Local Fields

Harry Armitage

November 20, 2020

Contents

1 Basic Theory **3**
1.1 Absolute Values . . . 3

2 Valuation Rings **6**

3 The p-adic Numbers **8**
3.1 Brief Digression on Inverse Limits . . . 9

4 Complete Valued Fields **11**
4.1 Hensel's Lemma . . . 11

5 Teichmüller Lifts **13**

6 Extensions of Complete Valued Fields **16**

7 Local Fields **20**
7.1 More On Inverse Limits . . . 21

8 Local Fields II **21**
8.1 Witt Vectors . . . 22

9 Archimedean Local Fields **25**

10 Global Fields **27**
10.1 Dedekind Domains . . . 29

11 Dedekind Domains II **30**
11.1 Dedekind Domains and Extensions . . . 31

12 Dedekind Domains & Extensions **33**
12.1 Completions . . . 34

13 Decomposition Groups **36**

14 Ramification Theory **39**
14.1 Unramified and Totally Ramified Extensions . . . 39

15 Structure of Units **42**

16 Higher Ramification Groups **43**
16.1 Upper Numbering of Ramification Groups 46

17 Proof of Herbrand's Theorem **47**

18 Local Class Field Theory **50**
18.1 Infinite Galois Theory 50
18.2 Weil Group 51

19 Local Class Field Theory **53**
19.1 Properties of the Artim map 54
19.2 Construction of $\mathrm{Art}_{\mathbb{Q}_p}$ 55
19.3 General Case 56

1 Basic Theory

Suppose we have a diophantine polynomial $f(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r]$. Then we might want to find integer solutions to the equation $f(x_1, \dots, x_r) = 0$. However, it turns out this can be very difficult to do, for instance showing $x^n + y^n - z^n = 0$ has no solutions for $x, y, z \in \mathbb{Z}$ took hundreds of years and a lot of advanced mathematics.

Instead, we study congruences of the form $f(x_1, \dots, x_r) \equiv 0 \mod p^n$, for prime p and integer n. This then becomes a finite computation, and hence a much easier problem. Local fields will give us a way to package all this information together.

1.1 Absolute Values

Definition 1.1. *Let K be a field. An* **absolute value** *on K is a function* $|\cdot| : K \to \mathbb{R}_{\geq 0}$ *such that:*

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x||y| \ \forall x, y \in K$
3. $|x + y| \leq |x| + |y| \ \forall x, y \in K$

We say that $(K, |\cdot|)$ *is a valued field.*

Examples:

1. $K = \mathbb{R}$ or $\mathbb{C}$ with $|\cdot|$ the usual absolute value. We write $|\cdot|_\infty$ for this absolute value.
2. K is any field. The ***trivial absolute value*** on K is defined by:

$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases} \tag{1}$$

   We will ignore this absolute value in this course.

3. $K = \mathbb{Q}$, p a prime. For $0 \neq x \in \mathbb{Q}$, we can write $x = p^n \frac{a}{b}$, where $a, b \in \mathbb{Z}, (a, p) = 1$, and $(b, p) = 1$. The ***p-adic absolute value*** is defined to be:

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

   We check the axioms.

   1. Clear from the definition.
   2. $|xy|_p = |p^{m+n} \frac{ac}{bd}|_p = p^{-m-n} = |x|_p |y|_p$
   3. Wlog, $m \geq n$. $|x + y|_p = \left| p^n \left(\frac{ad + p^{m-n} bc}{bd} \right) \right|_p \leq p^{-n} = \max(|x|_p, |y|_p)$

An absolute value on K induces a metric $d(x, y) = |x - y|$ on K, and hence induces a topology on K. As an exercise, check that $+, \cdot$ are continuous.

Definition 1.2. *Let* $|\cdot|, |\cdot|'$ *be absolute values on a field K. We say that* $|\cdot|, |\cdot|'$ *are* **equivalent** *if they induce the same topology on K. An equivalence class of absolute values is called a* **place***.*

Proposition 1.3. *Let* $|\cdot|, |\cdot|'$ *be non-trivial absolute values on K. The following are equivalent:*

1. *$|\cdot|, |\cdot|'$ are equivalent.*
2. *$|x| < 1 \iff |x|' < 1 \; \forall x \in K$.*
3. *$\exists\, c \in \mathbb{R}_{>0}$ s.t. $|x|^c = |x|' \; \forall x \in K$*

Proof.
<u>*1. $\implies$ 2.*</u>

$$\begin{aligned} |x| < 1 &\iff x^n \to 0 \text{ w.r.t. } |\cdot| && (2) \\ &\iff x^n \to 0 \text{ w.r.t. } |\cdot|' && (3) \\ &\iff |x|' < 1 && (4) \end{aligned}$$

<u>*2. $\implies$ 3.*</u> Let $a \in K^\times$ s.t. $|a| < 1$, which exists since $|\cdot|$ is non-trivial. We need to show that, for all $x \in K^\times$, we have:

$$\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}$$

Assume $\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}$. Then choose $m, n \in \mathbb{Z}$ so that $\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}$. Then we have:

$$\begin{aligned} n \log|x| &< m \log|a| \\ n \log|x|' &> m \log|a|' \end{aligned}$$

and hence $|\frac{x^n}{a^m}| < 1, |\frac{x^n}{a^m}|' > 1, \lightning$.

<u>*3. $\implies$ 1.*</u> This is clear, as open balls in one topology will also be open balls in the other, hence the topologies will be the same. □

In this course, we will be mainly interested in the following types of absolute values:

Definition 1.4. *An absolute value $|\cdot|$ on K is said to be* **non-archimedean** *if it satisfies the ultrametric inequality $|x + y| \leq \max(|x|, |y|)$*

If $|\cdot|$ is not non-archimedean, then it is archimedean.
<u>Examples:</u>

1. $|\cdot|_\infty$ on $\mathbb{R}$ is archimedean.
2. $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$.

Lemma 1.5 (All triangles are isosceles)**.** *Let $(K, |\cdot|)$ be a non-archimedean valued field, and $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$.*

Proof. Observe that $|1| = |1 \cdot 1| = |1| \cdot |1|$, and so $|1| = 1$ or 0. But $1 \neq 0$, so $|1| = 1$. Similarly, $|-1| = 1$, and so $|-y| = |y|$ for all $y \in K$.

Then if $|x| < |y|$, $|x - y| \leq \max(|x|, |y|) = |y|$.

At the same time $|y| \leq \max(|x|, |x - y|) \implies |y| \leq |x - y|$.

Hence $|y| = |x - y|$. □

Proposition 1.6. *Let $(K, |\cdot|)$ be non-archimedean, and $(x_n)_{n=1}^{\infty}$ be a sequence in K.*
If $|x_n - x_{n+1}| \to 0$, then $(x_n)_{n=1}^{\infty}$ is Cauchy.
In particular, if K is in addition complete, then $(x_n)_{n=1}^{\infty}$ converges.

Proof. For $\varepsilon > 0$, choose N such that $|x_n - x_{n+1}| < \varepsilon \ \forall n > N$.
Then for $N < n < m$, we have:

$$|x_n - x_m| = |(x_n - x_{n+1}) + (x_{n+1} - x_{n+1}) + \ldots + (x_{m-1} - x_m)| < \varepsilon$$

And so the sequence is Cauchy. □

For example, if $p = 5$, construct the sequence $(x_n)_{n=1}^{\infty}$ such that:

1. $x_n^2 + 1 \equiv 0 \mod 5^n$
2. $x_n \equiv x_{n+1} \mod 5^n$

as follows:

Take $x_1 = 2$. Suppose we have constructed x_n. Let $x_n^2 + 1 = a5^n$, and set $x_{n+1} = x_n + b5^n$. Then $x_{n+1}^2 + 1 = x_n^2 + 2b5^n x_n + b^2 5^{2n} + 1 = a5^n + 2b5^n x_n + b^2 5^{2n}$.

We choose b such that $a + 2bx_n \equiv 0 \mod 5$, i.e. $b \equiv -\frac{a}{2x_n} \mod 5$, and then we have $x_{n+1}^2 + 1 \equiv 0 \mod 5^{n+1}$ as desired.

The second property implies that $|x_{n+1} - x_n|_5 < 5^{-n} \to 0$, and so the sequence is Cauchy. Now suppose that $x_n \to L \in \mathbb{Q}$. Then $x_n^2 \to L^2$. But the first property then gives us that $x_n^2 \to -1 \implies L^2 = -1 \lightning$. So $(\mathbb{Q}, |\cdot|_5)$ is not complete.

Definition 1.7. *The p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.*

We have an analogy with $\mathbb{R}$, in that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$.

If $(K, |\cdot|)$ is a valued field, for $x \in K$, $r \in \mathbb{R}_{>0}$, we define:

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

and call these the ***open*** and ***closed balls*** of radius r centred at x, respectively.

Lemma 1.8. *Let $(K, |\cdot|)$ be non-archimedean. Then:*

1. *If $z \in B(x, r)$, then $B(z, r) = B(x, r)$.*
2. *If $z \in \overline{B}(x, r)$, then $\overline{B}(z, r) = \overline{B}(x, r)$.*
3. *$B(x, r)$ is closed.*
4. *$\overline{B}(x, r)$ is open.*

Proof.

1. Let $y \in B(x, r)$. Then $|x - y| < r \implies |z - y| = |(z - x) + (x - y)| \leq \max(|z - x|, |x - y|) < r$.
2. Same as in *1.*, but with $\leq$ instead of $<$.

3. Let $y \notin B(x,r)$. We need to show there is an open neighbourhood of y not intersecting $B(x,r)$. If $z \in B(x,r) \cap B(y,r)$, then $B(x,r) = B(z,r) = B(y,r)$. But then $y \in B(x,r)$↯. So $B(x,r)$ and $B(y,r)$ are disjoint, and so $B(x,r)$ is closed.

4. If $z \in \overline{B}(x,r)$, then we need to show there is an open neighbourhood of z contained in $\overline{B}(x,r)$. But $B(z,r) \subseteq \overline{B}(z,r) = \overline{B}(x,r)$, and so $\overline{B}(x,r)$ is open.

□

2 Valuation Rings

Definition 2.1. *Let K be a field. A* **valuation** *on K is a function $v : K^\times \to \mathbb{R}$ such that:*

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

Fix $0 < \alpha < 1$. If v is a valuation on K, then $|x| = \begin{cases} \alpha^{v(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$ determines a non-archimedean absolute value. Conversely, a non-archimedean absolute value determines a valuation $v(x) = \log_\alpha |x|$.

We will ignore the trivial valuation $v(x) \equiv 0$, which corresponds to the trivial absolute value.

We say v_1, v_2 are ***equivalent*** if $\exists\ c \in \mathbb{R}_{>0}$ such that $v_1(x) = cv_2(x)\ \forall x \in K^\times$.

Examples:

- $K = \mathbb{Q}$, $v_p(x) = -\log_p |x|_p$ is the p-adic valuation.
- k any field, $K = k(t) = \mathrm{Frac}(k[t])$, the rational function field. $v\left(t^n \frac{f(t)}{g(t)}\right) = n$ where $f, g \in k[t]$, $f(0), g(0) \neq 0$. This is the t-adic valuation.
- $K = k((t)) = \mathrm{Frac}(k[[t]])$, the field of ***formal Laurent series over k***. Then we have $v\left(\sum_i a_i t^i\right) = \min\{i : a_i \neq 0\}$ is the t-adic valuation on K.

Definition 2.2. *Let $(K, |\cdot|)$ be a non-archimedean valued field. The* **valuation ring** *of K is defined to be:*

$$\begin{aligned} \mathcal{O}_K &= \{x \in K : |x| \leq 1\} \quad (= \bar{B}(0,1)) \\ &= \{x \in K^\times : v(x) \geq 0\} \cup \{0\} \end{aligned}$$

Proposition 2.3.

1. *$\mathcal{O}_K$ is an open subring of K.*
2. *The subsets $\{x \in K : |x| \leq r\}$ and $\{x \in K : |x| < r\}$ for $r \leq 1$ are open ideals in $\mathcal{O}_K$.*
3. *$\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$.*

Proof.

1. $|1| = 1, |0| = 0$, so $1, 0 \in \mathcal{O}_K$. $|-x| = |x|$, so $x \in \mathcal{O}_K \implies -x \in \mathcal{O}_K$. If $x, y \in \mathcal{O}_K$, then $|x+y| \leq \max(|x|, |y|) \leq 1$, and so $x + y \in \mathcal{O}_K$, and $|xy| = |x||y| \leq 1$, so $xy \in \mathcal{O}_K$. Since $\mathcal{O}_K = \bar{B}(0,1)$, it is open.

2. The proof of this is the same as *1.*
3. Note that $|x||x^{-1}| = |xx^{-1}| = 1$. So $|x| = 1 \iff |x^{-1}| = 1$. This can happen if and only if $x, x^{-1} \in O_K$, i.e. $x \in O_K^\times$.

□

As a point of notation, we will define $m := \{x \in O_K : |x| < 1\}$, a maximal ideal of O_K, and $k := O_K/m$ to be the ***residue field***.

We say a ring R is ***local*** if it has a unique maximal ideal. As an exercise, prove that R is local if and only if $R \setminus R^\times$ is an ideal of R. We can use this to prove the following:

Corollary 2.4. *O_K is a local ring with a unique maximal ideal m.*

Proof. Suppose $x \in O_K \setminus m$. Then $|x| = 1$, so $x^{-1} \in O_K$, and so any ideal containing x contains $x^{-1}x = 1$, i.e. is all of O_K, and hence m is the unique maximal ideal in O_K. □

Examples:

- $K = k((t)), O_K = k[[t]], m = (t)$, and the residue field is k.
- $K = \mathbb{Q}$ with $|\cdot|_p$. $O_K = \mathbb{Z}_{(p)}, m = p\mathbb{Z}_{(p)}, k = \mathbb{F}_p$.

Definition 2.5. *Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \cong \mathbb{Z}$, we say v is a* **discrete valuation***, and K is said to be a* **discretely valued field***. An element $\pi \in O_K$ is a* **uniformizer** *if $v(\pi) = 0$ and $v(\pi)$ generates $v(K^\times)$.*

Remark: If v is a discrete valuation, we can replace it with an equivalent one such that $v(K^\times) = \mathbb{Z} \subseteq \mathbb{R}$. Such v are called ***normalized valuations***, and have $v(\pi) = 1$ for π a uniformizer.

Lemma 2.6. *Let v be a valuation on K. Then the following are all equivalent:*

1. *v is discrete.*
2. *O_K is a PID.*
3. *O_K is noetherian.*
4. *m is principal.*

Proof.
1. $\implies$ 2. Let $I \subseteq O_K$ be a non-zero ideal. Let $x \in I$ such that $v(x) = \min\{v(a) : a \in I\}$, which exists since v is discrete. Then $xO_K = \{a \in O_K : v(a) \geq v(x)\} \subseteq I$, and hence $xO_K = I$ by definition of x - if $y \in I \setminus (x)$, then $v(y) < v(x)$↯.

2. $\implies$ 3. Every PID is noetherian, as all ideals are finitely generated (by a single element).

3. $\implies$ 4. Write $m = x_1O_K + \ldots + x_nO_K$. WLOG, $v(x_1) \leq v(x_2) \leq \ldots \leq v(x_n)$. Then $m = x_1O_K$.

4. $\implies$ 1. Let $m = \pi O_K$ for some $\pi \in O_K$, and let $c = v(\pi)$. Then if $v(x) > 0$, $x \in m$ and hence $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \emptyset$. Since $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, we have $v(K^\times) = c\mathbb{Z}$. □

Lemma 2.7. *Let v be a discrete valuation on K, and $\pi \in O_K$ a uniformizer. Then for any $x \in K^\times$ there exists $n \in \mathbb{Z}$ and $u \in O_K^\times$ such that $x = \pi^n u$. In particular, $K = O_K\left[\frac{1}{x}\right]$ for any $x \in m$ and hence* $K = \operatorname{Frac} O_K$.

