\sigma_i(y_k) = \mathrm{Tr}_{L/K}(x_j y_k) = \delta_{j,k}$. But $\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$, so $\Delta(x_1, \dots, x_n)\Delta(y_1, \dots, y_n) = 1$. Write $D_{L/K}^{-1} = \beta\mathcal{O}_L$ with some $\beta \in L$. Then $d_{L/K}^{-1} = \Delta(x_1, \dots, x_n)^{-1} = \Delta(y_1, \dots, y_n) = \Delta(\beta x_1, \dots, \beta x_n) = N_{L/K}(\beta)^2 \Delta(x_1, \dots, x_n) = N_{L/K}(\beta)^2 d_{L/K}$. Then $d_{L/K}^{-1} = N_{L/K}(\beta) = N_{L/K}(D_{L/K}^{-1})$. In general, localize at $S = \mathcal{O}_K \setminus \mathfrak{p}$ and use $S^{-1}D_{L/K} = D_{S^{-1}\mathcal{O}_K/S^{-1}\mathcal{O}_L}$ and same for the discriminant. □

Theorem 6.6. *If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and α has monic minimal polynomial $g(x) \in \mathcal{O}_K[x]$, then $D_{L/K} = (g'(\alpha))$.*

Proof. Let $\alpha = \alpha_1, \dots, \alpha_n$ be the roots of g. Write $\frac{g(x)}{x-\alpha} = \beta_{n-1}x^{n-1} + \beta_{n-2}x^{n-2} + \dots + \beta_0$ with $\beta_i \in \mathcal{O}_L$ and $\beta_{n-1} = 1$. We claim that

$$\sum_{i=1}^n \frac{g(x)}{x - \alpha_i} \cdot \frac{\alpha_i^r}{g'(\alpha_i)} = x^r$$

for $0 \le r \le n-1$. Indeed, the difference is a polynomial of degree $< n$ which vanishes at $\alpha_1, \dots, \alpha_n$.

Equating coefficients of X^s gives $\mathrm{Tr}_{L/K}(\frac{\alpha^r \beta_s}{g'(\alpha)}) = \delta_{rs}$. So the dual basis (and hence the $\mathcal{O}_K$-basis of $D_{L/K}^{-1}$) of $1, \alpha, \dots, \alpha^{n-1}$ is $\frac{\beta_0}{g'(\alpha)}, \dots, \frac{\beta_{n-1}}{g'(\alpha)} = \frac{1}{g'(\alpha)}$. So $D_{L/K}^{-1}$ is generated as a fractional ideal by $\frac{1}{g'(\alpha)}$. □

P prime of $\mathcal{O}_L$, $\mathfrak{p} = P \cap \mathcal{O}_K$. We identify $D_{L_P/K_\mathfrak{p}}$ with a power of P.

Theorem 6.7. $D_{L/K} = \prod_P D_{L_P/K_\mathfrak{p}}$.

Proof. Let $x \in L$, $\mathfrak{p} \subseteq \mathcal{O}_K$ prime. Then $(*)$ $\mathrm{Tr}_{L/K}(x) = \sum_{P|\mathfrak{p}} \mathrm{Tr}_{L_P/K_\mathfrak{p}}(x)$. Let $r(P) = v_P(D_{L/K})$, $s(P) = v_P(D_{L_P/K_\mathfrak{p}})$.

"$\subseteq$" (i.e. $r(P) \geq s(P)$). Fix P and let $x \in P^{-s(P)} \setminus P^{-s(P)+1}$. Then $v_P(x) = -s(P)$ and $v_{P'}(x) \geq 0 \geq -s(P)$ for all $P' \neq P$. Then $\mathrm{Tr}_{L_{P'}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_L$ and for all P'. So by $(*)$ $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_L$ and for all $\mathfrak{p}$, so $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K$ for all $y \in \mathcal{O}_L$, i.e. $x \in D_{L/K}^{-1}$. So $-s(P) = v_P(x) \geq -r(P)$.

"$\supseteq$" (i.e $r(P) \leq s(P)$). Fix P and let $x \in P^{-r(P)} \setminus P^{-r(P)+1}$. Then $v_P(x) = -r(P)$ and $v_{P'}(x) \geq 0$ for all $P' \neq P$. By $(*)$ we have

$$\mathrm{Tr}_{L_P/K_\mathfrak{p}}(xy) = \mathrm{Tr}_{L/K}(xy) - \sum_{P'|\mathfrak{p}, P' \neq P} \mathrm{Tr}_{L_{P'}/K_\mathfrak{p}}(xy)$$

for all $y \in \mathcal{O}_L$. By continuity $\mathrm{Tr}_{L_P/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_{L_P}$, so $x \in D_{L_P/K_\mathfrak{p}}^{-1}$, i.e. $-v_P(x) = r(P) \leq s(P)$. □

Corollary 6.8. $d_{L/K} = \prod_P d_{L_P/K_\mathfrak{p}}$.

6.2 Unramified and totally ramified extensions of local fields

Let L/K be a finite separable extension of non-archimedean local fields.

Definition. *L/K is* unramified *(resp.* ramified*,* fully ramified*) if $e_{L/K} = 1$ (resp. $e_{L/K} > 1$, $e_{L/K} = [L : K]$).*

Lemma 6.9. *Let $M/L/K$ be finite extensions of local fields. Then $f_{M/K} = f_{M/L} f_{L/K}$, $e_{M/K} = e_{M/L} e_{L/K}$.*

Proof. Clear from the definitions. □

Theorem 6.10. *There exists a field K_0 with $K \subseteq K_0 \subseteq L$ such that*

i) K_0/K is unramified.

ii) L/K_0 is totally ramified.

Moreover $[K_0 : K] = f_{L/K}, [L : K_0] = e_{L/K}$ and K_0/K is Galois.

Proof. Let $k = \mathbb{F}_q$, so that $k_L = \mathbb{F}_{q^f}$, $f = f_{L/K}$. Set $m = q^f - 1$. Let $[\cdot] : \mathbb{F}_{q^f} \to L$ be the Teichmüller lift for L. Let $\xi_m = [\alpha]$, for α a generator of $\mathbb{F}_{q^f}^\times$. Then ξ_m is a primitive m-th root of unity. Set $K_0 = K(\xi_m)$. This is Galois as it is the splitting field of $x^m - 1$. Let res : $\mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_0/K)$ be the natural map. For $\sigma \in \mathrm{Gal}(K_0/K)$, we have $\sigma(\xi_m) = \xi_m$ if $\sigma(\xi_m) \equiv \xi_m \bmod \mathfrak{m}_0$, since $\mathcal{O}_{K_0}^\times \to k_0^\times$ induces a bijection between the m-th roots of unity. Hence res is injective. So $f_{K_0/K} \leq \#\,\mathrm{Gal}(K_0/K) \leq \#\,\mathrm{Gal}(k_0/k) = f_{K_0/K}$, so we get $[K_0 : K] = f_{K_0/K} = f$ and $e_{K_0/K} = 1$ and res is an isomorphism. By multiplicativity of residue class/ramification degrees, we get $f_{L/K_0} = 1$ and $e_{L/K_0} = e_{L/K} = [L:K]/[K_0 : K] = [L : K_0]$. □

Theorem 6.11. $k = \mathbb{F}_q$. *For any* $n \geq 1$ *there exists a unique unramified extension* L/K *of degree* n*. Moreover,* L/K *is Galois and the natural restriction map* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ *is an isomorphism. In particular,* $\mathrm{Gal}(L/K) = \langle \mathrm{Frob}_{L/K} \rangle$ *where* $\mathrm{Frob}_{L/K}(x) \equiv x^q \mod \mathfrak{m}_L$ *for all* $x \in \mathcal{O}_L$*.*

Proof. For $n \geq 1$, take $L = K(\zeta_m)$, where $m = q^n - 1$ and ζ_m is a primitive m-root of unity. As in the theorem $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is an isomorphism. Therefore L/K is unramified. Then L/K is unramified and $\mathrm{Gal}(L/K)$ is generated by a lift of $x \mapsto x^q$.[1] Uniqueness: If L/K is degree n and unramified, then $\zeta_m \in L$ by Hensel's Lemma or Teichmüller lift and thus $L = K(\zeta_m)$ for degree reasons. □

Corollary 6.12. L/K *is finite Galois. The map* $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/K)$ *is surjective.*

Proof. res factors as $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K_0/K) \xrightarrow{\simeq} \mathrm{Gal}(k_L/k)$. □

Definition. L/K *finite Galois. The* inertia subgroup *is*

$$I_{L/K} := \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)).$$

Since $e_{L/K} f_{L/K} = [L : K]$, we have $\# I_{L/K} = e_{L/K}$. Also $I_{L/K} = \mathrm{Gal}(L/K_0)$.

Theorem 6.13.

(i) Let L/K *be finite totally ramified,* $\pi_L \in \mathcal{O}_L$ *a uniformizer. Then the minimal polynomial of* π_L *is Eisenstein,* $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ *and* $L = K(\pi_L)$*.*

(ii) Conversely, if $f(x) \in \mathcal{O}_K[x]$ *is Eisenstein and* α *is a root of* f*, then* $L = K(\alpha)$ *is a totally ramified extension of* K *and* α *is a uniformizer in* L*.*

Proof.

(i) Let $e = [L : K]$ and $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathcal{O}_K[x]$ be the minimal polynomial of π_L. Then $m \leq e$. Since $v_L(K^\times) = e\mathbb{Z}$, we have $v_L(a_i \pi_L^i) \equiv i \mod e$ for $i < m$, hence these terms have distinct valuations. As $\pi_L^m = -\sum_{i=0}^{m-1} a_i \pi_L^i$ we have $m = v_L(\pi_L^m) = \min_{0 \leq i \leq m-1}(i + e v_k(a_i))$. But this can only happen if $e = m$, $v_K(a_i) \geq 1$ for all i and $v_K(a_0) = 1$. So f is Eisenstein and $L = K(\pi_L)$. For $y \in L$ write $y = \sum_{i=0}^{e} b_i \pi_L^i$, $b_i \in K$. Then $v_L(y) = \min_{0 \leq i \leq e-1}(i + e v_K(b_i))$. Thus $y \in \mathcal{O}_L$ iff $v_L(y) \geq 0$ iff $v_K(b_i) \geq 0$ iff $y \in \mathcal{O}_K[\pi_L]$.

[1] To get the inequality $[L : K] \leq n$ take the minimal polynomial of ζ_m and show that it is irreducible over k.

(ii) Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$ be Eisenstein, and let $e := e_{L/K}$ where $L = K(\alpha)$. Thus $v_L(a_i) \geq e$ and $v_L(a_0) = e$. If $v_L(\alpha) \leq 0$, we have $nv_L(\alpha) < v_L(a_{n-1}\alpha^{n-1} + \cdots + a_0)$, contradiction. So $v_L(\alpha) > 0$. Then for $i \neq 0$, $v_L(a_i\alpha^i) > e = v_L(a_0)$. Therefore $nv_L(\alpha) = v_L(\alpha^n) = v_L(-\sum_{i=0}^{n-1} a_i\alpha^i) = e$.

□

6.3 Structure of Units

Let K be a finite extension of $\mathbb{Q}_p$, let $e := e_{K/\mathbb{Q}}$, π uniformizer in K.

Proposition 6.14. *If $r > e/(p-1)$, then*

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

converges on $\pi^r\mathcal{O}_K$ and induces an isomorphism $(\pi^r\mathcal{O}_K, +) \cong (1 + \pi^r\mathcal{O}_K, \times)$.

Proof. $v_K(n!) = ev_p(n!) = e\frac{n-s_p(n)}{p-1} \leq e\frac{n-1}{p-1}$, so for $x \in \pi^r\mathcal{O}_K$ and $n \geq 1$ we have

$$v_K(x^n/n!) \geq nr - e\frac{n-1}{p-1} = r + (n-1)\underbrace{(r - \frac{e}{p-1})}_{>0}.$$

So $v_K(x^n/n!) \to \infty$ as $n \to \infty$, so $\exp(x)$ converges. Since $v_K(x^n/n!) \geq r$ for $n \geq 1$, $\exp(x) \in 1 + \pi^r\mathcal{O}_K$.

Similarly consider $\log : 1+\pi^r\mathcal{O}_K \to \pi^r\mathcal{O}_K$ where $\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}x^n$. Note that $v_K(x^n/n) = rn - ev_p(n) \geq rn - e\frac{n-1}{p-1} = (n-1)(r - \frac{e}{p-1}) + r$, so the series converges and also $v(\log(1+x)) \geq r$, so log maps $1 + \pi^r\mathcal{O}_K$ into $\pi^r\mathcal{O}_K$.

The identities $\exp(X+Y) = \exp(X)\exp(Y), \exp(\log(1+X)) = 1+X, \log(\exp(X)) = X$ hold in $\mathbb{Q}[\![X, Y]\!]$. So $\exp : (\pi^r\mathcal{O}_K, +) \to (1 + \pi^r\mathcal{O}_K, \times)$ is an isomorphism. □

For K a local field we let $U_K = \mathcal{O}_K^\times$.

Definition. *For $s \in \mathbb{Z}_{\geq 1}$, the s-th unit group $U_K^{(s)}$ is defined by $U_K^{(s)} = (1 + \pi^s\mathcal{O}_K, \times)$. We set $U_K^{(0)} = U_K$.*

We have $\ldots \subseteq U_K^{(s)} \subseteq U_K^{(s-1)} \subseteq \ldots \subseteq U_K^{(0)} = U_K$.

Proposition 6.15.

(i) $U_K^{(0)}/U_K^{(1)} \cong (k^\times, \times)$

(ii) $U_K^{(s)}/U_K^{(s+1)} \cong (k, +)$ *for* $s \geq 1$.

Proof. For (i) note that the reduction map $\mathcal{O}_K^\times \to k^\times$ is surjective with kernel $1 + \pi\mathcal{O}_K = U_K^{(1)}$.

For (ii) let $f : U_K^{(s)} \to k$ be defined by $1 + \pi^s x \mapsto x \bmod \pi$. This is a surjective group homomorphism with kernel $U_K^{(s+1)}$. □

Corollary 6.16. *Let $[K : \mathbb{Q}_p] < \infty$. There exists a finite index subgroup of $\mathcal{O}_K^\times$ isomorphic to $(\mathcal{O}_K, +)$.*

Proof. Let $r > \frac{e}{p-1}$. Then $U_K^{(r)} \cong (\mathcal{O}_K, +)$ by the first proposition and $U_k^{(r)} \subseteq U_K$ has finite index. □

Remark: This is not true for K equal characteristic.

Example. Consider $\mathbb{Z}_p$ for $p > 2$. Then $e = 1$, so that we can take $r = 1$. Then using the Teichmüller lift we get

$$\mathbb{Z}_p^\times \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

For $p = 2$ take $r = 2$, then $\mathbb{Z}_2^\times \xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + 4\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

6.4 Higher ramification groups

Let L/K be a finite Galois extension of local fields, $\pi_L \in \mathcal{O}_L$ a uniformizer, v_L the normalized valuation on L.

Definition. *For $s \in \mathbb{R}_{\geq -1}$, the* s-th ramification group *is*

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

E.g. $G_{-1}(L/K) = \operatorname{Gal}(L/K)$ and $G_0(L/K) = \{\sigma \in \operatorname{Gal}(L/K) \mid \sigma(x) \equiv x \bmod \pi \text{ for all } x \in \mathcal{O}_L\} = \ker(\operatorname{Gal}(L/K) \to \operatorname{Gal}(k_L/k)) = I_{L/K}$.