Proof. For any $x \in K^\times$, let n be such that $v(x) = v(\pi^n) = nv(\pi)$, then $v(x\pi^{-n}) = 0 \implies u = x\pi^{-n} \in O_K^\times$. □

Definition 2.8. *A ring R is called a* **discrete valuation ring (DVR)** *if it is a PID with exactly one non-zero prime ideal.*

Lemma 2.9.

1. *Let v be a discrete valuation on K. Then O_K is a DVR.*
2. *Let R be a DVR. Then there is a valuation v on $K := \mathrm{Frac}(R)$ such that $R = O_K$.*

Proof.

1. O_K is a PID by **2.6**. Let $0 \neq I \subseteq O_K$ be an ideal, then $I = (x)$ for some x. If $x = \pi^n u$ for π a uniformizer, then (x) is prime if and only if $n = 1$, and $I = (\pi) = m$.
2. Let R be a DVR with maximal ideal m. Then $m = (\pi)$ for some $\pi \in R$. Since PIDs are UFDs, we may write $x \in R \setminus \{0\}$ uniquely as $\pi^n u, n \geq 0, u \in R^\times$. Then any $y \in K \setminus \{0\}$ can be written uniquely as $\pi^m u, u \in R^\times, m \in \mathbb{Z}$. Then define $v(\pi^m u) = m$, and it is easy to check v is a valuation and $O_K = R$.

□

Examples:

- $\mathbb{Z}_{(p)}$ is a DVR, the valuation ring of $|\cdot|_p$ on $\mathbb{Q}$.
- $k[[t]]$ is a DVR, the valuation ring of the t-adic valuation on $k((t))$.
- $K = k(t), K' = K\left(t^{\frac{1}{2}}, t^{\frac{1}{4}}, t^{\frac{1}{8}}, \ldots\right)$. The t-adic valuation extends to K', but we must have $v(t^{\frac{1}{2^n}}) = \frac{1}{2^n}$, which is not discrete.

3 The p-adic Numbers

Recall that $\mathbb{Q}_p$ is defined to be the completion of $\mathbb{Q}$ with respect to the metric induced by $|\cdot|_p$. On example sheet 1, we prove that $\mathbb{Q}_p$ is a field. $|\cdot|_p$ extends from $\mathbb{Q}$ to $\mathbb{Q}_p$, and the associated valuation is discrete, so $\mathbb{Q}_p$ is a discretely valued field.

Definition 3.1. *The* **ring of p-adic integers**, *$\mathbb{Z}_p$, is the valuation ring $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.*

$\mathbb{Z}_p$ is a discrete valuation ring with maximal ideal $p\mathbb{Z}_p$, and all non-zero ideals in $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$ for $n \in \mathbb{N}$.

Proposition 3.2. *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. In particular, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$.*

Proof. We need to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. We know that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Since $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is a closed ball and hence open, $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$.

$$\begin{aligned}\mathbb{Z}_p \cap \mathbb{Q} &= \{x \in \mathbb{Q} : |x|_p \leq 1\} \\ &= \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid b\right\} \\ &= \mathbb{Z}_{(p)}\end{aligned}$$

Thus it suffices to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$.

Let $\frac{a}{b} \in \mathbb{Z}_{(p)}$, so that $a, b \in \mathbb{Z}, p \nmid b$. For $n \in \mathbb{N}$, choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \mod p^n$. Then $y_n \to \frac{a}{b}$ as $n \to \infty$.

In particular, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ which is complete. □

3.1 Brief Digression on Inverse Limits

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings together with homomorphisms $\varphi_n : A_{n+1} \to A_n$, called transition maps. The ***inverse limit*** of $(A_n)_{n=1}^{\infty}$ is the set of sequences of elements given by:

$$\varprojlim_n A_n = \left\{(a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} A_n : \varphi_n(a_{n+1}) = a_n\right\}$$

so that $a_{n+1} \xmapsto{\varphi_n} a_n \xmapsto{\varphi_{n-1}} a_{n-1}$. If the A_n are groups/rings, then $\varprojlim_n A_n$ is a group/ring respectively.

Let $\theta_m : \varinjlim_n A_n \to A_m$ denote the natural projection map.

The inverse limit satisfies the following universal property:

Proposition 3.3. *Let $((A_n)_{n=1}^{\infty}, (\varphi_n)_{n=1}^{\infty})$ as above. Then for any set/group/ring B together with homomorphisms $\psi_n : B \to A_n$ such that the diagram*

$$\begin{tikzcd} B \arrow[r, "\psi_{n+1}"] \arrow[dr, "\psi_n"'] & A_{n+1} \arrow[d, "\varphi_n"] \\ & A_n \end{tikzcd}$$

commutes for all n, there is a unique homomorphism $\psi : B \to \varprojlim_n A_n$ such that $\theta_n \circ \psi = \psi_n$.

Proof. Define $\psi : B \to \prod_{n=1}^{\infty} A_n$ by $b \mapsto \prod_{n=1}^{\infty}\{\psi_n(b)\}$.

Then $\psi_n = \varphi_n \circ \psi_{n+1} \implies \psi(b) \in \varprojlim_n A_n$.

This map is clearly unique, as it is determined by $\psi_n = \varphi_n \circ \psi_{n+1}$, and is a homomorphism of rings. □

Definition 3.4. *Let R be a ring and $I \subseteq R$ an ideal. The* **I-adic completion of R** *is the ring $\widehat{R} := \varprojlim_n R/I^n$, where $\varphi_n : R/I^{n+1} \to R/I^n$ is the natural projection.*

Note that there is a natural map $i : R \longrightarrow \widehat{R}$ by the universal property. We say that R is I-adically complete if i is an isomorphism.

As a fact, $\ker(i : R \longrightarrow \widehat{R}) = \bigcap_{n=1}^{\infty} I^n$.

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

Proposition 3.5. *Assume that K is complete. Then:*

1. $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$, *i.e. $\mathcal{O}_K$ is π-adically complete.*
2. *If in addition K is discretely valued and π is a uniformizer, then every element $x \in \mathcal{O}_K$ can be written uniquely as $x = \sum_{i=0}^{\infty} a_i\pi^i$ for $a_i \in A$ where A is a set of coset representatives for $k := \mathcal{O}_K/\pi\mathcal{O}_K$.*

   Moreover, any series $\sum_{i=0}^{\infty} a_i\pi^i$ converges in $\mathcal{O}_K$.

Proof.

1. There is a natural map $i : \mathcal{O}_K \longrightarrow \varprojlim_n \mathcal{O}_K/\pi\mathcal{O}_K$. Since $\bigcap_{n=1}^{\infty} \pi^n\mathcal{O}_K = \{0\}$, i is injective. Now let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$, and for each n choose $y_n \in \mathcal{O}_K$ a lift of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$.

   Let v be the valuation on K normalised such that $v(\pi) = 1$, then $v(y_n - y_{n+1}) \geq n$, as $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$.

   So $(y_n)_{n=1}^{\infty}$ is a Cauchy sequence in $\mathcal{O}_K$, but $\mathcal{O}_K$ is complete as $\mathcal{O}_K \subseteq K$ is closed, and we assumed K complete.

   So $y_n \longrightarrow y$ and $i(y) = (x_n)_{n=1}^{\infty}$, so i is surjective, and hence an isomorphism.
2. Let $x \in \mathcal{O}_K$. Choose a_i inductively as follows:

   Choose $a_0 \in A$ such that $a_0 \equiv x \mod \pi\mathcal{O}_K$. Suppose we have chosen $a_0, \ldots, a_k$ such that $\sum_{i=0}^{k} a_i\pi^i \equiv x \mod \pi^{k+1}$, Then $a_i\pi^i - x = c\pi^{k+1}$ for some $c \in \mathcal{O}_K$. Then choose $a_{k+1} \equiv c \mod \pi\mathcal{O}_K$.

   Then $\sum_{i=0}^{k+1} a_i \equiv x \mod \pi^{k+2}\mathcal{O}_K$, and so $\sum_{i=0}^{\infty} a_i = x$.

   For uniqueness, assume that $\sum_{i=0}^{\infty} a_i\pi^i = \sum_{i=0}^{\infty} b_i\pi^i \in \mathcal{O}_K$. Let n be minimal such that $a_n \neq b_n$. Then $\sum_{i=0}^{\infty} a_i \not\equiv \sum_{i=0}^{\infty} b_i\pi^i \mod \pi^{n+1}$ $\lightning$.

   For the moreover part, any series of this form defines a Cauchy sequence, which as in *1* converges in $\mathcal{O}_K$.

□

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

Corollary 3.6. *If K is as in 2 of **3.5**, then every $x \in K$ can be written uniquely as a series of the form $\sum_{i=n}^{\infty} a_i\pi^i$, $a_i \in A$. Conversely, any such expression defines an element of K.*

Proof. Use the fact that $K = \mathcal{O}_K\left[\frac{1}{\pi}\right]$. □

Corollary 3.7.

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

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

Proof.

1. By **3.5** it is sufficient to show that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Note that there is a natural map $f_n : \mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$, since $\mathbb{Z} \subseteq \mathbb{Z}_p$.

   We have that $\ker f_n = \{x \in \mathbb{Z} : |x|_p \le p^{-n}\} = p^n\mathbb{Z}$.

   Hence, $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$ is injective.

   For surjectivity, let $\bar{c} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, and $c \in \mathbb{Z}_p$ a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we can choose $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$. This is a closed ball and hence open, so $f_n(x) = \bar{c}$, and the map is surjective.

2. Follows from **3.6**, noting that $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ by *1*.

□

Examples:

- $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \ldots \in \mathbb{Q}_p$.
- Let $K = k((t))$ with the t-adic valuation. Then $\mathcal{O}_K = k[[t]] = \varprojlim_n k[[t]]/(t^n)$. Moreover, $\mathcal{O}_K$ is the t-adic completion of $k[t]$.

4 Complete Valued Fields

4.1 Hensel's Lemma

For complete valued fields, there is a nice way to produce solutions in $\mathcal{O}_K$ to certain equations from the solutions mod m.

Given $f \in R[x]$ for some ring R, we will denote by f' the ***formal derivative*** of f, which is the image of f under the linear map taking $x^n \mapsto nx^{n-1}$.

Theorem 4.1 (Hensel's Lemma, version 1)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) \in \mathcal{O}_K[x]$, and assume there exists $a \in \mathcal{O}_K$ 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 $(x_n)_{n=1}^{\infty}$ in $\mathcal{O}_K$ such that:

(i) $f(x_n) \equiv 0 \mod \pi^{n+2r}$

(ii) $x_{n+1} \equiv x_n \mod \pi^{n+r}$

Take $x_1 = a$; then $f(x_1) \equiv 0 \mod \pi^{1+2r}$.

Suppose we've constructed $x_1, \ldots, x_n$ satisfying (i) and (ii). Define $x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)}$. Since $x_n \equiv x_1 \mod \pi^{r+1}$, $v(f'(x_n)) = r$, and hence $\frac{f(x_n)}{f'(x_n)} \equiv 0 \mod \pi^{n+r}$ by (i).

It follows that $x_{n+1} \equiv x_n \mod \pi^{n+r}$, so (ii) holds.

Note that for x, y indeterminates, $f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \ldots$, where $f_i(x) \in O_K[x]$, and $f_0(x) = f(x)$, $f_1(x) = f'(x)$.

Thus $f(x_{n+1}) = f(x_n) + f'(x_n)c + f_2(x_n)c^2 + \ldots$, where $c = -\frac{f(x_n)}{f'(x_n)} \equiv 0 \mod \pi^{n+r}$. Then since $v(f_i(x_n)) \geq 0$, we have $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \mod \pi^{n+2r+1}$, and so (i) holds.

This gives a construction of $(x_n)_{n=1}^{\infty}$. Property (ii) implies our sequence is Cauchy, so by completeness it converges to $x \in O_K$. Then $f(x) = \lim_{n\to\infty} f(x_n) = 0$, which is zero by (i).

Moreover, (ii) implies:

$$\begin{aligned} a = x_1 \equiv x_n &\mod \pi^{r+1} \ \forall n \\ \implies a \equiv x &\mod \pi^{r+1} \\ \implies |x - a| &< |f'(a)| \end{aligned}$$

This proves existence.

For uniqueness, suppose x' also satisfies $f(x') = 0$, $|x' - a| < |f'(a)|$. Let $\delta = |x' - x| \gneq 0$.

Then $|x' - a| < |f'(a)|$, $|x - a| < |f'(a)|$, and the ultrametric inequality implies:

$$|\delta| = |x - x'| < |f'(a)| = |f'(x)|$$

But $0 = f(x') = f(x+\delta) = f(x) + f'(x) + \delta + \ldots$, where absolute value of the higher order terms is $\leq |\delta|^2$.

Hence $|f'(x)\delta| \leq |\delta|^2 \implies |f'(x)| \leq |\delta| \lightning$. □

The following corollary is a slightly weaker result, but will often turn out to be more useful for what we want to do.

Corollary 4.2. *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) \in O_K[x]$, and $\bar{c} \in k := O_K/m$ a simple root of $\bar{f}(x) := f(x) \mod m \in k[x]$ (i.e. not a root of $\bar{f}'(x)$).*

Then there is a unique $x \in O_K$ such that $f(x) = 0$ and $x \equiv \bar{c} \mod m$.

Proof. Apply **4.1** to a lift $c \in O_K$ of $\bar{c}$. Then $|f(c)| < |f'(c)|^2 = 1$, since $\bar{c}$ is a simple root. □

Example: $f(x) = x^2 - 2$ has a simple root mod 7. Thus $\sqrt{2} \in \mathbb{Z}_7 \subseteq \mathbb{Q}_7$.

Corollary 4.3.

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

Proof.

$p > 2$: Let $b \in \mathbb{Z}_p^\times$. By **4.2** applied to $f(x) = x^2 - b$, we have $b \in (\mathbb{Z}_p^\times)^2$ if and only if $b \in (\mathbb{F}_p^\times)^2$.

Thus $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$, since $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

We have an isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \cong \mathbb{Q}_p^\times$, given by $(u, n) \mapsto u\pi^n$.

Thus $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$.

$\underline{p = 2}$: Let $b \in \mathbb{Z}_2^\times$. Consider $f(x) = x^2 - b$. Then $f'(x) = 2x \equiv 0 \mod 2$, so we can't use **4.1**.

Let $b \equiv 1 \mod 8$. Then $|f(1)|_2 \leq 2^{-3} < |f'(1)|_2^2 = 2^{-2}$. So by Hensel's lemma, $f(x)$ has a root in $\mathbb{Z}_2$.

Hence $b \in (\mathbb{Z}_p^\times)^2 \iff b \equiv 1 \mod 8$. So $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \equiv (\mathbb{Z}/8\mathbb{Z})^\times \equiv (\mathbb{Z}/2\mathbb{Z})^2$. Again, using $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$, we find that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$.

□

The proof of Hensel's lemma uses the iteration $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, which is the same iteration as used in the Newton-Raphson method for functions on the real numbers. In this case however we can do one better, as Hensel's lemma lets us know when the iteration will converge.

For later applications, we will need the following version of Hensel's lemma:

Theorem 4.4 (Hensel's Lemma, version 2)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field, and $f(x) \in \mathcal{O}_K[x]$, and suppose that $\bar{f}(x) := f(x) \mod m \in k[x]$ factorises as:*

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x)$$

with $\bar{g}(x), \bar{h}(x)$ coprime.