Note: For $s \in \mathbb{Z}_{\geq 0}$, $G_s(L/K) = \ker(\operatorname{Gal}(L/K) \to \operatorname{Aut}(\mathcal{O}_L/\pi_L^{s+1}\mathcal{O}_L))$, hence $G_s(L/K)$ is a normal subgroup of $\operatorname{Gal}(L/K)$.

We get a filtration $\ldots \subseteq G_s \subseteq G_{s-1} \subseteq \ldots \subseteq G_{-1} = \operatorname{Gal}(L/K)$.

Remark: G_s can only change at integer values of s. The indexing using real numbers is used to define the *upper numbering* (see Chapter 9).

Theorem 6.17.

(i) For $s \geq 0$, $G_s = \{\sigma \in G_0 \mid v_L(\sigma(\pi_L) - \pi_L) \geq s + 1\}$.

(ii) $\bigcap_{s=0}^\infty G_s = \{1\}$.

(iii) Let $s \in \mathbb{Z}_{\geq 0}$. There is an injective group homomorphism $G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$ induced by $\sigma \mapsto \sigma(\pi_L)/\pi_L$. This map is independent of the choice of π_L.

Proof. Let $K_0 \subseteq L$ be the maximal unramified extension of K in L. Upon replacing K by K_0 we may assume that L/K totally ramified.

(i) We know that $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. From this it follows that if $v_L(\sigma(\pi_L) - \pi_L) \geq s+1$, then $v_L(\sigma(x) - x) \geq s+1$ for all $x \in \mathcal{O}_L$. Indeed, if $x = f(\pi_L)$ with $f \in \mathcal{O}_K[x]$, then $\sigma(x) - x = f(\sigma(\pi_L)) - f(\pi_L) = (\sigma(\pi_L) - \pi_L)g(\pi_L)$ for some polynomial $g \in \mathcal{O}_L[x]$. Then $v_L(\sigma(x) - x) \geq v_L(\sigma(\pi_L) - \pi_L) \geq s+1$.

(ii) Suppose $\sigma \in \mathrm{Gal}(L/K), \sigma \neq 1$. Then $\sigma(\pi_L) \neq \pi_L$ as $L = K(\pi_L)$. Hence $v_L(\sigma(\pi_L) - \pi_L) < \infty$, so $\sigma \notin G_s$ for some $s > 0$.

(iii) Note: For $\sigma \in G_s, s \in \mathbb{Z}_{\geq 0}$ we have $\sigma(\pi_L) \in \pi_L + \pi_L^{s+1}\mathcal{O}_L$, so $\sigma(\pi_L)/\pi_L \in 1 + \pi_L^s\mathcal{O}_L = U_L^{(s)}$. We claim $\varphi : G_s \to U_L^{(s)}/U_L^{(s+1)}$, $\sigma \mapsto \sigma(\pi_L)/\pi_L$ is a group homomorphism with kernel G_{s+1}. For $\sigma, \tau \in G_s$, let $\tau(\pi_L) = u\pi_L$, $u \in \mathcal{O}_L^\times$, then $(\sigma\tau)(\pi_L)/\pi_L = \sigma(\tau(\pi_L))/\tau(\pi_L) \cdot \tau(\pi_L)/\pi_L = \frac{\sigma(u)}{u}\frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L}$. But $\sigma(u) \in u + \pi_L^{s+1}\mathcal{O}_L$, so $\frac{\sigma(u)}{u} \in 1 + \pi_L^{s+1}\mathcal{O}_L = U_L^{(s+1)}$. So φ is a homomorphism. Moreover $\ker\varphi = \{\sigma \in G_s \mid \sigma\pi_L \equiv \pi_L \bmod \pi_L^{s+1}\} = G_{s+1}$.

□

Corollary 6.18. *Let L/K be a finite Galois extension of local fields. Then* $\mathrm{Gal}(L/K)$ *is solvable.*

Proof. For $s \in \mathbb{Z}_{\geq -1}$ we have $G_s/G_{s+1} \cong$ a subgroup of $\mathrm{Gal}(k_L/k)$ if $s = -1$, $(k_L^\times, \times)$ if $s = 0$ or $(k_L, +)$ if $s \geq 1$. This gives us a filtration of $\mathrm{Gal}(L/K)$ with abelian quotients ending at 1. □

Let $p = \operatorname{char} k$. Then $\#(G_0/G_1)$ is coprime to p and $\#G_1 = p^n$ for some $n \geq 0$. Thus G_1 is the unique (since normal) Sylow p subgroup of $G_0 = I_{L/K}$.

Definition. *The group G_1 is the* wild inertia group *and G_0/G_1 is the* tame quotient. *Let L/K be a finite separable extension of local fields. Say L/K is* tamely ramified *if* $\operatorname{char} k \nmid e_{L/K}$ *(equivalently $G_1 = 1$ if L/K is Galois). Otherwise L/K is* wildly ramified.

Theorem 6.19. *Let $[K : \mathbb{Q}_p] < \infty$, L/K finite, $D_{L/K} = (\pi_L)^{\delta(L/K)}$. Then $\delta(L/K) \geq e_{L/K} - 1$, with equality iff L/K is tamely ramified.*

In particular, L/K is unramified iff $D_{L/K} = \mathcal{O}_L$.

Proof. By Exercise Sheet 3 we have $D_{L/K} = D_{L/K_0}D_{K_0/K}$. So it suffices to check two cases.

(i) L/K unramified. Then $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$ with $k_L = k(\overline{\alpha})$. Let $g(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α. Since $[L:K] = [k_L:k]$, $\overline{g}(x) \in k[x]$ is the minimal polynomial of $\overline{\alpha}$. So $\overline{g}(x)$ is separable and hence $g'(\alpha) \not\equiv 0 \bmod \pi_L$. Thus $D_{L/K} = (g'(\alpha)) = \mathcal{O}_L$.

(ii) L/K totally ramified. Then $[L:K] = e$ and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ where π_L is the root of some Eisenstein polynomial $g(x) = x^e + \sum_{i=0}^{e-1} a_i x^i \in \mathcal{O}_K[x]$. Then $g'(\pi_L) = e\pi_L^{e-1} + \sum_{i=1}^{e-1} i a_i \pi_L^{i-1}$. Then $v_L(g'(\pi_L)) \geq e-1$ with equality iff $p \nmid e$.

□

Corollary 6.20. *Let L/K be an extension of number fields, $P \subseteq \mathcal{O}_L$, $P \cap \mathcal{O}_K = \mathfrak{p}$. Then $e(P \mid \mathfrak{p}) > 1$ iff $P \mid D_{L/K}$.*

Proof. Combine the theorem with the fact that the global different is the product of the local differents. □

Example. Let $K = \mathbb{Q}_p$, ξ_{p^n} a primitive p^n-th root of unity and $L = \mathbb{Q}_p(\xi_{p^n})$. Then the p^n-th cyclotomic polynomial is $\Phi_{p^n}(x) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + 1 \in \mathbb{Z}_p[x]$.

Example Sheet 3: $\Phi_{p^n}(x)$ is irreducible, so $\Phi_{p^n}(x)$ is the minimal polynomial of ξ_{p^n}. $L/\mathbb{Q}_p$ is Galois, totally ramified, degree $p^{n-1}(p-1)$.

Let $\pi = \xi_{p^n} - 1$. This is a uniformizer of $\mathcal{O}_L$. Then $\mathcal{O}_L = \mathbb{Z}_p[\xi_{p^n} - 1] = \mathbb{Z}_p[\xi_{p^n}]$. Then $\mathrm{Gal}(L/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. Let σ_m be the Galois automorphism with $\sigma_m(\xi_{p^n}) = \xi_{p^n}^m$. Then $v_L(\sigma_m(\pi) - \pi) = v_L(\xi_{p^n}^m - \xi_{p^n}) = v_L(\xi_{p^n}^{m-1} - 1)$. Suppose $m \not\equiv 1 \bmod p^n$. Let k be maximal such that $p^k \mid m-1$. Then $\xi_{p^n}^{m-1}$ is a primitive p^{n-k}-th root of unity and hence $\xi_{p^n}^{m-1} - 1$ is a uniformizer in $L' = \mathbb{Q}_p(\xi_{p^n}^{m-1})$. So $v_L(\xi_{p^n}^{m-1} - 1) = e_{L/L'} = e_{L/\mathbb{Q}_p}/e_{L'/\mathbb{Q}_p} = [L:\mathbb{Q}_p]/[L':\mathbb{Q}_p] = p^k$. So $\sigma_m \in G_i$ iff $p^k \geq i+1$. Thus

$$G_i \cong \begin{cases} (\mathbb{Z}/p^n\mathbb{Z})^\times & i \leq 0, \\ (1+p^k\mathbb{Z})/p^n\mathbb{Z} & p^{k-1} - 1 < i \leq p^k - 1, 1 \leq k \leq n-1, \\ \{1\} & p^{n-1} - 1 < i. \end{cases}$$

7 Local Class Field Theory

Recall some infinite Galois theory:

Proposition 7.1. *Let L/K be a Galois extension. The restriction maps* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ *for finite subextensions F/K induce an isomorphism*

$$\mathrm{Gal}(L/K) \xrightarrow{\simeq} \varprojlim_{F/K \text{ finite}} \mathrm{Gal}(F/K).$$

We give $\mathrm{Gal}(L/K)$ the topology for which the above isomorphism becomes a homeomorphism.

Example. $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q) \simeq \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$. Under this isomorphism the Frobenius $\mathrm{Fr}_q \in \mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$ corresponds to $1 \in \widehat{\mathbb{Z}}$.

Theorem 7.2 (Fundamental theorem of Galois theory)**.** *Let L/K be a Galois extension. Endow* $\mathrm{Gal}(L/K)$ *with the profinite topology. Then there is a bijection:*

$$\begin{aligned} \{\textit{subextensions of } L/K\} &\longleftrightarrow \{\textit{closed subgroups of } \mathrm{Gal}(L/K)\} \\ F &\longmapsto \mathrm{Gal}(L/F) \\ L^H &\longleftarrow\!\shortmid H \end{aligned}$$

Moreover, F/K is finite iff $\mathrm{Gal}(L/F)$ *is open and F/K Galois iff* $\mathrm{Gal}(L/F)$ *is normal in* $\mathrm{Gal}(L/K)$ *in which case* $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.

7.1 Weil Group

Let K be a local field, L/K a separable algebraic extension.

Definition.

(i) L/K is unramified *if F/K is unramified for all finite subextensions F/K.*

(ii) L/K is totally ramified *if F/K is totally ramified for all finite subextensions F/K.*

Proposition 7.3. *Let L/K be an unramified extension. Then L/K is Galois and* $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$.

Proof. Every finite subextension F/K is unramified, hence Galois. So L/K is Galois. Moreover there exists a diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(k_L/k) \\ \downarrow \simeq & & \downarrow \simeq \\ \varprojlim_{F/K} \mathrm{Gal}(F/K) & \dashrightarrow & \varprojlim_{k'/k} \mathrm{Gal}(k'/k) \end{array}$$

The subextensions $L/F/K$ correspond via $F \mapsto k_F$ bijectively to the intermediate extensions $k_L/k'/k$ and the Galois groups are isomorphic via the reduction map, hence we get an isomorphism of the bottom two groups and the diagram commutes. $\square$

If $L_1, L_2/K$ are finite unramified, then L_1L_2/K is unramified by Exercise Sheet 3. Thus for any L/K there exists a maximal unramified subextension K_0/K.

Let L/K be Galois. There exists a surjection $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(K_0/K) \simeq \mathrm{Gal}(k_L/k)$. Set $I_{L/K} = \ker(\mathrm{res})$ (Inertia subgroup).

Let $\mathrm{Fr}_{k_L/k} \in \mathrm{Gal}(k_L/k)$ be the Frobenius $x \mapsto x^{\#k}$ and let $\langle \mathrm{Fr}_{k_L/k} \rangle$ be the subgroup generated by $\mathrm{Fr}_{k_L/k}$.

Definition. *Let L/K be Galois. The* Weil group $W(L/K) \subseteq \mathrm{Gal}(L/K)$ *is* $\mathrm{res}^{-1}(\langle \mathrm{Fr}_{k_L/k} \rangle)$.

Remark: If k_L/k is finite, then $W(L/K) = \mathrm{Gal}(L/K)$. Otherwise $W(L/K) \subsetneq \mathrm{Gal}(L/K)$.

There is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_{L/K} & \longrightarrow & W(L/K) & \longrightarrow & \langle \mathrm{Fr}_{k_L/k} \rangle & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I_{L/K} & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(k_L/k) & \longrightarrow & 0 \end{array}$$

with exact rows.

We endow $W(L/K)$ with the weakest topology such that

(1) $W(L/K)$ is a topological group.

(2) $I_{L/K}$ is an open subgroup of $W(L/K)$ where $I_{L/K} = \mathrm{Gal}(L/K_0)$ is equipped with the profinite topology.

I.e. open sets are translates of open sets in $I_{L/K}$ by elements of $W(L/K)$.

Warning: If k_L/k is infinite, $W(L/K)$ does not carry the subspace topology in $\mathrm{Gal}(L/K)$, e.g. $I_{L/K} \subseteq W(L/K)$ is not open in subspace topology.

Proposition 7.4. *Let L/K be Galois.*

(i) $W(L/K)$ is dense in $\mathrm{Gal}(L/K)$

(ii) *If* F/K *is a finite subextension of* L/K*, then* $W(L/F) = W(L/K) \cap \mathrm{Gal}(L/F)$*.*

(iii) *If* F/K *is a finite Galois subextension, then*

$$W(L/K)/W(L/F) \cong \mathrm{Gal}(F/K).$$

Proof.

(i) $W(L/K)$ dense in $\mathrm{Gal}(L/K)$ iff for all F/K finite Galois subextensions $W(L/K)$ intersects every coset of $\mathrm{Gal}(L/F)$ iff for all F/K finite Galois subextensions $W(L/K) \to \mathrm{Gal}(F/K)$ is surjective. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_{L/K} & \longrightarrow & W(L/K) & \longrightarrow & \langle \mathrm{Fr}_{k_{L/k}} \rangle & \longrightarrow & 0 \\ & & \downarrow a & & \downarrow b & & \downarrow c & & \\ 0 & \longrightarrow & I_{F/K} & \longrightarrow & \mathrm{Gal}(F/K) & \longrightarrow & \mathrm{Gal}(k_F/k) & \longrightarrow & 0 \end{array}$$

Let K_0/K be the maximal unramified extension contained in L. Then $K_0 \cap F$ is the maximal unramified extension in F. Then $\mathrm{Gal}(L/K_0) \twoheadrightarrow \mathrm{Gal}(F/(K_0 \cap F))$, so a is surjective. Since $\mathrm{Gal}(k_F/k)$ is generated by $\mathrm{Fr}_{k_F/k} = \mathrm{Fr}_{k_{L/k}}|_{k_F}$, c is surjective. By diagram chase, b is surjective.

(ii) Easy from the definitions.

(iii)

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

Note that $W(L/K)\,\mathrm{Gal}(L/F) = \mathrm{Gal}(L/K)$ as $W(L/K)$ is dense in $\mathrm{Gal}(L/K)$ by (i). □

7.2 Statements of local class field theory

Let K be a local field and let K^{ab} be the maximal abelian extension in K^{sep}.

We know that $K^{\mathrm{ur}} = \bigcup_{m=1}^{\infty} K(\zeta_{q^m-1})$ where $q = \#k$. Then $k_{K^{\mathrm{ur}}} = \mathbb{F}_q^{\mathrm{alg}}$ and $\mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}}$.

So K^{ur} is abelian and hence $K^{\mathrm{ur}} \subseteq K^{\mathrm{ab}}$. There is an exact sequence

$$0 \to I_{K^{\mathrm{ab}}/K} \to W(K^{\mathrm{ab}}/K) \to \mathbb{Z} \to 0.$$

Theorem 7.5.