Then there is a factorisation $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$, with $g(x) \equiv \bar{g}(x) \mod m, \bar{h}(x) \equiv h(x)$ $\mod m$*, and* $\deg \bar{g} = \deg g$.

Proof. Example sheet 1. □

Corollary 4.5. *Let $f(x) = a_n x^n + \ldots + a_0 \in K[x]$ with $a_0, a_n \neq 0$. If $f(x)$ is irreducible, then $|a_i| \leq \max\{|a_0|, |a_n|\}$ for all i.*

Proof. Upon scaling, we may assume $f(x) \in \mathcal{O}_K[x]$ with $\max_i\{|a_i|\} = 1$. Thus we need to show that $\max\{|a_0|, |a_1|\} = 1$. If not, let r be minimal such that $|a_r| = 1$, then $0 < r < n$. Thus we have $\bar{f}(x) = x^r(a_r + \ldots a_n x^{n-r}) \mod m$.

Then **4.5** tells us this factorisation lifts to a factorisation in $\mathcal{O}_K[x]$, which is a contradiction. □

5 Teichmüller Lifts

Recall that every element of $\mathbb{Q}_p$ can be written as $x = \sum_{i=n}^{\infty} a_i p^i$, where $a_i \in \{0, \ldots, p-1\} =: A$.

We chose this set A since we found that we needed coset representatives for $\mathbb{F}_p \leq \mathbb{Z}_p$. However, this choice of A doesn't respect any of the algebraic structure on $\mathbb{Z}_p$.

It turns out there is a natural choice of coset representatives in many cases which does respect some algebraic structure.

Definition 5.1. *A ring R of characteristic p is* **perfect** *if the Frobenius map* Frob : $x \mapsto x^p$ *is an automorphism of R. A field of characteristic p is perfect if it is perfect as a ring.*

Note that since $\operatorname{char} R = p$, $(x + y)^p = x^p + y^p$, so the Frobenius map is a ring homomorphism, so all that is needed is that it is bijective.

Examples:

1. $\mathbb{F}_p$ and $\bar{\mathbb{F}}_p$ are perfect fields.
2. $\mathbb{F}_p[t]$ is not perfect - $t \notin \text{im(Frob)}$.
3. $\mathbb{F}_p\left(t^{1/p^\infty}\right) := \mathbb{F}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$ is a perfect field. This is the smallest perfect field containing $\mathbb{F}_p(t)$, so we call it the ***perfection*** of $\mathbb{F}_p(t)$. The t-adic absolute value extends to $\mathbb{F}_p(t^{1/p^\infty})$, and the completion of $\mathbb{F}_p(t^{1/p^\infty})$ is called a ***perfectoid field***. These were the subject of Peter Scholze's PhD thesis.

Fact: a field k is perfect if and only if any finite extension of k is separable.

Theorem 5.2. *Let $(K, |\cdot|)$ be a complete discretely valued field such that $k := O_K/m$ is a perfect field of characteristic p. Then there is a unique map*

$$[\cdot] : k \to O_K$$

such that:

1. *$a \equiv [a] \mod m$ for all $a \in k$.*
2. *$[ab] \equiv [a][b]$ for all $a, b \in k$.*

Moreover, if $\text{char}\, O_K = p$*, then $[\cdot]$ is a ring homomorphism.*

Definition 5.3. *The element $[a] \in O_K$ constructed in* **5.2** *is called the* **Teichmüller lift** *of a.*

The idea of the proof of this theorem is that, if $\alpha \in O_K$ be a lift of $a \in k$. α is well defined then up to the ideal πO_K (where π is a uniformizer).

Then let $\beta \in O_K$ be a lift of $a^{1/p}$; we claim that β is a "better" lift:

Let $\beta' \in O_k$ be another lift of $a^{1/p}$. Then $\beta = \beta' + \pi u, u \in O_K$, and so $\beta^p = \beta'^p + \sum_{i=1}^{\infty} \binom{p}{i} \beta'^i (\pi u))^{p-i}$. Since $p \in \pi$, this sum term lies in $\pi^2 O_K$, and so β is well defined up to $\pi^2 O_K$.

The idea is then to repeat this process, getting a sequence of better and better lifts each time, which will converge to a "canonical" lift. To do this rigorously we'll need the following lemma:

Lemma 5.4. *Let $(K, |\cdot|)$ be as in* **5.3***, and fix $\pi \in O_K$ a uniformizer. Let $x, y \in O_K$ such that $x \equiv y \mod \pi^k$, for $k \geq 1$. Then $x^p \equiv y^p \mod \pi^{k+1}$.*

Proof. Let $x = y + u\pi^k$. Then:

$$\begin{aligned} x^p &= \sum_{i=0}^{p} \binom{p}{i} y^i (u\pi^k)^{p-i} \\ &= y^p + pu\pi^k y^{p-1} + \sum_{i=2}^{p} \binom{p}{i} y^i (u\pi^k)^{p-i} \quad \text{for } p > 2 \end{aligned}$$

Since $O_K/\pi O_K$ is of characteristic p, we have $p \in (\pi)$. Thus $pu\pi^k y^{p-1} \in \pi^{k+1} O_K$. Additionally, for $i \geq 2$, $(u\pi^k)^i \in \pi^{k+1} O_K$.

Hence $x^p \equiv y^p \mod \pi^{k+1}$. □

*Proof of **Theorem 5.2**.* 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:

$$x_i := y_i^{p^i}$$

Then $x_i \equiv y_i^{p^i} \equiv \left(a_i^{1/p^i}\right)^{p^i} \equiv a \mod \pi$.

We then claim that $(x_i)_{i=1}^{\infty}$ is a Cauchy sequence, and that its limit $x_i \to x$ is independent of the choice of y_i.

By construction, $y_i \equiv y_{i+1}^p \mod \pi$. By **5.4** and using induction on k, we have $y_i^{p^k} \equiv y_{i+1}^{p^{k+1}} \mod \pi^{k+1}$, and hence $x_i \equiv x_{i+1} \mod \pi^{i+1}$, and so the sequence is Cauchy, so converges in $\mathcal{O}_K$ to some x.

Suppose we had chosen different y_is, getting a different sequence $(x_i')_{i=1}^{\infty}$. Then $x_i' \to x' \in \mathcal{O}_K$.

Then let $(x_i'')_{i=1}^{\infty} = \begin{cases} x_i & i \text{ even} \\ x_i' & i \text{ odd} \end{cases}$. Then (x_i'') is also Cauchy, and has convergent subesquences to x and x', so $x = x'$, and our choice of y_i didn't matter.

We then define $[a] = x$.

$x \equiv a \mod \pi$, so the first condition is satisfied.

For the second condition, 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 $\lim_{i\to\infty} z_i = [b]$.

Now $u_i y_i$ is a lift of $(ab)^{1/p^i}$, hence $[ab] = \lim\limits_{i\to\infty} x_i z_i = \lim\limits_{i\to\infty} x_i \lim\limits_{i\to\infty} z_i = [a][b]$.

If char $\mathcal{O}_K = p$, then $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$ (raise both sides to p^i and use perfectness $\implies$ bijectivity of Frob). Then we have:

$$\begin{aligned}
[a+b] &= \lim_{i\to\infty} (y_i + u_i)^{p^i} \\
&= \lim_{i\to\infty} y_i^{p^i} + u_i^{p^i} \\
&= \lim_{i\to\infty} x_i + z_i \\
&= [a] + [b]
\end{aligned}$$

It is easy to check that $[0] = 0, [1] = 1$, and so $[\cdot]$ is a ring homomorphism.

For uniqueness, let $\phi : k \to \mathcal{O}_K$ be another such map. Then for $a \in k$, $\phi(a^{1/p^i})$ is a lift a^{1/p^i}. It follows that:

$$[a] = \lim_{i\to\infty} \phi(a^{1/p^i})^{p^i} = \lim_{i\to\infty} \phi(a) = \phi(a)$$

□

<u>Example:</u> $K = \mathbb{Q}_p$, then $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$. For $a \in \mathbb{F}_p^{\times}$, $[a]^{p-1} = [a^{p-1}] = [1] = 1$, and so $[a]$ is a $(p-1)^{\text{th}}$ root of unity. More generally:

Lemma 5.6. *Let $(K, |\cdot|)$ be a complete discretely valued field. If $k := \mathcal{O}_K/m \subseteq \mathbb{F}_p$, then $[a] \in \mathcal{O}_K^{\times}$ is a root of unity.*

Proof. $a \in k \implies a \in \mathbb{F}_{p^n}$ for some n, so $[a]^{p^n-1} = [1] = 1$. □

Theorem 5.7. *Let $(K, |\cdot|)$ be a complete discretely valued field with* $\operatorname{char} K = p > 0$. *Then $K \cong k((t))$.*

Proof. Since $K = \operatorname{Frac}(O_K)$, it suffices to show that $O_K \cong k[[t]]$. Fix $\pi \in O_K$ a uniformizer, and let $[\cdot] : k \to O_K$ be the Teichmüller map, and define:

$$\varphi : k[[t]] \to O_K$$
$$\sum_{i=0}^{\infty} a_i t^i = \sum_{i=0}^{\infty} [a_i] \pi^i$$

Then φ is a ring homomorphism since $[\cdot]$ is, and it is a bijection by **3.5**. □

6 Extensions of Complete Valued Fields

Theorem 6.1. *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*

$$|y|_L = |N_{L/K}(y)|^{\frac{1}{n}} \ \forall y \in L$$

2. *L is complete with respect to $|\cdot|_L$.*

Recall that if L/K is finite then $N_{L/K} : L \to K$ is defined by $N_{L/K} = \operatorname{Det}_K(\operatorname{mult}_y)$, where mult_y is the K-linear map induced by multiplication by y.

We have also that:

- $N_{L/K}(xy) = N_{L/K}(x) N_{L/K}(y)$
- If $x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$ is the minimal polynomial of $y \in L$, then $N_{L/K}(y) = a_0^m$ for some $m \geq 1$.

Note that the n^{th} root is not necessary for $|\cdot|_L$ to be an absolute value, but is necessary for it to extend $|\cdot|$, as for $x \in K$, $N_{L/K}(x) = \operatorname{Det} \operatorname{diag}(x, x, \ldots, x) = x^n$.

We will spend this section proving **6.1**.

Definition 6.2. *Let $(K, |\cdot|)$ be a non-archimedean valued field, and V a vector space over K. A norm on V is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ satisfying:*

1. $\|x\| = 0 \iff x = 0$
2. $\|\lambda x\| = |\lambda| \|x\| \ \forall \lambda \in K, x \in V$
3. $\|x + y\| \leq \max(\|x\|, \|y\|)$

For example, if V is finite dimensional and $e_1, \ldots, e_n$ is a basis of V. The sup norm on V is defined by

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

where $x = \sum_{i=1}^n x_i e_i$. As an exercise, show $\|\cdot\|_{\sup}$ is a norm.

Definition 6.3. *Two norms $\|\cdot\|_1, \|\cdot\|_2$ are equivalent if there are $C, D > 0$ such that*

$$C\|x\|_1 \leq \|x\|_2 \leq D\|x\|_1 \ \forall x \in V$$

A norm defines a metric on V, and hence a topology, and equivalent norms induce the same topology.

Proposition 6.4. *Let $(K, |\cdot|)$ be complete and non-archimedean, and V be a finite dimensional vector space over K. Then V is complete with respect to $\|\cdot\|_{\sup}$.*

Proof. Let $(v_i)_{i=1}^{\infty}$ be a Cauchy sequence in V, and let $e_1, \ldots, e_n$ be a basis for V. Write $v_1 = \sum_{j=1}^{n} x_j^i e_j$; then $(x_j^i)_{i=1}^{\infty}$ is a Cauchy sequence in K.

Let $x_j^i \to x_j \in K$, then $v_i \to v = \sum_{i=1}^{n} x_j e_j$. □

Theorem 6.5. *Let $(K, |\cdot|)$ be complete and non-archimedean, and V a finite dimensional vector space over K. Then any two norms on V are equivalent. In particular, V is complete with respect to any norm.*

Proof. Since equivalence defines an equivalence relation on a set of norms, it suffices to show that any norm is equivalent to $\|\cdot\|_{\sup}$.

Let $e_1, \ldots, e_n$ be a basis for V, and set $D := \max_i \|e_i\|$.

Then for $x = \sum_{i=1}^{n} x_i e_i$, we have

$$\begin{aligned}
\|x\| &\leq \max_i \|x_i e_i\| \\
&= \max_i |x_i| \|e_i\| \\
&\leq D \max_i |x_i| \\
&= D\|x\|_{\sup}
\end{aligned}$$

To find C such that $C\|\cdot\|_{\sup} \leq \|\cdot\|$, we induct on $n = \dim V$.

If $n = 1$, then $\|x\| = \|x_1 e_1\| = |x_1| \|e_1\|$, so take $C = \|e_1\|$.

Then for $n > 1$, for each i, define $V_i := \operatorname{Span}\langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n \rangle$.

By induction, V_i is complete with respect to $\|\cdot\|$ and hence closed. Then $e_i + V_i$ is also closed for all i, and hence $S := \bigcup_{i=1}^{n} e_i + V_i$ is a closed subset not containing 0.

Thus there is $C > 0$ such that $B(0, C) \cap S = \emptyset$.

Let $x = \sum_{i=1}^{n} x_i e_i$, and suppose $|x_j| = \max_i |x_i|$. Then $\|x\|_{\sup} = |x_j|$, and moreover, $\frac{1}{x_j} x \in S$.

So $\|\frac{1}{x_j} x\| \geq C, so \|x\| \geq C|x_j| = C\|x\|_{\sup}$.

The completeness of V follows since V is complete with respect to $\|\cdot\|_{\sup}$. □

Definition 6.6. *Let $R \subseteq S$ be rings. We say $s \in S$ is* **integral** *over R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(s) = 0$. The* **integral closure** *$R^{\operatorname{int}(S)}$ of R inside S is defined to be*

$$R^{\operatorname{int}(S)} = \{s \in S : s \text{ integral over } R\}$$

We say R is integrally closed in S if $R^{\mathrm{int}(S)} = R$.

Proposition 6.7. *$R^{\mathrm{int}(S)}$ is a subring of S. Moreover, $R^{\mathrm{int}(S)}$ is integrally closed in S.*

Proof. Example sheet 2. □

Lemma 6.8. *Let $(K, |\cdot|)$ be a non-archimedean valued field. Then O_K is integrally closed in K.*

Proof. Let $x \in K$ be integral over O_K, and without loss of generality $x \neq 0$.

Then let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in O_K[x]$ such that $f(x) = 0$. Then:

$$1 = -\frac{1}{x}a_{n-1} - a_{n-2}\frac{1}{x^2} - \ldots - a_0\frac{1}{x^n}$$

If $|x| > 1$, we have $1 = |1| = |-\frac{1}{x}a_{n-1} - \ldots - a_0\frac{1}{x^n}| < 1 ↯$.

But then $|x| \leq 1$, so $x \in O_K$. □

Proof of Theorem 6.1. We show $|\cdot|_L = |N_{L/K}(\cdot)|$ satisfies the three axioms in the definition of absolute values.

1.

$$\begin{aligned} |y|_L = 0 &\iff |N_{L/K}(y)| = 0 \\ &\iff N_{L/K}(y) = 0 \\ &\iff y = 0 \end{aligned}$$

2.

$$\begin{aligned} |y_1y_2|_L &= |N_{L/K}(y_1y_2)|^{1/n} \\ &= |N_{L/K}(y_1y_2)|^{1/n} \\ &= |N_{L/K}(y_1)N_{L/K}(y_2)|^{1/n} \\ &= |N_{L/K}(y_1)|^{1/n}|N_{L/K}(y_2)|^{1/n} \\ &= |y_1|_L|y_2|_L \end{aligned}$$

3. Set $O_L = \{y \in L : \|y\|_L \leq 1\}$. We then claim that O_L is the integral closure of O_K inside L.

   To see this let $0 \neq y \in O_L$, we want to show that y is integral over O_K. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$ be the minimal polynomial of y. Then there is $m \geq 1$ with $N_{L/K}(y) = a_0^m$.

   By **4.5**, since f is irreducible, the coefficient with the largest absolute value is either the first or the last in f. I.e.:

   $$|a_i| \leq \max(|N_{L/K}(y)^{1/m}|, 1) =$$

   Now, since $|N_{L/K}(y)| \leq 1$, we have $|a_i| \leq 1$, i.e. $a_i \in O_K$.

   Hence $f \in O_K[x]$, and y is integral over O_K.

Conversely, let $y \in L$ be integral over O_K. Then $N_{L/K}(y) = \left(\prod_{\sigma:L\to\bar{K}} \sigma(y)\right)^d$ for some $d \geq 1$, where $\bar{K}$ is an algebraic closure of K and σ runs over all K-algebra homomorphisms.

For all such $\sigma : L \longrightarrow \bar{K}$, $\sigma(y)$ satisfies the same monic polynomials as y, so is also integral over O_K. Thus $N_{L/K}(y) \in K$ is integral over O_K, and hence $N_{L/K}(y) \in O_K$.

But then $|N_{L/K}(y)| \leq 1$, and so $y \in O_L$, so $O_K^{\mathrm{int}(L)} = O_L$, and the claim is proved.

Now let $x, y \in L$. Without loss of generality, assume that $|x|_L \leq |y|_L$. Then $|\frac{x}{y}|_L \leq 1$, and so $\frac{x}{y} \in O_L$.

Since $1 \in O_L$ and $O_K^{\mathrm{int}(L)}$, we have $1 + \frac{x}{y} \in O_L$, and hence $|1 + \frac{x}{y}| \leq 1$, i.e., $|x + y| \leq |y| = \max(|y|_L, |x|_L)$ as required.

For uniqueness, suppose $|\cdot|'_L$ is another absolute value on L extending $|\cdot|$, then note that $|\cdot|_L, |\cdot|'_L$ are norms on L, hence induce the same topology on L, hence are equivalent, hence $|\cdot|'_L = |\cdot|_L^c$ for some $c > 0$. Since they agree on K, $c = 1$.

For the completeness part, since $|\cdot|_L$ defines a norm on K, **6.5** implies that L is complete with respect to $|\cdot|_L$. □

Corollary 6.9. *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field, and L/K a finite extension. Then*

1. *L is discretely valued with respect to $|\cdot|_L$.*
2. *O_L is the integral closure of O_K in L.*

Proof.

1. Let v be the valuation on K, v_L the valuation on L such that v_L extends v, and let $n = [L : K]$.

   Then for $y \in L^\times$, $|y|_L = |N_{L/K}(y)|^{1/n}$.

   Hence $v_L(y) = \frac{1}{n}v(N_{L/K}(y))$, and so $v_L(L^\times) \subseteq \frac{1}{n}v(K^\times)$, hence v_L is discrete.
2. Proved in the previous section.

□

Corollary 6.10. *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field, and $\bar{K}/K$ an algebraic closure of K. Then $|\cdot|$ extends to a unique absolute value $|\cdot|_{\bar{K}}$ on $\bar{K}$.*

Proof. Let $x \in \bar{K}$. Then x is algebraic over K, so $x \in L$ for some L/K finite. Define $|x|_{\bar{K}} = |x|_L$. This is well defined, i.e. is independent of L by the uniqueness proven in **6.1**. The axioms for $|\cdot|_{\bar{K}}$ to be an absolute value can be checked over finite extensions, as can uniqueness. □

N.B.: $|\cdot|_{\bar{K}}$ is *never* discrete. Take $x \in K, |x| = 1$ (e.g. $p \in \mathbb{Q}_p$). Then for all $n \geq 0, v_{\bar{K}}(\sqrt[n]{x}) = \frac{1}{n}$, which can get arbitrarily close to zero as x has all its roots in $\bar{K}$.

7 Local Fields

Definition 7.1. *Let $(K, |\cdot|)$ be a valued field. Then we say K is a* **local field** *if it is complete and locally compact.*

For example, $\mathbb{R}$ and $\mathbb{C}$ are local fields.

Proposition 7.2. *Let $(K, |\cdot|)$ be a non-archimedean complete valued field. Then the following are equivalent:*

1. *K is locally compact.*
2. *O_K is compact.*
3. *v is discrete and $k := O_K/m$ is finite.*

Proof.

1. $\implies$ 2. Let $U \ni 0$ be a compact neighbourhood of 0. Then $\exists\ x \in O_K$ such that $xO_K \subseteq U$. Since xO_K is closed, xO_K is compact, and hence O_K is compact, as there is a homeomorphism $xO_K \xrightarrow{x^{-1}} O_K$.

2. $\implies$ 1. O_K is compact, so $a + O_K$ is compact for all $a \in K$, and hence K is locally compact as every $a \in K$ has compact neighbourhood $a + O_K$.

2. $\implies$ 3. Let $x \in m$, and $A_x \subseteq O_K$ be a set of coset representatives for O_K/xO_K.

Then $O_K = \bigcup_{y \in A_x} y + xO_K$, which is a disjoint union of open subsets, and hence an irreducible open cover. So by compactness, A_x is finite. So O_K/m, which is a quotient of O_K/xO_K, is finite.

Now suppose that v is not discrete. Let $x = x_1, x_2, x_3, \ldots$ be a sequence such that

$$v(x_1) > v(x_2) > v(x_3) > \ldots > 0$$

Then we have

$$xO_K \subsetneq x_2O_K \subsetneq x_3O_K \subsetneq \ldots \subsetneq O_K$$

But O_K/xO_K is finite, so can only have finitely many subgroups as an additive group $\lightning$.

Hence v must be discrete.

3. $\implies$ 2. Since O_K is a metric space, it suffices to show O_K is sequentially compact. Let $(x_n)_{n=1}^{\infty}$ be a sequence in O_K and fix $\pi \in O_K$ a uniformizer.

Then since $\pi^i O_K/\pi^{i+1}O_K \cong k, O_K/\pi^i O_K$ is finite, as $O_K \supseteq \pi O_k \supseteq \ldots \supseteq \pi^i O_K$, and each quotient is finite, hence the total quotient is finite.

Since $O_K/\pi O_K$ is finite, there is some $a \in O_K/\pi O_K$ and a subsequence $(x_{1,n})_{n=1}^{\infty}$ such that $x_{1,n} \equiv a \mod \pi$.

Define $y_1 = x_{1,1}$.

Since $O_K/\pi^2 O_K$ is finite, there is some $a_2 \in O_K/\pi^2 O_K$ and a subsequence $(x_{2,n})_{n=1}^{\infty}$ such that $x_{2,n} \equiv a_2 \mod \pi^2 O_K$.

Define $y_2 = x_{2,2}$.

Continuing in this fashion, we get the sequences $(x_{i,n})_{n=1}^{\infty}$ for $i = 1, 2, \ldots$, such that $(x_{i+1,n})_{n=1}^{\infty}$ is a subsequence of $(x_{i,n})_{n=1}^{\infty}$, and, for any i, there is some $a_i \in \mathcal{O}_K/\pi^i\mathcal{O}_K$ with $x_{i,n} \equiv a_i \mod \pi^i$ for all n.

Then necessarily $a_i \equiv a_{i+1} \mod \pi^i$ for all i. With $y_i = x_{i,i}$, we have $y_i \equiv y_{i+1} \mod \pi^i$, and so y_i is Cauchy, and hence converges by completeness, and hence $\mathcal{O}_K$ is sequentially compact.

□

Examples:

1. $\mathbb{Q}_p$ is a local field.
2. $\mathbb{F}_p((t))$ is a local field.

7.1 More On Inverse Limits

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings and $\varphi_n : A_{n+1} \to A_n$ be homomorphisms.

Definition 7.3. *Assume A_n is finite for all n. Then the* **profinite topology** *on $A := \varprojlim_n A_n$ is the weakest topology on A such that $A \to A_n$ is continuous for all n, where A_n are equipped with the discrete topology.*

A with the profinite topology is then compact, totally disconnected, and Hausdorff.

Proposition 7.4. *Let $(K, |\cdot|)$ be a local field. Under the isomorphism*

$$\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$$

where π is a uniformizer, the topology on $\mathcal{O}_K$ induced via $|\cdot|$ coincides with the profinite topology.

Proof. Just need to check that, if

$$\mathcal{B} := \{a + \pi^n\mathcal{O}_K : n \in \mathbb{N}_{\geq 1}, a \in A_{\pi^n}\}$$

where A_{π^n} is a set of coset representatives for $\mathcal{O}_K/\pi^n\mathcal{O}_K$, then $\mathcal{B}$ is a basis of open sets in both topologies.

For $|\cdot|$, this is immediate.

For the profinite topology, $\mathcal{O}_K \to \mathcal{O}_K/\pi^n\mathcal{O}_K$ is continuous if and only if $a + \pi^n\mathcal{O}_K$ is open for all $a \in A_{\pi^n}$. Then $\mathcal{B}$ is a basis for the profinite topology. □

This gives another proof that $\mathcal{O}_K$ is compact.

8 Local Fields II

Lemma 8.1. *Let K be a non-archimedean local field and L/K a finite extension. Then L is a local field.*

Proof. **6.1** tells us that L is complete and discretely valued, so it suffices to show that $k_L := \mathcal{O}_L/m_L$ is finite.

Let $\alpha_1, \ldots, \alpha_n$ be a basis for L as a K-vector space. Then the supremum norm is equivalent to $|\cdot|_L$, and so there is some $r > 0$ such that

$$\mathcal{O}_L \subseteq \{x \in L : \|x\|_{\sup} \leq r\}$$

Take $a \in K$ such that $|a| \geq r$, then:

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

and so $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$-module, hence the residue field k_L is finitely generated over k. Since it is a finite extension of a finite field, k_L is finite, and so L is local. $\square$

Theorem 8.2 (Classification of Local Fields)**.** *Let K be a local field. Then either:*

1. $K \cong \mathbb{R}$ *or* $K \cong \mathbb{C}$
2. *K is a finite extension of* $\mathbb{Q}_p$
3. $K \cong \mathbb{F}_{p^n}((t))$ *for p prime, $n \geq 1$.*

We will aim to prove this over the following few pages.

Definition 8.3. *We say a discretely valued field $(K, |\cdot|)$ has* **equal characteristic** *if* $\operatorname{char}(K) = \operatorname{char}(k)$*. Otherwise we say it has* **mixed characteristic***.*

For example, $\operatorname{char}\mathbb{Q}_p = 0, \operatorname{char}\mathbb{F}_p = p$, so $\mathbb{Q}_p$ has mixed characteristic. Note that, if K is a local field, $\operatorname{char} k = p > 0$, and hence K has equal characteristic (respectively mixed) if $\operatorname{char} K = p$ (respectively $\operatorname{char} K = 0$).

Theorem 8.4. *Let K be a local field of equal characteristic $p > 0$. Then*

$$K \cong \mathbb{F}_{p^n}((t))$$

for some $\operatorname{char} K > 0$.

Proof. K is complete and discretely valued, with positive characteristic. Moreover, $k \cong \mathbb{F}_{p^n}$ is finite, hence perfect. By **5.7**, $K \cong \mathbb{F}_{p^n}((t))$. $\square$

8.1 Witt Vectors

This section is non-examinable.

Consider the ring $\mathbb{Z}_p$. Let $x = \sum_{i=0}^{\infty}[x_i]_{p^i}, y = \sum_{i=0}^{\infty}[y_i]p^i$ where $x_i, y_i \in \mathbb{F}_p, x, y \in \mathbb{Z}_p$.

Then, if $x + y = s = \sum_{i=0}^{\infty}[s_i]p^i$, we might ask if we can write s_i in terms of the x_j, y_j.

Reducing mod p, we obtain that $x_0 + y_0 = s_0 \in \mathbb{F}_p$, so s_0 is determined by x_0, y_0. What about s_1?

Reducing mod p^2, $[x_0] + [y_0] + p[x_1] + p[y_1] \equiv [s_0] + p[s_1] \mod p^2$.

Hence $p[s_1] \equiv ([x_0] + [y_0] - [s_0]) + p[x_1] + p[y_1] \mod p^2$.

So we need to compute $[x_0]+[y_0]-[s_0] \mod p^2$. Note that $[x_0^{1/p}]+[y_0^{1/p}] \equiv [s_0^{1/p}] \mod p$.
By lemma 5.4:

$$\begin{aligned}[s_0] &\equiv ([x_0^{1/p}] + [y_0^{1/p}])^p \mod p^2 \\ &\equiv [x_0] + [y_0] + \sum_{d=1}^{p-1} \binom{p}{d} [x_0^{d/p}][y_0^{(p-d)/p}] \mod p^2\end{aligned}$$

Hence s_1 is determined by x_0, y_0, x_1, y_1. This can be continued in a similar pattern for $s_2, s_3, \ldots$. Witt noticed the general pattern:

Definition 8.5. *The n^{th}* **Witt polynomial** *w_n is defined by:*

$$w_n(x_0, x_2, \ldots, x_n) = \sum_{i=0}^{n} p^i x^{p^{n-i}} \in \mathbb{Z}[x_0, x_1, \ldots, x_n]$$

Define $S_n \in \mathbb{Q}[x_0, y_0, \ldots, x_n, y_n]$ inductively by

$$w_n(S_0, \ldots, S_n) = w_n(x_0, \ldots, x_n) + w_n(y_0, \ldots, y_n)$$

Witt showed that $S_n \in \mathbb{Z}[x_0, y_0, \ldots, x_n, y_n]$. E.g.

- $S_0 = x_0 + y_0$
- $S_1 = x_1 + y_1 + \sum_{d=1}^{p-1} \frac{1}{p} \binom{p}{d} x_0^d y_0^{p-d}$

Theorem 8.6. *Suppose that*

$$\sum_{i=0}^{\infty}[x_i]p^i + \sum_{i=0}^{\infty}[y_i]p^i = \sum_{i=0}^{\infty}[s_i]p^i \in \mathbb{Z}_p$$

Then we have $s_n = S_n(x_0^{1/p^n}, y_0^{1/p^n}, x_1^{1/p^{n-1}}, y_1^{1/p^{n-1}}, \ldots, x_n, y_n)$.

Proof. Example sheet 2. Hint: Use lemma **5.4**. □

Similarly, define $Z_n \in \mathbb{Q}[x_0, y_0, \ldots, x_n, y_n]$ by

$$w_n(Z_0, \ldots, Z_n) = w_n(x_0, \ldots, x_n) w_n(y_0, \ldots, y_n)$$

Then again Witt showed $Z_n \in \mathbb{Z}[x_0, \ldots, x_n]$, and that

$$\sum_{i=0}^{\infty}[x_i]p^i \sum_{i=0}^{\infty}[y_i]p^i = \sum_{i=0}^{\infty}[z_i]p^i$$

where $z_n = Z_n(x_0^{1/p^n}, y_0^{1/p^n}, \ldots, x_n, y_n)$.

Conclusion: the ring structure on $\mathbb{Z}_p$ can be reconstructed from the arithmetic of $\mathbb{F}_p$.