(1) (Local Artin reciprocity) There exists a unique topological isomorphism $\mathrm{Art}_K : K^\times \xrightarrow{\simeq} W(K^{\mathrm{ab}}/K)$ *satisfying the following properties:*

  (i) $\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Fr}_{K^{\mathrm{ur}}/K}$ *for any uniformizer* $\pi \in K$.

  (ii) For each finite subextension L/K *in* K^{ab}/K, $\mathrm{Art}_K(N_{L/K}(L^\times))|_L = \{1\}$.

(2) Let L/K *be finite abelian. Then* Art_K *induces an isomorphism* $K^\times/N_{L/K}(L^\times) \simeq W(K^{\mathrm{ab}}/K)/W(K^{\mathrm{ab}}/L) \simeq \mathrm{Gal}(L/K)$

Remarks:

(i) Special case of Local Langlands.

(ii) Used to characterize global Artin map of global class field theory.

Properties of the Artin map:

- (Existence theorem) For any open finite index subgroup $H \subseteq K^\times$ there exists a finite abelian extension L/K such that $N_{L/K}(L^\times) = H$. In particular, Art_K induces an (inclusion reversing) isomorphism of posets:

$$\begin{aligned} \{\text{open finite index subgroups of } K^\times\} &\longleftrightarrow \{\text{finite abelian extensions } L/K\} \\ H &\longmapsto (K^{\mathrm{ab}})^{\mathrm{Art}_K(H)} \\ N_{L/K}(L^\times) &\longleftarrow L/K \end{aligned}$$

- (Norm functoriality) Let L/K be a finite separable extension. There is a commutative diagram:

$$\begin{array}{ccc} L^\times & \xrightarrow{\mathrm{Art}_L} & W(L^{\mathrm{ab}}/L) \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \mathrm{res}} \\ K^\times & \xrightarrow{\mathrm{Art}_K} & W(K^{\mathrm{ab}}/K) \end{array}$$

Proposition 7.6. *Let* L/K *be a finite abelian extension of degree* n. *Then* $e_{L/K} = [\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$.

Proof. For $x \in L^\times$, we have $v_K(N_{L/K}(x)) = f_{L/K} v_L(x)$. So we get a surjection

$$K^\times/N_{L/K}(L^\times) \overset{v_K}{\twoheadrightarrow} \mathbb{Z}/f_{L/K}\mathbb{Z}$$

with kernel

$$(\mathcal{O}_K^\times N_{L/K}(L^\times))/N_{L/K}(L^\times) = \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap N_{L/K}(L^\times)) = \mathcal{O}_K^\times/N_{L/K}(\mathcal{O}_L^\times).$$

By Theorem 7.5 (2), $n = [K^\times : N_{L/K}(L^\times)] = f_{L/K}[\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$. □

Corollary 7.7. *Let* L/K *be a finite abelian extension. Then* L/K *is unramified iff* $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$.

7.3 Construction of $\mathrm{Art}_{\mathbb{Q}_p}$

Recall: $\mathbb{Q}_p^{\mathrm{ur}} = \bigcup_{m=1}^{\infty} \mathbb{Q}_p(\zeta_{p^m-1}) = \bigcup_{p\nmid m} \mathbb{Q}_p(\zeta_m)$.

$\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$ with $\theta_n : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$. For $n \geq m \geq 1$ there is a commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) & \xrightarrow{\text{res}} & \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) \\ \simeq\big\downarrow \theta_n & & \simeq\big\downarrow \theta_m \\ (\mathbb{Z}/p^n\mathbb{Z})^\times & \xrightarrow{\text{proj}} & (\mathbb{Z}/p^m\mathbb{Z})^\times \end{array}$$

Set $\mathbb{Q}_p(\zeta_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}_p(\zeta_{p^n})$. Then $\mathbb{Q}_p(\zeta_{p^\infty}/\mathbb{Q}_p)$ is Galois and we have

$$\theta : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \xrightarrow{\simeq} \varprojlim_{n\geq 1} (\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}_p^\times.$$

We have $\mathbb{Q}_p(\zeta_{p^\infty}) \cap \mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p$, so there is an isomorphism $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \simeq \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times$.

Theorem 7.8 (Local Kronecker-Weber)**.** $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{ur}}\mathbb{Q}_p(\zeta_{p^\infty})$.

Proof. Omitted □

Construct $\mathrm{Art}_{\mathbb{Q}_p}$ as follows: We have $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p^\times$. Then

$\mathrm{Art}_{\mathbb{Q}_p}(p^n u) = ((\mathrm{Fr}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p})^n, \theta^{-1}(u^{-1})) \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \simeq \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$.

The image lies in $W(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$.

7.4 Construction of Art_K

Let K be a local field, π a uniformizer of K. For $n \geq 1$, we will construct totally ramified Galois extensions $K_{\pi,n}$ such that:

(i) $K \subseteq \ldots \subseteq K_{\pi,n} \subseteq K_{\pi,n+1} \subseteq \ldots$.

(ii) For $n \geq m \geq 1$ there is a commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(K_{\pi,n}/K) & \longrightarrow & \mathrm{Gal}(K_{\pi,m}/K) \\ \simeq\big\downarrow \psi_n & & \simeq\big\downarrow \psi_m \\ \mathcal{O}_K^\times/U_K^{(n)} & \xrightarrow{\text{proj}} & \mathcal{O}_K^\times/U_K^{(m)} \end{array}$$

(iii) Setting $K_{\pi,\infty} = \bigcup_{n=1}^{\infty} K_{\pi,n}$ we have $K^{\mathrm{ab}} = K^{\mathrm{ur}}K_{\pi,\infty}$.

Then (ii) implies that there is an isomorphism $\Psi : \mathrm{Gal}(K_{\pi,\infty}/K) \xrightarrow{\simeq} \varprojlim_n \mathcal{O}_K/U_K^{(n)} \cong \mathcal{O}_K^\times$.

Define Art_K by:

$$\begin{aligned} K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times &\longrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K), \\ x = \pi^n u &\longmapsto (\mathrm{Fr}^n_{K^{\mathrm{ur}}/K}, \Psi^{-1}(u^{-1})) \end{aligned}$$

Remark: Both $K_{\pi,\infty}$ and the isomorphism $K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$ depend on π, but Art_K does not.

Goal: Construct $K_{\pi,n}$.

8 Lubin-Tate Theory

8.1 Formal group laws

Let R be a ring.

Definition. *A (1-dimensional commutative)* formal group law *over R is a power series $F(X,Y) \in R[\![X,Y]\!]$ satisfying*

(i) $F(X,Y) \equiv X + Y \mod (X,Y)^2$

(ii) $F(X,F(Y,Z)) = F(F(X,Y),Z)$

(iii) $F(X,Y) = F(Y,X)$

Examples.

- $\widehat{\mathbb{G}}_a(X,Y) = X + Y$ (formal additive group)
- $\widehat{\mathbb{G}}_m(X,Y) = X + Y + XY$ (formal multiplicative group)

Lemma 8.1. *Let F be a formal group law over R. Then*

(i) $F(X,0) = X$, $F(0,Y) = Y$

(ii) There exists a unique $i(X) \in XR[\![X]\!]$ such that $F(X,i(X)) = 0$.

Proof. Example sheet 4. □

Let K be a complete non-archimedean valued field, F a formal group law over $\mathcal{O}_K$. Then $F(x,y)$ converges for all $x,y \in \mathfrak{m}_K$ to an element in $\mathfrak{m}_K$. Defining $x \cdot_F y = F(X,Y)$ turns $(\mathfrak{m}_K, \cdot_F)$ into a commutative group.