Definition 8.7. *A ring A is a strict p-ring if it is p-adically complete, p is not a zero divisor in A, and A/pA is a perfect ring of characteristic p.*

Theorem 8.8 (Existence of Witt vectors)**.** *Let R be a perfect ring of characteristic p.*

1. *There exists a strict p-ring $W(R)$ called the* **Witt vectors** *of R such that $W(R)/pW(R) \cong R$, which is unique up to isomorphism.*
2. *If R' is another perfect ring and $f : R \to R'$ is a ring homomorphism, then there is a unique homomorphism $F : W(R) \to W(R')$ such that following diagram commutes*

$$\begin{tikzcd} W(R) \arrow[r, "F"] \arrow[d] & W(R') \arrow[d] \\ R \arrow[r, "f"] & R' \end{tikzcd}$$

$W(R)$ is sort of a mixed-characteristic analogue of $R[[t]]$, where p plays the role of t. (E.g. note that $R[[t]]/(t) \cong R$.)

Sketch proof. For a detailed proof, see Rabinoff: The Theory of Witt Vectors.

1. Define $W(R) = \{(a_i)_{i=0}^{\infty} : a_i \in R\}$, and define addition and multiplication by:

$$\begin{aligned} (a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty} &= (s_n)_{n=0}^{\infty} \\ (a_n)_{n=0}^{\infty}(b_n)_{n=0}^{\infty} &= (z_n)_{n=0}^{\infty} \end{aligned}$$

   where $s_n = S_n(a_0, \dots, b_n)$, $z_n = Z_n(a_0, \dots, b_n)$ are as above.

   Check that this defines a ring structure. For $a = (a_0, a_1, \dots) \in W(R)$, then $pa = (0, a_0^p, a_1^p, \dots)$, and so p is not a zero divisor.

   Moreover, $W(R)/p^iW(R) = \{(a_n)_{n=0}^{i} : a_n \in R\}$, the sequences of length i. We then compute explicitly $W(R) \cong \varprojlim_i W(R)/p^iW(R)$.

2. For $f : R \to R'$, define $F : W(R) \to W(R')$ by $F[a_0, a_1, \dots] = (f(a_0), f(a_1), \dots) \in W(R')$, and check this works.

□

If $R = \mathbb{F}_p$, then $W(\mathbb{F}_p) \cong \mathbb{Z}_p$, and the isomorphism is given by

$$(a_0, a_1, \dots) \mapsto \sum_{i=0}^{\infty} \left[a_i^{1/p^i}\right] p^i$$

Proposition 8.9. *Let $(K, |\cdot|)$ be a complete discretely valued field such that $p \in \mathcal{O}_K$ is a uniformizer and $k := \mathcal{O}_K/m$ is perfect. Then $\mathcal{O}_K \cong W(k)$.*

Proof. By uniqueness of $W(k)$, it suffices to prove that $\mathcal{O}_K$ is a strict p-ring. This is clear from properties of $\mathcal{O}_K$. □

If k is a perfect field, $K = \mathrm{Frac}(W(k))$, then K is a complete discretely valued field with $\mathcal{O}_K \cong W(K)$ and $p \in \mathcal{O}_K$ is a uniformizer, so in fact the converse of the above proposition holds.

Proposition 8.10. *Let $(K, |\cdot|)$ be a complete discretely valued field with $k := \mathcal{O}_K/m$ perfect, then $\mathcal{O}_K$ is finite over $W(k)$.*

Proof. Consider the subset $R \subseteq \mathcal{O}_K$ defined by $R = \{\sum_{i=0}^{\infty}[a_i]p^i : a_i \in k\}$. Calculating as in the example of $\mathbb{Z}_p$ shows that $R \cong W(k)$. Let π be a uniformizer in $\mathcal{O}_K$ and let $e \in \mathbb{N}$ such that $ev(\pi) = v(p)$.

Let $M = \bigoplus_{i=0}^{\infty} \pi^i R \subseteq \mathcal{O}_K$, an R-submodule.

Since $\sum_{n=0}^{\infty}[x_n]\pi^n \equiv \sum_{n=0}^{e-1}[x_n]\pi^n \mod p\mathcal{O}_K$, and so M generates $\mathcal{O}_K$ modulo $p\mathcal{O}_K$ as an R-module.

Hence $\mathcal{O}_K = M + p\mathcal{O}_K$.

Iterating, $\mathcal{O}_K = M + pM + p^2M + \ldots + p^m\mathcal{O}_K = M + p^m\mathcal{O}_K$, and so $M \to \mathcal{O}_K/p^m\mathcal{O}_K$ is surjective for all m.

Using the fact that $M \cong \varprojlim_n M/p^nM$, we can show that $M \to \mathcal{O}_K$ is surjective, and so $M = \mathcal{O}_K$. □

Theorem 8.11. *Let K be a non-archimedean local field of mixed characteristic. Then K is a finite extension of $\mathbb{Q}_p$.*

Proof. Let $k = \mathbb{F}_{p^n}$ for some primes p. Then by **8.10**, K is a finite extension of $\mathrm{Frac}(W(\mathbb{F}_{p^n}))$. It suffices to show that $W(\mathbb{F}_{p^n})$ is finite over $\mathbb{Z}_p$.

Let $e_1, \ldots, e_n \in \mathbb{F}_{p^n}$ be a basis of $\mathbb{F}_{p^n}$ as an $\mathbb{F}_p$ vector space, and we write

$$M := \bigoplus_{i=1}^{n} W(\mathbb{F}_p)[e_i] \subseteq W(\mathbb{F}_{p^n})$$

which is a $W(\mathbb{F}_p)$ submodule.

For $x = \sum_{i=0}^{\infty}[x_i]p^i \in W(\mathbb{F}_{p^n})$, let $x_0 = \sum_{i=1}^{\infty} \lambda_i e_i$ for $\lambda \in \mathbb{F}_p$.

Then $x - \sum_{i=1}^{\infty}[\lambda_i][e_i] \in pW(\mathbb{F}_{p^n})$, and so $W(\mathbb{F}_{p^n}) = M + pW(\mathbb{F}_{p^n})$.

Arguing as in the previous proposition shows that $M = W(\mathbb{F}_{p^n})$. □

End of non-examinable content.

---

9 Archimedean Local Fields

Lemma 9.1. *An absolute value $|\cdot|$ on a field is non-archimedean if and only if $|n|$ is bounded for all $n \in \mathbb{Z}$.*

Proof. For the forwards direction, since $|-1| = 1$, $|-n| = |n|$, it suffices to show that $|n|$ is bounded for $n \geq 1$. By the ultrametric inequality, $|n| = |1 + 1 + \ldots + 1| \leq 1$.

For the other direction, suppose $|n| \leq B$ for all $n \in \mathbb{Z}$. The let $x, y \in K$ with $|x| \leq |y|$. Then $|x + y|^m = |\sum_{i=0}^{m}\binom{m}{i}x^iy^{m-i}| \leq \sum_{i=0}^{m}|\binom{m}{i}x^iy^{m-i}| \leq B(m+1)|y|^m$.

Taking m^{th} roots, $|x + y| \leq |y|[B(m+1)]^{1/m} \to |y| = \max(|x|, |y|)$ as $m \to \infty$. □

Corollary 9.2. *If $(K, |\cdot|)$ is a valued field of positive characteristic, then K is non-archimedean.*

Proof. Given the homomorphism $\phi : \mathbb{Z} \to K; 1 \mapsto 1$, we have $\phi(\operatorname{char} K) = 0$, and hence $\{\phi(n) : n \in \mathbb{Z}\}$ is finite, so $|n|$ bounded for $n \in \mathbb{Z}$. Then apply **9.1**. $\square$

Theorem 9.3 (Ostrowski's Theorem)**.** *Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.*

Proof. We split the proof into the archimedean and non-archimedean cases.

- Archimedean

  We fix $b > 1$ an integer such that $|b| > 1$, which exists by **9.1**. Let $a > 1$ be an integer and write b^n in base a:
  $$b^n = c_m a^m + c_{m-1} a^{m-1} + \ldots + c_0$$
  where $0 \leq c_i < a$. Now let $B = \max_{0 \leq c < a}(|c|)$, then we have
  $$\begin{aligned} |b^n| &\leq (m+1)B \max(|a|^m, 1) \\ |b| &\leq [(n(\log_a b) + 1)B]^{1/n} \max(|a|^{\log_a b}, 1) \\ |b| &\leq \max(|a|^{\log_a b}, 1) \end{aligned}$$

  Then $|a| > 1$, and $|b| \leq |a|^{\log_a b}$. Switching the roles of a and b, we get $|a| \leq |b|^{\log_b a}$.

  Hence $\frac{\log|a|}{a} = \frac{\log|b|}{b} = \lambda > 0$ say, and $|a| = a^\lambda$ for all $a \in \mathbb{Z}$. But then $|x| = |x|_\infty^\lambda$ for any $x \in \mathbb{Q}$, and so $|\cdot|$ is equivalent to $|\cdot|_\infty$.

- Non-archimedean

  As in **9.3**, we have $|n| \leq 1$ for all $n \in \mathbb{Z}$. Since $|\cdot|$ is non-trivial, there is some $n \in \mathbb{Z}_{>1}$ such that $|n| < 1$.

  Write $n = p_1^{e_1} \ldots p_r^{e_r}$ as a decomposition into prime factors. Then $|p| < 1$ for some $p \in \{p_1, \ldots, p_r\}$.

  Suppose that $|q| < 1$ for some prime $q \neq p$.

  Then $q = rp + sq$ for $r, s \in \mathbb{Z}$, and $1 = |1| = |rp + sq| \leq \max|rp|, |sq| < 1$. So p is the only prime with absolute value less than 1, and has absolute value $\alpha < 1$. But then using multiplicativity and unique prime factorisation, $|\cdot|$ is equivalent to $|\cdot|_p$.

$\square$

Theorem 9.4. *Let $(K, |\cdot|)$ be an archimedean local field. Then $K = \mathbb{R}$ or $\mathbb{C}$ and $|\cdot|$ is equivalent to $|\cdot|_\infty$.*

Proof. If $\operatorname{char} K > 0$, then K is non-archimedean by **9.2**, so we only need to deal with characteristic 0. So $\mathbb{Q} \subseteq K$.

Since $|\cdot|$ is archimedean, the restriction of $|\cdot|$ to $\mathbb{Q}$ must be equivalent to $|\cdot|_\infty$ by Ostrowski. Since K is complete, $\mathbb{R} \subseteq K$.

We first consider the case when $\mathbb{C} \subseteq K$. By uniqueness of extensions of absolute values, $|\cdot|$ when restricted to $\mathbb{C}$ is equivalent to $|\cdot|_\infty$.

Suppose that $\alpha \in K \setminus \mathbb{C}$. Then $f(x) = |x - \alpha|$ is a continuous function on $\mathbb{C}$ and hence attains a lower bound at $b \in \mathbb{C}$.

Set $\beta = \alpha - b \neq 0$, and we let $c \in \mathbb{C}$ such that $0 < |c| < |\beta|$.

Then $|\beta - a| \geq |\beta|$ for any $a \in \mathbb{C}$. Then

$$\begin{aligned} \frac{|\beta - c|}{|\beta|} \leq \frac{|\beta - c|}{|\beta|} \prod_{\substack{\zeta^n=1 \\ \zeta \neq 1}} \frac{|\beta - \zeta c|}{|\beta|} &= \frac{|\beta^n - c^n|}{|\beta|^n} \\ &= |1 - \left(\frac{c}{\beta}\right)^n| \\ &\to 1 \text{ as } n \to \infty \end{aligned}$$

So $|\beta - c| \leq |\beta|$, and hence $|\beta - c| = |\beta|$.

Replace β by $\beta - c$ and iterating, we obtain $|\beta - mc| = |\beta|$ for all $m \in \mathbb{N}$.

But then $|m||c| = |mc| \leq |\beta - mc| + |beta| = 2|\beta|$, and so $|\cdot|$ must be non-archimedean by **9.1** $\lightning$, and hence $K = \mathbb{C}$.

Now suppose that $\mathbb{C} \not\subseteq K$. Define $L = K(\mathrm{i})$ where $\mathrm{i}^2 = -1$. We can extend $|\cdot|$ to an absolute value $|\cdot|_L$ on L given by $|a + \mathrm{i}b|_L = \sqrt{|a|^2 + |b|^2}$ for $a, b \in K$.

Applying the above argument gives $K(\mathrm{i}) = L = \mathbb{C}$, and hence $K = \mathbb{R}$. □

We are now ready to finish the classification of local fields.

*Proof of **Theorem 8.2**.*
If $|\cdot|$ is archimedean, use **9.4**.

If $|\cdot|$ is non-archimedean with characteristic 0, use **8.11**.

If $|\cdot|$ is non-archimedean with positive characteristic, use **8.4**. □

10 Global Fields

Definition 10.1. *A* **global field** *is a field which is either:*

- *An algebraic number field - a finite extension of $\mathbb{Q}$.*
- *A global function field - the rational function field of an algebraic curve over a finite field. Equivalently, they are finite extensions of $\mathbb{F}_p(t)$.*

In this course, we will mainly focus on the number field case.

We will show that local fields are completions of global fields.

Lemma 10.2. *Let $(K, |\cdot|)$ be a complete discretely valued field, L/K a Galois extension, and $|\cdot|_L$ the unique extension of $|\cdot|$ to L.*

Then for $x \in L, \sigma \in \mathrm{Gal}(L/K)$, we have $|\sigma(x)|_L = |x|_L$.

Proof. Since $x \mapsto |\sigma(x)|_L$ is another absolute value on L extending $|\cdot|$ on K. Hence by uniqueness, $|x|_L = |\sigma(x)|_L$. □

Lemma 10.3 (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 $\alpha_1, \dots, \alpha_n$ in $\bar{K}$, a separable algebraic closure of K.*

Suppose $\beta \in \bar{K}$ with

$$|\beta - \alpha_1| < |\beta - \alpha_i| \text{ for } i = 2, \dots, n$$

Then $\alpha_1 \in K(\beta)$.

Proof. Let $L = K(\beta), L' = L(\alpha_1, \dots, \alpha_n)$. Since L' is the splitting field of a separable polynomial, L'/L is Galois. Let $\sigma \in \mathrm{Gal}(L'/L)$. Then, since $\sigma(\beta) = \beta$, $|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1|$.

So $\sigma(\alpha_1) = \alpha_1$ for all $\sigma \in \mathrm{Gal}(L'/L)$. But then $\alpha \in L = K(\beta)$. □

Proposition 10.4 (Nearby polynomials define the same extension)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field, and $f(x) = \sum_{i=0}^n a_i x^i \in O_K[x]$ be a separable irreducible monic polynomial.*

Let $\alpha \in \bar{K}$ be a root of f. Then there is some $\varepsilon > 0$ such that, for any $g(x) = \sum_{i=0}^n b_i x^i \in O_K[x]$ monic, with $|a_i - b_i| < \varepsilon$, there exists a root β of $g(x)$ such that $K(\alpha) = K(\beta)$.

Proof. Let $\alpha = \alpha_1, \dots, \alpha_n \in \bar{K}$ be the roots of f which are necessarily distinct. Then $f'(\alpha) \neq 0$.

Choose ε sufficiently small so that

$$|g(\alpha_1)| < |f'(\alpha_1)|^2$$
$$|f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha_1)|$$

Then we have $|g(\alpha_1)| < |f'(\alpha_1)|^2 = |g'(\alpha_1)|^2$.

By Hensel's lemma applied to the field $K(\alpha_1)$, there is some $\beta \in K(\alpha_1)$ with $g(\beta) = 0$ and $|\beta - \alpha_1| < |g'(\alpha)|$.

Since $|g'(\alpha)| = |f'(\alpha)| = \prod_{i=2}^n |\alpha_1 - \alpha_i| \leq |\alpha_1 - \alpha_i|$ for $i = 2, \dots, n$, since $|\alpha_1 - \alpha_i| \leq 1$, as all roots lie in $O_{\bar{K}}$.

Since $|\beta - \alpha_1| < |g'(\alpha_1)| = |f'(\alpha_1)| \leq |\alpha_1 - \alpha_i| = |\beta - \alpha_i|$, and by Krasner's lemma we have $K(\alpha) = K(\beta)$. □

Theorem 10.5. *Let K be a local field. Then K is the completion of a global field.*

Proof. We split into cases:

1. $|\cdot|$ is archimedean

   Then $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$, and $\mathbb{C}$ is the completion of $\mathbb{Q}(i)$ with respect to $|\cdot|_\infty$.

2. K non-archimedean and has equal characteristic

   Then $K \cong \mathbb{F}_q((t))$, and K is the completion of $F_q(t)$ with respect to the t-adic absolute value.

3. K non-archimedean and has mixed characteristic

   Then $K \cong \mathbb{Q}_p(\alpha)$ for α a root of monic irreducible polynomial over $\mathbb{Z}_p$.

   Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we can choose $g(x) \in \mathbb{Z}[x]$ as in **10.4**. Then $K = \mathbb{Q}_p(\beta)$ where β is a root of g. Since $\beta \in \bar{\mathbb{Q}}$, we have $\mathbb{Q}(\beta) \subseteq \mathbb{Q}_p(\beta) = K$. So K is the completion of $\mathbb{Q}(\beta)$.

□

10.1 Dedekind Domains

The global analogue of a discrete valuation ring is a Dedekind domain.

Definition 10.6. *A* **Dedekind domain** *is a ring R such that:*

1. *R is a Noetherian integral domain.*
2. *R is integrally closed in* $\mathrm{Frac}(R)$.
3. *Every non-zero prime ideal is maximal.*

Examples:

- The ring of integers in a number field is a Dedekind domain.
- Any PID (hence DVR) is a Dedekind domain.

Theorem 10.7. *A ring R is a DVR if and only if R is a Dedekind domain with exactly one non-zero prime ideal.*

Lemma 10.8. *Let R be a Noetherian ring and $I \subseteq R$ a non-zero ideal. Then there exists non-zero prime ideals $p_1, \ldots, p_r \subseteq R$ such that $p_1 p_2 \ldots p_r \subseteq I$.*

Proof. Suppose not. Since R is Noetherian, we can choose I maximal with this property. Then I is not prime, so there exists $x, y \in R \setminus I$ such that $xy \in I$.

Let $I_1 = I + (x), I_2 = I + (y)$. Then by maximality of I, there are $p_1, \ldots, p_r, q_1, \ldots, q_s$ prime ideals such that $p_1 \ldots p_r \subseteq I_1; q_1 \ldots q_s \subseteq I_2$.

But then $p_1 \ldots p_r q_1 \ldots q_s \subseteq I_1 I_2 = I \lightning$. □

Lemma 10.9. *Let R be an integral domain which is integrally closed in $K = \mathrm{Frac}(R)$. Let $I \subseteq R$ be a non-zero finitely generated ideal and $x \in K$. Then if $xI \subseteq I$, we have $x \in R$.*

Proof. Let $I = (c_1, \ldots, c_n)$. We write $xc_i = \sum_{i=1}^n a_{ij} c_i$ for some $a_{ij} \in R$. Let A be the matrix $A = (a_{ij})_{1 \leq i,j \leq n}$, and $B = x\mathrm{Id}_n - A \in M_{n \times n}(K)$.

Let $\mathrm{Adj}(B)$ be the adjugate matrix for B.

Then $B \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$ in K^n. Multiplying both sides by $\mathrm{Adj}(B)$, we get:

$$(\det B)\mathrm{Id}_n \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

and so $\det B = 0$. But $\det B$ is a monic polynomial in x with coefficients in R. So x is integral over R, and hence $x \in R$. □

Proof of ***10.7****.* The forwards direction is immediate.

For the reverse direction, we need to show that R is a PID. The assumption implies that R is a local ring with unique maximal ideal m.

Step 1: m is principal.

Let $0 \neq x \in m$. By **10.7**, $(x) \supseteq m^n$ for some $n \geq 1$. Let n be minimal such, then we may choose $y \in m^{n-1} \setminus (x)$.

Set $\pi := \frac{x}{y}$. Then $ym \subseteq m^n \subseteq (x)$, and so $\pi^{-1}m \subseteq R$.

If $\pi^{-1}m \subseteq m$, then $\pi^{-1} \in R$ by **10.8**, and so $y \in (x)$ $\lightning$.

Hence $\pi^{-1}m = R$, since m is the unique maximal ideal and so any elements not in m are units.

So $m = \pi R$ is principal.

Step 2: R is a PID.

Let $I \subseteq R$ be a non-zero ideal. Consider the sequence of ideals

$$I \subseteq \pi^{-1} I \subseteq \pi^{-2} I \subseteq \dots \text{ in } K$$

Then $\pi^{-k}I \neq \pi^{-(k+1)}I$ for all k, by **10.9**, and so the inclusions are strict. Since R is Noetherian, we may choose a maximal n such that $\pi^{-n}I \subseteq R$.

If $\pi^{-n}I \subseteq m = (\pi)$, then $\pi^{-(n+1)}I \subseteq R$ $\lightning$.

Thus $\pi^{-n}I = R$, and hence $I = (\pi^n)$. □

11 Dedekind Domains II

Let R be an integral domain, and $S \subseteq R$ a multiplicatively closed subset. Then the ***localisation of R with respect to S***, $S^{-1}R$ is the ring

$$S^{-1}R := \left\{ \frac{r}{s} : r \in R, s \in S \right\} \subseteq \operatorname{Frac}(R)$$

If p is a prime ideal in R, we write $R_{(p)}$ for the localisation with respect to $S = R \setminus p$.

Examples:

- $p = (0), R_{(p)} = \operatorname{Frac}(R)$
- $R = \mathbb{Z}, \mathbb{Z}_{(p)} = \left\{ \frac{a}{p^n} : a \in \mathbb{Z}, n \geq 0 \right\}$

If R is noetherian, then $S^{-1}R$ is also noetherian. There is always a bijection

$$\{\text{prime ideals in } S^{-1}R\} \leftrightarrow \{\text{prime ideals } p \subseteq R \text{ s.t. } p \cap S = \emptyset\}$$

given by $pS^{-1}R \leftrightarrow p$.

Corollary 11.1. *Let R be a Dedekind domain, and $p \subseteq R$ a non-zero prime. Then $R_{(p)}$ is a DVR.*

Proof. By properties of localisation, $R_{(p)}$ is a noetherian integral domain with a unique non-zero prime ideal $pR_(p)$. It suffices to show $R_{(p)}$ is also integrally closed in $\mathrm{Frac}(P_{(p)}) = \mathrm{Frac}(R)$, since then $R_{(p)}$ will be a Dedekind, and so by **10.7** is a DVR.

Let $x \in \mathrm{Frac}(R)$ be integral over $R_{(p)}$. Multiplying by denominators of a monic polynomial satisfied by x, we obtain

$$sx^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, a_i \in R, s \in S$$

Multiplying by s^{n-1} we get that xs is integral over R, so $xs \in R$ as R is a Dedekind domain, so $x \in R_{(p)}$. □

Definition 11.2. *If R is a Dedekind domain, and $p \subseteq R$ a non-zero prime ideal, then we write v_p for the normalised valuation on* $\mathrm{Frac}(R) = \mathrm{Frac}(R_{(p)})$ *corresponding to the DVR $R_{(p)}$.*

For example, if $R = \mathbb{Z}, p = (p), v_p$ is the p-adic valuation on $\mathbb{Z}$.

Theorem 11.3. *Let R be a Dedekind domain. Then every non-zero prime ideal $I \subseteq R$ can be written uniquely as a product of prime ideals:*

$$I = p_1^{e_1} \ldots p_r^{e_r}, p_i \textit{ distinct}$$

Note that this is clear for PIDs, as they are UFDs.

Proof. We will quote the following properties of localisations:

1. If $I \nsubseteq p$ then $IR_p \subsetneq pR_{(p)}$.
2. $I = J \iff IR_{(p)} = JR_{(p)}\ \forall p$ prime ideals.

Let $I \subseteq R$ be a non-zero ideal. Then by **10.8**, there are prime ideals $p_1, \ldots, p_r$ such that $p_1^{\beta_1} \ldots p_r^{\beta_r} \subseteq I$, where $\beta_i > 0$.

Then $IR_{(p)} = \begin{cases} R_{(p)} & p \notin \{p_1, \ldots, p_r\} \\ p^{\alpha_i} R_{(p)} & p = p_i \end{cases}$

Here $0 \leq \alpha_i, \beta_i$, the second case follows from **11.1**.

Then $I = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ by the second quoted property.

For uniqueness, if $I = p_1^{\alpha_1} \ldots p_r^{\alpha_r} = p_1^{\gamma_1} \ldots p_r^{\gamma_r}$, then $p_i^{\alpha_i} R_{(p_i)} = p_i^{\gamma_i} R_{(p_i)}$, and so $\alpha_i = \gamma_i$ by unique factorisation in DVRs. □

11.1 Dedekind Domains and Extensions

Let L/K be a finite extension. Then for $x \in L$, we write $\mathrm{Tr}_{L/K}(x) \in K$ for the ***trace*** of the K-linear map given by multiplication by x.

If L/K is separable and $\sigma_1, \ldots, \sigma_n : L \to \bar{K}$ denotes the set of embeddings of L into a separable closure $\bar{K}$, then

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

Lemma 11.4. *Let L/K be a finite separable extension of fields. Then the symmetric bilinear pairing*

$$(\cdot,\cdot) : L \times L \longrightarrow K; (x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$$

is non-degenerate.

Proof. By the primitive element theorem, $L = K(\alpha)$ for some $\alpha \in L$. We consider the matrix A for $(\cdot,\cdot)$ in the K-basis for L given by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Then:

$$A_{ij} = \mathrm{Tr}_{L/K}(\alpha^{i+j}) = [B^2]_{ij}$$

where B is the $n \times n$ Vandermonde matrix with

$$B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \cdots & \sigma_n(\alpha) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\alpha^{n-1}) & \sigma_2(\alpha^{n-1}) & \cdots & \sigma_n(\alpha^{n-1}) \end{pmatrix}$$

Then $\det A = (\det B)^2 = \left[\prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha)) \right]^2 \neq 0$, since $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$. □

In fact, a finite extension of fields L/K is separable if and only if the trace form in non-degenerate.

Theorem 11.5. *Let $\mathcal{O}_K$ be a Dedekind domain and L a finite separable extension of $K = \mathrm{Frac}(\mathcal{O}_K)$. Then the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K \in L$ is a Dedekind domain.*

Proof. Since $\mathcal{O}_L \subseteq L$, it is an integral domain. We need to show that:

1. $\mathcal{O}_L$ is noetherian.
2. $\mathcal{O}_L$ is integrally closed in L.
3. Every non-zero prime ideal $P \subseteq \mathcal{O}_L$ is maximal.

We'll check these in order:

1. Let $e_1, \ldots, e_n \in L$ be a K-basis for L. Upon scaling by K, we may assume that $e_i \in \mathcal{O}_L$. Let $f_i \in L$ be the dual basis with respect to the trace form $(\cdot,\cdot)$.

   Let $x \in \mathcal{O}_L$ and write $x = \sum_{i=1}^n \lambda_i f_i$ for $\lambda_i \in K$. Then $\lambda_i = \mathrm{Tr}_{L/K}(xe_i) \in \mathcal{O}_K$, as for any $z \in \mathcal{O}_L$, $\mathrm{Tr}_{L/K}(z)$ is a sum of elements which are integral over $\mathcal{O}_K$, and so $\mathrm{Tr}_{L/K}(z)$ is integral over $\mathcal{O}_K$, hence in $\mathcal{O}_K$ as $\mathcal{O}_K$ is Dedekind.

   Thus $\mathcal{O}_L \subseteq \mathcal{O}_K f_1 + \ldots + \mathcal{O}_K f_n$.

   Since $\mathcal{O}_K$ is noetherian, $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$-module, and so $\mathcal{O}_L$ is noetherian.
2. Example sheet 2.
3. Let $\mathcal{P}$ be a non-zero prime ideal of $\mathcal{O}_L$, and define $p := \mathcal{P} \cap \mathcal{O}_K$, a prime ideal of $\mathcal{O}_K$.

   Let $x \in \mathcal{P}$, then x satisfies an equation of the form

   $$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, a_i \in \mathcal{O}_K$$

But then $a_0 \in O \cap O_K$ is a non-zero element of p, and so p is non-zero, and hence maximal.

We have $O_K/p \hookrightarrow O_L/\mathcal{P}$, and $O_L/\mathcal{P}$ is a finite dimensional vector space over O_K/p. Since $O_L/\mathcal{P}$ is an integral domain, it is a field.

□

Note that **11.5** in fact holds without the assumption that L/K is separable.

Corollary 11.6. *The ring of integers inside a number field is a Dedekind domain.*

Convention: if O_K is the ring of integers of a number field, $\mathfrak{p} \subseteq O_K$ a non-zero prime ideal, then we normalise $|\cdot|_\mathfrak{p}$ so that

$$|x|_\mathfrak{p} = N_\mathfrak{p}^{-v_\mathfrak{p}(x)}, \text{ where } N_\mathfrak{p} = \# O_K/\mathfrak{p}$$

12 Dedekind Domains & Extensions

Let O_K be a Dedekind domain.

Lemma 12.1. *Let $0 \neq x \in O_K$. Then:*

$$(x) = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_\mathfrak{p}(x)}$$

Note that this product is finite.

Proof. $xO_{K,(\mathfrak{p})} = (\mathfrak{p}O_{K,(\mathfrak{p})})^{v_\mathfrak{p}(x)}$ by definition of $v_\mathfrak{p}(x)$.

The lemma then follows from properties of localisation:

$I = S \iff IO_{K,(\mathfrak{p})} = JO_{K,(\mathfrak{p})}$ for all prime ideals $\mathfrak{p}$. □

Notation: for O_K a Dedekind domain, L/K a finite separable extension, $\mathcal{P} \subseteq O_L$, $\mathfrak{p} \subseteq O_K$ nonzero prime ideals, we write $\mathcal{P}|\mathfrak{p}$ if when we write

$$\mathfrak{p}O_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}, \quad e_i > 0$$

$\mathcal{P}$ is one of the $\mathcal{P}_i$.

Theorem 12.2. *Let O_K be a Dedekind domain and L a finite separable extension of $K = \mathrm{Frac}(O_K)$.*

For $\mathfrak{p}$ a nonzero prime ideal of O_K, we write $\mathfrak{p}O_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$, where $e_i > 0$. Then the absolute values on L extending $|\cdot|_\mathfrak{p}$ up to equivalence are precisely $|\cdot|_{\mathcal{P}_1}, \dots, |\cdot|_{\mathcal{P}_r}$.

Proof. By **12.1**, for any $x \in O_K$ and $i = 1, \dots, r$, we have $v_{\mathcal{P}_i}(x) = e_i v_\mathfrak{p}(x)$.

Hence, up to equivalence, $|\cdot|_{\mathcal{P}_i}$ extend to $|\cdot|_\mathfrak{p}$.

Now suppose that $|\cdot|$ is an absolute value on L extending $|\cdot|_\mathfrak{p}$. Then $|\cdot|$ is bounded on $\mathbb{Z}$, and hence by $|\cdot|$ is non-archimedean.

Now let $R = \{x \in L : |x| \leq 1\} \subseteq L$ be the valuation ring for L with respect to $|\cdot|$. Then $O_K \subseteq R$, and since R is integrally closed in L (see section 6), we have $O_L \subseteq R$.