$\widehat{\mathbb{G}}_m$ over $\mathbb{Z}_p$ gives $x \cdot_{\widehat{\mathbb{G}}_m} y = x+y+xy$ for $x,y \in p\mathbb{Z}_p$. There is an isomorphism $(p\mathbb{Z}_p, \cdot_{\widehat{\mathbb{G}}_m}) \cong (1+p\mathbb{Z}_p, \times)$, $x \mapsto 1+x$.

Definition. *Let F,G be formal group laws over R. A* homomorphism *$f : F \to G$ is an element $f(X) \in XR[\![X]\!]$ such that $f(F(X,Y)) = G(f(X),f(Y))$. A homomorphism $f : F \to G$ is an isomorphism if there exists a homomorphism $g : G \to F$ such that $f \circ g = X = g \circ f$.*

Define $\mathrm{End}_R(F)$ *to be the set of homomorphisms $f : F \to F$.*

Proposition 8.2. *Let R be a $\mathbb{Q}$-algebra. There is an isomorphism of formal group laws* $\exp : \widehat{\mathbb{G}}_a \xrightarrow{\simeq} \widehat{\mathbb{G}}_m$ *where* $\exp(X) = \sum_{n=1}^{\infty} \frac{X^n}{n!}$.

Proof. Define $\log X = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n}$. Then there is an equality of formal power series $\log \exp X = X = \exp \log X$ and $\exp(\widehat{\mathbb{G}}_a(X, Y)) = \widehat{\mathbb{G}}_m(\exp X, \exp Y)$. □

Lemma 8.3. $\mathrm{End}_R(F)$ *is a ring with addition* $f +_F g(X) = F(f(X), g(X))$ *and multiplication given by composition.*

8.2 Lubin-Tate formal groups

Let K be a local field with $\#k = q$.

Definition. *A* formal $\mathcal{O}_K$-module *over $\mathcal{O}_K$ is a formal group law $F(X, Y) \in \mathcal{O}_K[\![X, Y]\!]$ together with a ring homomorphism $[\cdot]_F : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$ such that for all $a \in \mathcal{O}_K$,* $[a]_F(X) \equiv aX \bmod X^2$ *A* homomorphism/isomorphism *$f : F \to G$ of formal $\mathcal{O}_K$modules is a homomorphism/isomorphism of formal group laws such that $f \circ [a]_F = [a]_G \circ f$ for all $a \in \mathcal{O}_K$.*

Definition. *Let $\pi \in \mathcal{O}_K$ be a uniformizer. A* Lubin-Tate series for π *is a power series $f(X) \in \mathcal{O}_K[\![X]\!]$ such that*

(a) $f(X) \equiv \pi X \bmod X^2$

(b) $f(X) \equiv X^q \bmod \pi$

Example. $K = \mathbb{Q}_p$, $f(X) = (X + 1)^p - 1$ is a Lubin-Tate series for p.

Theorem 8.4. *Let $f(X)$ be a Lubin-Tate series for π. Then:*

(i) There exists a unique formal group law F_f over $\mathcal{O}_K$ such that $f \in \mathrm{End}_{\mathcal{O}_K}(F_f)$.

(ii) There exists a ring homomorphism $[\cdot]_f : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F_f)$ which makes F_f into a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$.

(iii) If $g(x)$ is another Lubin-Tate series for π, then $F_f \cong F_g$ as formal $\mathcal{O}_K$-modules.

F_f is the Lubin-Tate formal group law *for π.*

Example. $K = \mathbb{Q}_p$, $f(X) = (X + 1)^p - 1$. The associated Lubin-Tate formal group F_f is $\widehat{\mathbb{G}}_m$. For this we need to show that $f \circ \widehat{\mathbb{G}}_m = \widehat{\mathbb{G}}_m \circ (f, f)$. We have

$$f(\widehat{\mathbb{G}}_m(X, Y)) = (1 + X + Y + XY)^p - 1 = (1 + X)^p(1 + Y)^p - 1 = \widehat{\mathbb{G}}_m(f(X), f(Y)).$$

Lemma 8.5. *Let $f(X), g(X)$ be two Lubin-Tate series for π. Let $L(X_1, \dots, X_n) = \sum_{i=1}^{n} a_i X_i$, with $a_i \in \mathcal{O}_K$. Then there exists a unique power series $F(X_1, \dots, X_n) \in \mathcal{O}_K[\![X_1, \dots, X_n]\!]$ such that:*

(i) $F(X_1,\ldots,X_n) \equiv L(X_1,\ldots,X_n) \bmod \deg 2$.

(ii) $f(F(X_1,\ldots,X_n)) = F(g(X_1),\ldots,g(X_n))$.

Proof. We show by induction that there exists a unique $F_m \in \mathcal{O}_K[X_1,\ldots,X_n]$ of total degree $\leq m$ such that

(a) $f(F_m(X_1,\ldots,X_n)) \equiv F_m(g(X_1),\ldots,g(X_n)) \bmod \deg m+1$.

(b) $F_m(X_1,\ldots,X_n) \equiv L(X_1,\ldots,X_n) \bmod \deg 2$

(c) $F_m \equiv F_{m+1} \bmod \deg m+1$.

For $m = 1$, take $F_1 = L$. Then (b) is satisfied. For (a) we compute $f(F_1(X_1,\ldots,X_n)) \equiv \pi L(X_1,\ldots,X_n) \equiv F_1(g(X_1),\ldots,g(X_n)) \bmod \deg 2$.

Suppose F_m is constructed where $m \geq 1$. Set $F_{m+1} = F_m + h$ where $h \in \mathcal{O}_K[X_1,\ldots,X_n]$ is homogeneous of degree $m+1$. Then since $f(X+Y) = f(X) + f'(X)Y + Y^2(\ldots)$ and $f'(X) \equiv \pi \bmod X$,

$$f \circ (F_m + h) \equiv f \circ F_m + \pi h \bmod \deg m+2.$$

Similarly,

$$(F_m + h) \circ g \equiv F_m \circ g + h(\pi X_1,\ldots,\pi X_n) \equiv F_m \circ g + \pi^{m+1} h(X_1,\ldots,X_m) \bmod \deg m+2.$$

Thus (a), (b) and (c) are satisfied iff $f \circ F_m - F_m \circ g \equiv (\pi - \pi^{m+1})h \bmod \deg m+2$. But $f(X) \equiv g(X) \equiv X^q \bmod \pi$, so

$$f \circ F_m - F_m \circ g \equiv F_m(X_1,\ldots,X_n)^q - F_m(X_1^q,\ldots,X_n^q) \bmod \pi.$$

Thus $f \circ F_m - F_m \circ g \in \pi\mathcal{O}_K[\![X_1,\ldots,X_n]\!]$. Let $r(X_1,\ldots,X_n)$ be the degree $m+1$ terms in $f \circ F_m - F_m \circ g$. Then set $h := \frac{1}{\pi(1-\pi^m)} r \in \mathcal{O}_K[X_1,\ldots,X_n]$ so that F_{m+1} satisfies (a), (b), (c). It is unique since h is determined by property (a).

Set $F = \lim_{m\to\infty} F_m$ which exists by (c). Uniqueness of F follows from uniqueness of the F_m. □

Proof of Theorem 8.4.

(i) By the Lemma there exists a unique $F_f(X,Y) \in \mathcal{O}_K[\![X,Y]\!]$ such that

- $F_f(X,Y) \equiv X + Y \bmod \deg 2$,
- $f(F_f(X,Y)) = F_f(f(X), f(Y))$.

We must prove that F_f is indeed a formal group law.

Associativity: $F_f(X, F_f(Y,Z)) \equiv X + Y + Z \equiv F_f(F_f(X,Y),Z) \bmod \deg 2$ and $f \circ F_f(X, F_f(Y,Z)) = F_f(f(x), f(F_f(Y,Z))) = F_f(f(x), F_f(f(Y), f(Z)))$. Similarly $f \circ F_f(F_f(X,Y),Z) = F_f(F_f(f(X),f(Y)), f(Z))$. Thus $F_f(X,F_f(Y,Z)) = F_f(F_f(X,Y),Z)$ by the uniqueness in the lemma.