Set $\mathcal{P} := \{x \in O_L : |x| < 1\}$. It is easy to check that $\mathcal{P}$ is a non-zero prime ideal.

E.g.: given $x, y \in \mathcal{P}$, then $x+y \in \mathcal{P}$. So if $r \in \mathcal{O}_L$, $x \in \mathcal{P}$, then $rx \in \mathcal{P}$, and that if $x, y \in \mathcal{O}_L$, $xy \in \mathcal{P}$ then $x \in \mathcal{P}$ or $y \in \mathcal{P}$, just using properties of non-archimedean absolute values.

Then $\mathcal{O}_{L,(\mathcal{P})} \subseteq R$, since $s \in \mathcal{O}_L \setminus \mathcal{P}$ gives $|s| = 1$. But $\mathcal{O}_{L,(\mathcal{P})}$ is a DVR and hence a maximal subring of L, and so $R = \mathcal{O}_{L,(\mathcal{P})}$. But then $|\cdot|$ is equivalent to $|\cdot|_{\mathcal{P}}$.

Since $|\cdot|$ extends $|\cdot|_{\mathfrak{p}}$, we have $\mathcal{P} \cap \mathcal{O}_K = \mathfrak{p}$, and so $\mathcal{P} = \mathcal{P}_i$ 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 - see example sheet 2. This absolute value is denoted $|\cdot|_\sigma$.

Corollary 12.3. *Let K be a number field, with ring of integers $\mathcal{O}_K$, then any absolute value on K is either:*

1. *$|\cdot|_{\mathfrak{p}}$ for some non-zero prime ideal $\mathfrak{p}$.*
2. *$|\cdot|_\sigma$ for some $\sigma : K \to \mathbb{R}, \mathbb{C}$.*

Proof. If $|\cdot|$ is non-archimedean. Then $|\cdot|_{\mathbb{Q}}$ is non-archimedean, so is equivalent to $|\cdot|_p$ for some prime p by Ostrowski. Then **12.2** implies that $|\cdot|$ is $|\cdot|_{\mathfrak{p}}$ for some $\mathfrak{p}$ a prime of $\mathcal{O}_K$ dividing (p).

The archimedean case is left as an exercise to example sheet 2. □

12.1 Completions

Now let L/K be an extension of number fields with rings of integers $\mathcal{O}_K, \mathcal{O}_L$ respectively. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ and $\mathcal{P} \subseteq \mathcal{O}_L$ be non-zero prime ideals such that $\mathcal{P}$ divides $\mathfrak{p}$. We write $K_{\mathfrak{p}}$ and $L_{\mathcal{P}}$ for the completions of K and L with respect to $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathcal{P}}$ respectively.

Lemma 12.4.

1. *The natural map $L \otimes_K K_{\mathfrak{p}} \to L_{\mathcal{P}}$ is surjective.*
2. *$[L_{\mathcal{P}} : K_{\mathfrak{p}}] \leq [L : K]$*

Proof. Let $M = LK_{\mathfrak{p}} \subseteq L_{\mathcal{P}}$. Then M is a finite extension of $K_{\mathfrak{p}}$ and $[M : K\mathfrak{p}] \leq [L : K]$, and moreover M is complete and, since $L \subseteq M \subseteq L_{\mathcal{P}}$, we have $L_{\mathcal{P}} = M$. □

Lemma 12.5 (Chinese Remainder Theorem)**.** *Let R be a ring, $I_1, \ldots, I_n \subseteq R$ be ideals such that $I_i + I_j = R$ for all $i \neq j$ (we say the I_i are pairwise coprime). Then:*

1. *$\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i = I$*
2. *$R/I \cong \prod_{i=1}^n R/I_i$*

Proof. Example sheet 2. □

Theorem 12.6. *$L \otimes_K K_{\mathfrak{p}} \cong \prod_{\mathcal{P}|\mathfrak{p}} L_{\mathcal{P}}$*

Proof. Write $L = K(\alpha)$ by separability, and let $f(x) \in K[x]$ be the minimal polynomial of α.

Let $f(x) = f_1(x) \ldots f_r(x)$ in $K_{\mathfrak{p}}[x]$ where $f_i(x) \in K_p[x]$ are distinct irreducibles.

Then $L \cong K[x]/f(x)$, and so by the Chinese remainder theorem:

$$\begin{aligned} L \otimes_K K_{\mathfrak{p}} &\cong K_{\mathfrak{p}}[x]/f(x) \\ &= \prod_{i=1}^{r} K_{\mathfrak{p}}[x]/f_i(x) \end{aligned}$$

Set $L_i := K_p[x]/f_i(x)$. Since f_i are irreducible, this is field, and hence a finite extension of $K_{\mathfrak{p}}$.

Then L_i contains both L and $K_{\mathfrak{p}}$, since $K[x]/f(x) \to K_{\mathfrak{p}}[x]/f_i(X)$ is injective, being a non-zero map of fields. Moreover, L is dense in L_i, since K is dense in $K_{\mathfrak{p}}$, we can approximate coefficients of an element of $K_{\mathfrak{p}}[x]/f_i(x)$ with an element of $K[x]/f(x)$.

Then the theorem follows from the following three claims:

1. $L_i \cong L_{\mathcal{P}}$ for some prime $\mathcal{P}$ of $\mathcal{O}_L$ dividing $\mathfrak{p}$.
2. Each $\mathcal{P}$ appears at most once.
3. Each $\mathcal{P}$ appears at least once.

Proof:

1. Since $[L_i : K_{\mathfrak{p}}] < \infty$, there is a unique absolute value $|\cdot|$ on L_i extending $|\cdot|_{\mathfrak{p}}$. By **12.2**, restricting this to L, it is equivalent to $|\cdot|_{\mathcal{P}}$ for some $\mathcal{P}|\mathfrak{p}$. Since L is dense in L_i and L_i is complete, we have $L_i \cong L_{\mathcal{P}}$.
2. Suppose $\varphi : L_i \to L_j$ is an isomorphism, preserving L and $K_{\mathfrak{p}}$, then φ is given by:

   $$\begin{aligned} \varphi : K_{\mathfrak{p}}[x]/f_i(x) &\to K_{\mathfrak{p}}[x]/f_j(x) \\ x &\mapsto x \end{aligned}$$

   But then $f_i(x) = f_j(x)$ and so $i = j$.
3. By **12.4**, the natural map $\pi_{\mathcal{P}} : L \otimes_K K_{\mathfrak{p}} \to L_{\mathcal{P}}$ is surjective for any $\mathcal{P}|\mathfrak{p}$.

   Since $L_{\mathcal{P}}$ is a field, $\pi_{\mathcal{P}}$ factors through L_i for some i, and hence $L_i \cong L_{\mathcal{P}}$ by surjectivity of $\pi_{\mathcal{P}}$.

□

For example, if $K = \mathbb{Q}, L = \mathbb{Q}(\mathrm{i}), f(x) = x^2 + 1$. Then Hensel tells us $\sqrt{-1} \in \mathbb{Q}_5$, so in $\mathbb{Q}_5$ $f(x)$ factorises. Hence (5) splits in $\mathbb{Q}(i)$, i.e. $5\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$.

Corollary 12.7. *For $x \in L$, we have*

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

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$. Let $\mathcal{B}_1, \dots, \mathcal{B}_r$ be bases for the completions $L_{\mathcal{P}_1}, \dots, L_{\mathcal{P}_r}$ as $K_{\mathfrak{p}}$-vector spaces.

Then $\mathcal{B} = \bigcup_{i=1}^{r} \mathcal{B}_i$ is a basis for $L \otimes_K K_{\mathfrak{p}}$.

Let $[\mathrm{mult}(x)]_{\mathcal{B}}$ (respectively $[\mathrm{mult}]_{\mathcal{B}_i}$) denote the matrix for the map $\mathrm{mult}(x) : L \otimes_K K_{\mathfrak{p}} \to L \otimes_K K_{\mathcal{P}}$ (respectively $\mathrm{mult}(x) : L_{\mathcal{P}_i} \to L_{\mathcal{P}_i}$) with respect to the basis $\mathcal{B}$ (respectively $\mathcal{B}_i$). Then

$$[\mathrm{mult}(x)]_{\mathcal{B}} = \mathrm{Diag}([\mathrm{mult}(x)]_{\mathcal{B}_\infty}, \dots, [\mathrm{mult}(x)]_{\mathcal{B}_r})$$

And hence

$$N_{L/K}(x) = \mathrm{Det}([\mathrm{mult}(x)]_{\mathcal{B}}) = \prod_{i=1}^{r} \mathrm{Det}([\mathrm{mult}(x)]_{\mathcal{B}_i}) = \prod_{i=1}^{r} N_{L_{\mathcal{P}_i}/K_{\mathfrak{p}}}(x)$$

□

13 Decomposition Groups

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

We've seen that if $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal then we may write

$$\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$$

where the $\mathcal{P}_i$ are distinct prime ideals of $\mathcal{O}_L$. Note that, for any i, $\mathfrak{p} \subseteq \mathcal{O}_K \cap \mathcal{P}_i \subsetneq \mathcal{O}_K$, and hence $\mathfrak{p} = \mathcal{O}_K \cap \mathcal{P}_i$.

Definition 13.1.

1. *e_i is the* **ramification index** *of $\mathcal{P}_i$ over $\mathfrak{p}$*
2. $\mathfrak{p}$ **ramifies** *in L if some $e_i > 1$.*

For example, if $\mathcal{O}_K = \mathbb{C}[t], \mathcal{O}_L = \mathbb{C}[T]$, with $\mathcal{O}_K \hookrightarrow \mathcal{O}_L; t \mapsto T^n$.

We have $t\mathcal{O}_L = T^n\mathcal{O}_L$, and so the ramification index of (T) over (t) is n. This corresponds geometrically to the degree n covering of Riemann surfaces $\mathbb{C} \to \mathbb{C}; x \mapsto x^n$ having a ramification point at 0, with ramification index n.

Definition 13.2. *$f_i := [\mathcal{O}_L/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is the* **residue class degree** *of $\mathcal{P}_i$ over $\mathfrak{p}$.*

Theorem 13.3.

$$\sum_{i=1}^{n} e_i f_i = [L : K]$$

Proof. Let $S = \mathcal{O}_K \setminus \mathfrak{p}$. We have the following facts, whose proofs are left as exercises:

- $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K$ in L.
- $S^{-1}\mathfrak{p}S^{-1}\mathcal{O}_L \cong S^{-1}\mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$.
- $S^{-1}\mathcal{O}_L/S^{-1}\mathcal{P}_i \cong \mathcal{O}_L/\mathcal{P}_i$, and $S^{-1}\mathcal{O}_K/S^{-1}\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$.

The second and third conditions imply that e_i, f_i don't change when we localise $\mathcal{O}_K, \mathcal{O}_L$ at $\mathfrak{p}$.

Thus we may assume that $\mathcal{O}_K$ is a DVR, and hence a PID.

By the Chinese remainder theorem, we have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^{r} \mathcal{O}_L/\mathcal{P}_i^{e_i}$$

Note that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a $k := \mathcal{O}_K/\mathfrak{p}$-vector space (as k a field), and so we can count dimensions of both sides.

For each i, we have a decreasing sequence of k-subspaces:

$$0 \subseteq \mathcal{P}_i^{e_i-1}/\mathcal{P}_i^{e_i} \subseteq \mathcal{P}_i^{e_i-2}/\mathcal{P}_i^{e_i} \subseteq \ldots \subseteq \mathcal{P}_i/\mathcal{P}_i^{e_i} \subseteq O_L/\mathcal{P}_i^{e_i}$$

So $\dim_k O_L/\mathcal{P}_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_k \left(\mathcal{P}_i^j/\mathcal{P}_i^{j+1}\right)$. Note that this quotient $\mathcal{P}_i^j/\mathcal{P}_i^{j+1}$ is an $O_L/\mathcal{P}_i$-module and $x \in \mathcal{P}_i^j/\mathcal{P}_i^{j+1}$ (for example, we can prove this after localising at $\mathcal{P}_i$). Then $\dim_k \mathcal{P}_i^j/\mathcal{P}_i^{j+1} = f_i$, and we have that

$$\dim_k \prod_{i=1}^r O_L/\mathcal{P}_i^{e_i} = \sum_{i=1}^r \dim_k O_L/\mathcal{P}_i^{e_i} = \sum_{i=1}^r e_i f_i$$

Now recall that O_K a DVR, and so the structure theorem for modules over PIDs gives O_L is a free module over O_K of rank $n = [L : K]$.

So $O_L/\mathfrak{p}O_L \cong (O_K/\mathfrak{p})^n$ as O_K-modules, and hence $\dim_k O_L/\mathfrak{p}O_L = n$. □

This theorem is the algebraic analogue of the fact that, for a degree n covering $X \to Y$ of compact Riemann surfaces and $x \in X$, we have

$$n = \sum_{x \in f^{-1}(y)} e_x$$

where e_x is the ramification index of x.

Now assume that L/K is Galois. Then, for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathcal{P}_i) \cap O_K = \mathfrak{p}$, and hence $\sigma(\mathcal{P}_i) \in \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$, and so $\mathrm{Gal}(L/K)$ acts on the set $\{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$.

Proposition 13.4. *The action of* $\mathrm{Gal}(L/K)$ *on* $\{\mathbb{P}_1, \ldots, \mathbb{P}_r\}$ *is transitive.*

Proof. Suppose the action is not transitive, so that there exists some $i \neq j$ with $\sigma(\mathcal{P}_i)$ is never $\mathcal{P}_j$ for any $\sigma \in \mathrm{Gal}(L/K)$.

Then the Chinese remainder theorem tells us we may pick $x \in O_L$ with $x \equiv 0 \mod \mathcal{P}_i$, and $x \equiv 1 \mod \sigma(\mathcal{P}_j)$ for all $\sigma \in \mathrm{Gal}(L/K)$.

But then $N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in O_K \cap \mathcal{P}_i = \mathfrak{p} \subseteq \mathcal{P}_j$.

Since $\mathcal{P}_j$ is prime, there is some $\tau \in \mathrm{Gal}(L/K)$ with $\tau(x) \in \mathcal{P}_j$, i.e. $x \in \tau^{-1}(\mathcal{P}_j)$, i.e. $x \equiv 0 \mod \tau^{-1}(\mathcal{P}_j)$↯. □

Corollary 13.5. *Suppose L/K is Galois. Then $e_1 = e_2 = \ldots = e_r =: e$; $f_1 = \ldots = f_r =: f$, and $n = efr$.*

Proof. For any $\sigma \in \mathrm{Gal}(L/K)$, we have

1. $\mathfrak{p} = \sigma(p) = \sigma(\mathcal{P}_1)^{e_1} \ldots \sigma(\mathcal{P}_r)^{e_r}$. By unique factorisation and transitivity, $e_1 = \ldots = e_r$.
2. $O_L/\mathcal{P}_i \cong O_L/\sigma(\mathcal{P}_i)$, and so $f_1 = \ldots = f_r$.

□

Let L/K be complete discretely valued fields with normalised valuations v_L, v_K, uniformisers π_L, π_K. Then the only prime ideals are π_L, π_K.

The ramification index is $e := e_{L/K} = v_L(\pi_K)$, i.e. $\pi_L^e O_L = \pi_K O_L$.

The residue class degree is $f := f_{L/K} = [k_L : k]$.

Corollary 13.6. *Suppose either*

1. *L/K is finite and separable*
2. *f is finite*

Then $[L : K] = ef$.

Proof.

1. **13.3**
2. Can apply the same proof as in **13.3** if we know O_L is finitely generated as an O_K-module.

   As before, $\dim_k O_L/\pi_K O_L = ef < \infty$, and so we can pick $x_1, \ldots, x_m \in O_L$, generating $O_L/\pi_K O_L$ over k.