Commutativity is proved similarly.

(ii) By the Lemma, for $a \in \mathcal{O}_K$ there exists a unique $[a]_{F_f} \in \mathcal{O}_K[\![X]\!]$ such that

- $[a]_{F_f} \equiv aX \mod X^2$
- $f \circ [a]_{F_f} = [a]_{F_f} \circ f$.

Then $[a]_{F_f} \circ F_f = F_f \circ [a]_{F_f}$ using a similar argument as above (uniqueness).

The map $[\cdot]_{F_f} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F_f)$ is a ring homomorphism (again verified using uniqueness). So F_f is a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. Also note that $[\pi]_{F_f} = f$.

(iii) If $g(X)$ is another Lubin-Tate series for π, let $\theta(X) \in \mathcal{O}_K[\![X]\!]$ be the unique power series such that $\theta(X) \equiv X \mod X^2$ and $\theta \circ f = g \circ \theta$. Then $\theta \circ F_f = F_g(\theta(X), \theta(Y))$ (uniqueness), so $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(F_f, F_g)$. Reversing roles of f, g, we obtain $\theta^{-1}(X) \in \mathcal{O}_K[\![X]\!]$, $\theta^{-1} \in \mathrm{Hom}_{\mathcal{O}_K}(F_g, F_f)$. Then $\theta^{-1} \circ \theta(X) = X$ and $\theta \circ \theta^{-1}(X) = X$ (uniqueness). So θ is an isomorphism of formal group laws.

Again by uniqueness we find that $\theta \circ [a]_{F_f}(X) = [a]_{F_f} \circ \theta(X)$ for all $a \in \mathcal{O}_K$ and hence θ is an isomorphism of formal $\mathcal{O}_K$-modules.

□

8.3 Lubin-Tate extensions

Let K be a non-archimedean local field, $\#k = q$, π uniformizer. Let K^{alg} be the algebraic closure of K, $\overline{\mathfrak{m}} \subseteq \mathcal{O}_{K^{\mathrm{alg}}}$ the maximal ideal.

Lemma 8.6. *Let F be a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. Then $\overline{\mathfrak{m}}$ becomes a (genuine) $\mathcal{O}_K$-module with $x +_F y = F(x, y)$ and $a \cdot_F x = [a]_F(x)$ for $x, y, \in \overline{\mathfrak{m}}$ and $a \in \mathcal{O}_K$.*

Proof. Given $x \in \overline{\mathfrak{m}}$, we have $x \in \mathfrak{m}_L$ for some L/K finite. Since $[a]_F \in \mathcal{O}_K[\![X]\!]$, $[a]_F(x)$ converges in L and its limit lies in $\mathfrak{m}_L \subseteq \overline{\mathfrak{m}}$. Similarly $x +_F y$ is well-defined. □

Definition. *Let $f(x)$ be a Lubin-Tate series for π and F_f the associated Lubin-Tate formal group law. The π^n-*torsion group *is*

$$\mu_{f,n} := \{x \in \overline{\mathfrak{m}} \mid \pi^n \cdot_{F_f} x = 0\} = \{x \in \overline{\mathfrak{m}} \mid f_n(x) = f \circ f \circ \cdots \circ f(x) = 0\}.$$

Note that $\mu_{f,n}$ is an $\mathcal{O}_K$-module and $\mu_{f,n} \subseteq \mu_{f,n+1}$.

Example. $K = \mathbb{Q}_p$, $f(X) = (X+1)^p - 1$. Then $[p^n]_{F_f}(x) = (x+1)^{p^n} - 1$. Thus $\mu_{f,n} = \{\zeta_{p^n}^i - 1 \mid i = 0, \dots, p^n - 1\}$.

Now let $f(X) = \pi X + X^q$. Then $f_n(X) = f \circ f_{n-1}(X) = f_{n-1}(X)(\pi + f_{n-1}(X)^{q-1})$. Set $h_n(X) = \frac{f_n(X)}{f_{n-1}(X)} = \pi + f_{n-1}(X)^{q-1}$. We set $f_0(X) = X$.

Proposition 8.7. *$h_n(X)$ is a separable Eisenstein polynomial of degree $q^{n-1}(q-1)$.*

Proof. It is clear that $h_n(X)$ is monic of degree $q^{n-1}(q-1)$. $f(X) \equiv X^q \bmod \pi$, so $f_{n-1}(X)^{q-1} \equiv X^{q^{n-1}(q-1)} \bmod \pi$. Since $f_{n-1}(X)$ has 0 constant term, $h_n(X) = \pi + f_{n-1}(X)^{q-1}$ has constant term π. Thus $h_n(X)$ is Eisenstein. Since $h_n(X)$ is irreducible, $h_n(X)$ is separable if $\operatorname{char} K = 0$, or if $\operatorname{char} K = p$ and $h_n'(X) \neq 0$. Assume $\operatorname{char} K = p$. Induct on n. $h_1(X) = \pi + X^{q-1}$ is separable. Suppose $h_{n-1}(X), \ldots, h_1(X)$ are separable. Then $f_{n-1}(X) = h_{n-1}(X) \cdots h_1(X)X$ is separable (product of separable irreducible polynomials of different degrees). Then $h_n(X) = \pi + f_{n-1}(X)^{q-1}$. We have $h_n'(X) = (q-1)f_{n-1}'(X)f_{n-1}(X)^{q-2} \neq 0$, so $h_n(X)$ is separable. □

Note that the proof also shows that $f_n(X)$ is separable.

Proposition 8.8.

(i) $\mu_{f,n}$ is a free module of rank 1 over $\mathcal{O}_K/\pi^n\mathcal{O}_K$.

(ii) If g is another Lubin-Tate series for π, then $\mu_{f,n} \cong \mu_{g,n}$ as $\mathcal{O}_K$-modules and $K(\mu_{f,n}) = K(\mu_{g,n})$.

Proof.

(i) Let $\alpha \in K$ be a root of $h_n(X)$. Since $h_n(X)$ and $f_{n-1}(X)$ are coprime, $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$. Then the map $\tilde{\varphi} : \mathcal{O}_K \to \mu_{f,n}, a \mapsto a \cdot_{F_f} \alpha$ is an $\mathcal{O}_K$-module homomorphism with $\pi^n\mathcal{O}_K \subseteq \ker \tilde{\varphi}$ and $\pi^{n-1} \notin \ker \tilde{\varphi}$. Therefore $\ker \tilde{\varphi} = \pi^n\mathcal{O}_K$. Thus $\tilde{\varphi}$ induces an injection $\varphi : \mathcal{O}_K/\pi^n\mathcal{O}_K \hookrightarrow \mu_{f,n}$. Since $f_n(X)$ is separable, $\#\mu_{f,n} = \deg f_n(X) = q^n = \#\mathcal{O}_K/\pi^n\mathcal{O}_K$. So φ is an isomorphism.

(ii) Let $\theta \in \operatorname{Hom}_{\mathcal{O}_K}(F_f, F_g)$ be an isomorphism of formal $\mathcal{O}_K$-modules. It induces an isomorphism $\theta : (\overline{\mathfrak{m}}, +_{F_f}, \cdot_{F_f}) \xrightarrow{\simeq} (\overline{\mathfrak{m}}, +_{F_g}, \cdot_{F_g})$ and hence $\mu_{f,n} \cong \mu_{g,n}$. Since $\mu_{f,n}$ is algebraic, $K(\mu_{f,n})/K$ is finite, hence complete. Since $\theta(X) \in \mathcal{O}_K[\![X]\!]$, for $x \in \mu_{f,n}$ we also have $\theta(x) \in K(\mu_{f,n})$. So $K(\mu_{g,n}) \subseteq K(\mu_{f,n})$. The same argument for θ^{-1} gives the reverse inclusion. □

Definition. $K_{\pi,n} := K(\mu_{f,n})$

Remark: $K_{\pi,n}$ does not depend on f by the proposition. We have $K_{\pi,n} \subseteq K_{\pi,n+1}$.

Proposition 8.9. *$K_{\pi,n}$ are totally ramified Galois extensions of degree $q^{n-1}(q-1)$.*

Proof. We may choose $f(X) = \pi X + X^q$. Then $K_{\pi,n}/K$ is Galois since $K_{\pi,n} = K(\mu_{f,n})$ is the splitting field of $f_n(X)$. Let α be a root of $h_n(X) = f_n(X)/f_{n-1}(X)$. It suffices to show $K(\alpha) = K(\mu_{f,n})$ since α is the root of an Eisenstein polynomial of degree $q^{n-1}(q-1)$. By the proposition every element $x \in \mu_{f,n}$ is of the form $a \cdot_{F_f} \alpha$ for some $a \in \mathcal{O}_K$. Since $K(\alpha)$ is complete and $[a]_{F_f}(X) \in \mathcal{O}_K[\![X]\!]$, we get $x = [a]_{F_f}(\alpha) \in K(\alpha)$. □

Let f be the Lubin-Tate series $\pi X + X^q$.

Theorem 8.10. *There are isomorphisms $\Psi_n : \mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ characterized by*

$$(*) \quad \Psi_n(\sigma) \cdot_{F_f} x = \sigma(x) \quad \forall x \in \mu_{f,n},\ \sigma \in \mathrm{Gal}(K_{\pi,n}/K)$$

Moreover, Ψ_n does not depend on f.

Proof. Let $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. Then σ preserves $\mu_{f,n}$, and acts continuously on $K(\mu_{f,n}) = K_{\pi,n}$. Since $F_f(X,Y) \in \mathcal{O}_K[\![X]\!]$, and $[a]_{F_f} \in \mathcal{O}_K[\![X]\!]$ for all $a \in \mathcal{O}_K$, we have $\sigma(x +_{F_f} y) = \sigma(x) +_{F_f} \sigma(y)$ and $\sigma(a \cdot_{F_f} x) = a \cdot_{F_f} \sigma(x)$ for all $x, y \in \mu_{f,n}, a \in \mathcal{O}_K$.

Thus $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n})$. this induces a group homomorphism $\mathrm{Gal}(K_{\pi,n}/K) \to \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n})$ which is injective since $K_{\pi,n} = K(\mu_{f,n})$. Since $\mu_{f,n} \cong \mathcal{O}_K/\pi^n$ as $\mathcal{O}_K$-module, we get

$$\mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n}) \cong \mathrm{Aut}_{\mathcal{O}_K/\pi^n}(\mu_{f,n}) \cong (\mathcal{O}_K/\pi^n)^\times$$

We obtain $\Psi_n : \mathrm{Gal}(K_{\pi,n}/K) \hookrightarrow (\mathcal{O}_K/\pi^n)^\times$ defined by: $\Psi_n(\sigma) \in (\mathcal{O}_K/\pi^n)^\times$ is the unique element such that $\Psi_n(\sigma) \cdot_{F_f} x = \sigma(x)$ for all $x \in \mu_{f,n}$. Since $[K_{\pi,n} : K] = q^{n-1}(q-1) = \#(\mathcal{O}_K/\pi^n)^\times$, Ψ_n is surjective by counting.

Let g be another Lubin-Tate series. Then we obtain $\Psi'_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\simeq} (\mathcal{O}_K/\pi^n)^\times$. Let $\theta : F_f \to F_g$ be an isomorphism of formal $\mathcal{O}_K$-modules. It induces an isomorphism $\theta : \mu_{f,n} \xrightarrow{\simeq} \mu_{g,n}$ of $\mathcal{O}_K$-modules. Hence for $x \in \mu_{f,n}$, $\theta(\Psi_n(\sigma) \cdot_{F_f} x) = \Psi_n(\sigma) \cdot_{F_g} \theta(x)$. But $\theta \in \mathcal{O}_K[\![X]\!]$ has coefficients in $\mathcal{O}_K$, so $\theta(\sigma x) = \sigma(\theta x)$ for all $x \in \mu_{f,n}$. Then $\theta(\Psi_n(\sigma) \cdot_{F_f} x) = \theta(\sigma x) = \sigma(\theta x) = \Psi'_n(\sigma) \cdot_{F_g} \theta(x)$, so $\Psi_n(\sigma) = \Psi'_n(\sigma)$. ☐

Set $K_{\pi,\infty} = \bigcup_{k=1}^{\infty} K_{\pi,n}$. Then there is an isomorphism

$$\Psi : \mathrm{Gal}(K_{\pi,\infty}/K) \cong \varprojlim_n (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times.$$

Theorem 8.11 (Generalized local Kronecker-Weber)**.** $K^{\mathrm{ab}} = K_{\pi,\infty}K^{\mathrm{ur}}$.

Proof. Omitted. ☐

Now we define Art_K by

$$\begin{aligned} K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times &\longrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K), \\ x = \pi^n u &\longmapsto (\mathrm{Fr}^n_{K^{\mathrm{ur}}/K}, \Psi^{-1}(u^{-1})) \end{aligned}$$

9 **Upper Numbering of Ramification Groups

Let L/K be a finite Galois extension of local fields. Define the function

$$\Phi := \Phi_{L/K} : \mathbb{R}_{\geq -1} \longrightarrow \mathbb{R},$$
$$\Phi(s) = \int_0^s \frac{dt}{[G_0 : G_t]}.$$

For $t \in [-1, 0)$ we set $\frac{1}{[G_0:G_t]} = [G_t : G_0]$.

For $m \leq s < m+1$ where $m \in \mathbb{Z}_{\geq -1}$ we have

$$\Phi(s) = \begin{cases} s[G_{-1} : G_0] & m = -1, \\ \frac{1}{\#G_0}(\#G_1 + \cdots + \#G_m + (s-m)\#G_{m+1}) & m \geq 0. \end{cases}$$

Φ is continuous, piecewise linear and strictly increasing. Therefore we can define $\Psi_{L/K} = \Phi_{L/K}^{-1}$.

Definition (Upper numbering)**.** *The higher ramification groups in* upper numbering *are defined by*

$$G^s(L/K) := G_{\Psi_{L/K}(s)}(L/K) \subseteq \mathrm{Gal}(L/K).$$

Key point: $G_s(L/K)$ behaves well w.r.t. subgroups. $G^s(L/K)$ behaves well w.r.t. quotients.

Let $L/F/K$ be fields with L/K Galois. Then $G_s(L/F) = G_s(L/K) \cap \mathrm{Gal}(L/F)$. If also F/K is Galois, then $G^t(L/K)\,\mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/F) = G^t(F/K)$ (Herbrand's theorem).

Example. $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\zeta_{p^n})$. Let $k \in \mathbb{Z}$, $1 \leq k \leq n-1$. For $p^{k-1} - 1 < s \leq p^k - 1$, $G_s \simeq \{m \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid m \equiv 1 \bmod p^k\} \cong U_{\mathbb{Q}_p}^{(k)}/U_{\mathbb{Q}_p}^{(n)}$.

G_s jumps at $p^k - 1$, $\Phi_{L/K}$ is linear on $[p^{k-1}-1, p^k-1]$, thus to compute $\Phi_{L/K}$, it suffices to compute $\Phi_{L/K}(p^k - 1)$. We have $\Phi_{L/K}(p^k-1) = (p-1) \cdot \frac{1}{p-1} + \frac{p^2-1-(p-1)}{p(p-1)} + \cdots = 1 + 1 + \cdots + 1 = k$. Then

$$G^s \cong \begin{cases} (\mathbb{Z}/p^n)^\times & s \leq 0, \\ (1+p^k\mathbb{Z})/p^n\mathbb{Z} & k-1 < s \leq k (1 \leq k \leq n-1), \\ 1 & s > n-1. \end{cases}$$

In particular $G^k \cong U_{\mathbb{Q}_p}^{(k)}/U_{\mathbb{Q}_p}^{(n)}$ $1 \leq k \leq n-1$.