   Then for $y \in O_L$, we can write

   $$y = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{m} a_{ij} x_j \right) \pi_K^i = \sum_{j=1}^{m} \left(\sum_{i=0}^{\infty} a_{ij} \pi_K^i \right) x_j$$

   where $a_{ij} \in O_K$. But the infinite sum in the middle of the RHS term is in O_K by completeness, and so the x_j generate O_L over O_K, and so we can in fact use the proof as in **13.3**.

□

Definition 13.7. *Let L/K be a finite Galois extension. Then the* **decomposition group** *at a prime $\mathcal{P}$ of O_L is the subgroup of* $\mathrm{Gal}(L/K)$ *defined by*

$$G_{\mathcal{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathcal{P}) = \mathcal{P}\}$$

13.4 shows that, for any $\mathcal{P}, \mathcal{P}'$ dividing $\mathfrak{p}$, $G_{\mathcal{P}}$ and $G_{\mathcal{P}'}$ are conjugate, and moreover $G_{\mathcal{P}}$ has size ef, via the orbit-stabilizer theorem.

Recall we write $L_{\mathcal{P}}$ and $K_{\mathfrak{p}}$ for the completions of L and K with respect to $|\cdot|_{\mathcal{P}}, |\cdot|_{\mathfrak{p}}$ respectively.

Proposition 13.8. *Suppose that L/K is finite and Galois, and $\mathcal{P}$ is a prime ideal of L dividing $\mathfrak{p}$.*

Then:

1. *$L_{\mathcal{P}}/K_{\mathfrak{p}}$ is also Galois.*
2. *There is a natural map*

   $$res : \mathrm{Gal}(L_{\mathcal{P}}/L_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$$

   which is injective, and has image $G_{\mathcal{P}}$. Here, res is short for "restriction".

Proof.

1. L/K Galois implies that L is the splitting field of a separable polynomial $f(x) \in K[x]$, and so $L_{\mathcal{P}}$ is the splitting field of f considered as an element of $K_{\mathfrak{p}}[x]$.

   Hence $L_{\mathcal{P}}/K_{\mathfrak{p}}$ is Galois.

2. Let $\sigma \in \mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$. Then $\sigma(L) = L$ since L/K is normal, and hence we have a map $\mathrm{res} : \mathrm{Gal}(L_{\mathcal{P}}/K_p) \to \mathrm{Gal}(L/K)$. Since L is dense in $L_{\mathcal{P}}$, res is injective.

   By **10.2**, $|\sigma(x)|_{\mathcal{P}} = |x|_{\mathcal{P}}$ for $x \in L_{\mathcal{P}}$, and so $\sigma(\mathcal{P}) = \mathcal{P}$ for all $\sigma \in \mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$.

   So $\mathrm{res}(\sigma) \in G_{\mathcal{P}}$.

   To show surjectivity, it suffices to show that $[L_{\mathcal{P}} : K_{\mathfrak{p}}] = ef = |G_{\mathcal{P}}|$.

   We have already seen $|G_{\mathcal{P}}| = ef$, and we can apply **13.6** to $L_{\mathcal{P}}/K_{\mathfrak{p}}$, noting that e, f don't change when we take completions.

□

14 Ramification Theory

14.1 Unramified and Totally Ramified Extensions

Let K be a non-archimedean local field, and L a finite separable extension of K. Then L is a local field.

Last time, we saw $[L : K] = e_{L/K} f_{L/K}$.

Lemma 14.1. *Let $M/L/K$ be finite separable extensions of local fields. Then:*

1. $e_{M/K} = e_{M/L} e_{L/K}$
2. $f_{M/K} = f_{M/L} f_{L/K}$

Proof.

2. $f_{M/K} = [k_M : k] = [k_m : k_L][k_L : k] = f_{M/L} f_{L/K}$.
1. Follows from (2) and the fact that $[L : K] = e_{L/K} f_{L/K}$.

□

Definition 14.2. *The extension L/K is said to be*

- **unramified** *if $e_{L/K}$, i.e. $f_{L/K} = [L : K]$*
- **ramified** *if $e_{L/K} > 1$, i.e. $f_{L/K} < [L : K]$*
- **totally ramified** *if $e_{L/K} = [L : K]$, i.e. $f_{L/K} = 1$*

Theorem 14.3. *Let L/K be a finite separable extension of local fields. Then there exists a field K_0 such that $K \subseteq K_0 \subseteq L$, with:*

1. *K_0/K unramified*
2. *L/K_0 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 $k_L = \mathbb{F}_{q^f}$ where $f = f_{L/K}$. Set $m = q^f - 1$. Then let $[\cdot] : \mathbb{F}_{q^f}^\times \to L^\times$ be the Teichmüller map for L, and let $\zeta_m = [a]$, where a generates $\mathbb{F}_{q^f}^\times$. Then ζ_m is a primitive m^{th} root of unity.

We set $K_0 = K(\zeta_m) \subseteq L$. Then K_0 is the splitting field of the separable polynomial $f(x) = x^m - 1 \in K[x]$, and hence K_0/K is Galois.

Since $|\zeta_m| = 1$, $\zeta_m \in \mathcal{O}_{K_0}^\times$. It follows that $k_0 := \mathcal{O}_{K_0}/\mathfrak{m}_0$ contains a primitive n^{th} root of unity, so $k_0 = \mathbb{F}_{q^f} \cong k_L$.

Now $\mathrm{Gal}(K_0/K)$ preserves $\mathcal{O}_{K_0}$ and $\mathfrak{m}_0$, using $|x| = |\sigma(x)|$. So there is a natural map

$$\mathrm{res} : \mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_0/k)$$

For $\sigma \in \mathrm{Gal}(K_0/K)$, we have

$$\sigma(\zeta_m) = \zeta_m \text{ if } \sigma(\zeta_m) \equiv \zeta_m \mod \mathfrak{m}_0$$

since $\sigma(\zeta_m) = [\mathrm{res}(\sigma)(\zeta_m \mod \mathfrak{m}_0)]$, and so res is injective, and so

$$|\,\mathrm{Gal}(K_0/K)| \leq |\,\mathrm{Gal}(k_0/k)| = f = f_{L/K}$$

and so $[K_0 : K] = f_{L/K}$ and res is an isomorphism, and K_0 is unramified.

Since $k_0 \cong k_L$, $f_{L/K_0} = 1$, hence L/K_0 is totally ramified. □

Theorem 14.4. *Let K be a non-archimedean local field with $k \cong \mathbb{F}_q$. For any $n \geq 1$, there is a unique unramified extension L/K of degree n. Moreover, L/K is Galois, and the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is an isomorphism. In particular, $\mathrm{Gal}(L/K)$ is a cyclic group, generated by an element $\mathrm{Frob}_{L/K}$ such that*

$$\mathrm{Frob}_{L/K}(x) \equiv x^q \mod \mathfrak{m}_L \ \forall x \in \mathcal{O}_L$$

Proof. For $n \geq 1$, we take $L = K(\xi_m)$, where $m = q^n - 1$ and $\zeta_m \in \bar{K}^\times$ is a primitive m^{th} root of unity. Then, as in the proof of **14.3**, $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, and is cyclic and generated by a lift of $x \mapsto x^q$.

Uniqueness is clear since, for L/K of degree n unramified, we have $\zeta_m \in L$, and hence $L = K(\zeta_m)$ by degree reasons. □

Corollary 14.5. *If K is a non-archimedean local field and L/K finite and Galois, then the natural map*

$$\mathit{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$$

is surjective.

Proof. With the notation of **14.3**, the map res factors as

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_L/k)$$

The inertia subgroup $I_{L/K} \subseteq \mathrm{Gal}(L/K)$ is defined to be the kernel of the surjective map

$$\mathrm{res} : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k)$$

Since $e_{L/K} f_{L/K} = [L : K]$, we have $|I_{L/K}| = e_{L/K}$.

There is an exact sequence

$$0 \longrightarrow I_{L/K} \xrightarrow{i} \mathrm{Gal}(L/K) \xrightarrow{p} \mathrm{Gal}(k_L/k) \longrightarrow 0$$

Now $I_{L/K} = \mathrm{Gal}(L/K_0)$, and so L_{K_0} is a totally ramified extension. □

Definition 14.6. *Let K be a local non-archimedean local field, with normalised valuation v. Let*

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathcal{O}_K[x]$$

We say $f(x)$ is **Eisenstein** *if $v(a_i) \geq 1$ for all i and $v(a_0) = 1$.*

Fact: Eisenstein polynomials are irreducible.

Theorem 14.7.

1. *If L/K is a finite totally ramified extension of non-archimedean local fields, then the minimal polynomial of $\pi_L \in \mathcal{O}_L$ is an Eisenstein polynomial, and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, and hence $L = K(\pi_L)$.*
2. *Conversely, if $f(x) \in \mathcal{O}_K[x]$ is Eisenstein and α is a root of f. Then $L := K(\alpha)/K$ is totally ramified.*

Proof.

1. Let v_L be the normalised valuation for L, and set $e := [L : K]$. Let $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in \mathcal{O}_K[x]$ be the minimal polynomial for π_L, which is monic since $\mathcal{O}_L$ is integral over $\mathcal{O}_K$.

   Then $m \leq e$.

   Since $v_L(K^\times) = e\mathbb{Z}$, we have

   $$v_L(a_i\pi_L^i) \equiv i \mod e \ \forall i < m$$

   so that these terms all have different residues mod e. We have

   $$\pi_L^m = -\sum_{i=0}^{m-1} a_i\pi_L^i$$

   and hence $m = v_L(\pi_L^m) = \min\limits_{0\leq i\leq m-1}(i + ev_k(a_i))$, so $v_K(a_i) \geq 1\ \forall i$, and so $m = e$ and $v_K(a_0) = 1$, hence $f(x)$ is Eisenstein, and $L = K(\pi_L)$.

   For $y \in L$, we write $y = \sum_{i=0}^{e-1} \pi_L^i b_i, b_i \in K$.

   Then $v_L(y) = \min\limits_{0\leq i\leq m-1}(i + ev_K(b_i))$, and so $y \in \mathcal{O}_L \iff v_L(y) \geq 0 \iff v_K(b_i) \geq 0\ \forall i$, i.e. $y \in \mathcal{O}_K[\pi_L]$.
2. Let $f(X) = x^n + a_{n-1} + \ldots + a_0$ be Eisenstein, and let $e := e_{L/K}$. Then $v_L(a_i) \geq e$, and $v_L(a_0) = e$.

   If $v_L(\alpha) \leq 0$ we have $v_L(\alpha^n) < v_L(\sum_{i=0}^{n-1} a_i\alpha^i)\lightning$, and so $v_L(\alpha) > 0$.

   For $i \neq 0$, $v_L(a_i\alpha^i) > e = v_L(a_0)$, and it follows that

   $$v_L(-\sum_{i=0}^{n-1} a_i\alpha^i) = e$$

   and hence $v_L(\alpha^n) = e \implies nv_L(\alpha) = e$.

   But $n = [L : K] \geq e \implies n = e$, and L is totally ramified.

□

15 Structure of Units

Let $[K : \mathbb{Q}_p] < \infty$, with normalised valuation v_K and uniformiser π, and write $e := e_{K/\mathbb{Q}_p}$, the absolute ramification index.

Proposition 15.1. *If $r > \frac{e}{p-1}$, then the series*

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

converges on $\pi^r \mathcal{O}_K$, and exp *determines an isomorphism between*

$$(\pi^r \mathcal{O}_K, +) \xrightarrow{\sim} (1 + \pi^r \mathcal{O}_K, \times)$$

Proof. $v_K(n!) = ev_p(n!) = e\frac{n-s_p(n)}{p-1} \leq e\frac{n-1}{p-1}$ - see example sheet 1.

For $x \in \pi^r \mathcal{O}_K$, we have for $n \geq 1$:

$$v_K(x^n/n!) \geq nr - e\frac{n-1}{p-1} = r + (n-1)\left(r - \frac{e}{p-1}\right)$$

Hence $v_K(x^n/n!) \to \infty$ as $n \to \infty$, and hence $\exp(x)$ converges.

Since $v_K\left(\frac{x^n}{n!}\right) \geq r$ for $n \geq 1$, $\exp(x) \in 1 + \pi^r \mathcal{O}_K$.

Similarly, consider $\log : 1 + \pi^r \mathcal{O}_K \to \pi^r \mathcal{O}_K$ given by

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

We can check convergence as before.

Recall properties of power series:

- $\exp(x+y) = \exp(x)\exp(y)$
- $\log(xy) = \log(x) + \log(y)$
- $\exp(\log(x)) = x = \log(\exp(x))$

Thus $\exp : (\pi^r \mathcal{O}_K, +) \to (1 + \pi^r \mathcal{O}_K, \times)$ is an isomorphism of groups. □

Now let K be a non-archimedean local field. We define a filtration on $\mathcal{O}_K^\times$. Write $U_K = \mathcal{O}_K^\times$, the unit group of $\mathcal{O}_K$.

Definition 15.2. *For $s \in \mathbb{Z}_{\geq 1}$, the s^{th} unit group $U_K^{(s)}$ is defined to be*

$$U_K^{(s)} = (1 + \pi^s \mathcal{O}_K, \times)$$

We set $U_K^{(0)} = U_K$. Then we have

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

Proposition 15.3. *We have:*

1. $U_K^{(0)}/U_K^{(1)} \cong (k^\times, \times)$
2. $U_K^{(s)}/U_K^{(s+1)} \cong (k, +)$

Proof.

1. Reduction mod π gives a natural; surjection $O_K^\times \to k^\times$. The kernel is then $1 + \pi O_K = U_K^{(1)}$.
2. Define $f : U_K^{(s)} \to k$ given by $1 + \pi^s x \mapsto x \mod \pi$.

   Then $(1+\pi^s x)(1+\pi^s y) = 1 + \pi^s(x + y + \pi^s xy)$. Since $x + y + \pi^s xy \equiv x + y \mod \pi$, f is a group homomorphism. It is easy to see that f is surjective, and that $\ker f = U_K^{(s+1)}$.

□

Corollary 15.4. *Let $[K : \mathbb{Q}_p] < \infty$. Then $O_K^\times$ has a subgroup of finite index isomorphic to $(O_K, +)$.*

Proof. Let $r > \frac{e}{p-1}$. Then $(O_K, +) \cong U_K^{(r)}$. So $U_K^{(r)} \subseteq U_K$ is of finite index by **15.3**. □

For example, in the case of $\mathbb{Z}_p$, if $p > 2, e = 1$, we can take $r = 1$. Then:

$$\mathbb{Z}_p^\times \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$
$$x \mapsto \left(x \mod p, \frac{x}{[x \mod p]}\right)$$

If $p = 2$, then we need $r = 2$. Then we get:

$$\mathbb{Z}_2^\times \xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + 4\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$$

This gives us another proof of the fact that

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^2 & p = 2 \end{cases}$$

16 Higher Ramification Groups

Let L/K be a finite Galois extension of non-archimedean local fields. We define an analogous filtration of $\mathrm{Gal}(L/K)$:

Definition 16.1. *Let v_L be the normalised valuation on L. For $s \in \mathbb{R}_{\geq -1}$, we define the s^{th} ramification group*

$$G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(x) - x) \geq s + 1 \ \forall x \in O_L\}$$

$G_{-1}(L/K) = \mathrm{Gal}(L/K)$.

$G_0(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) \equiv x \mod \pi_L \ \forall x \in O_L\} = \ker(\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k)) = I_{L/K}$

In general, for $s \in \mathbb{Z}_{\geq 0}$, $G_s(L/K)$ is the kernel of the map $\mathrm{Gal}(L/K) \to \mathrm{Aut}(O_L/\pi_L^{s+1}O_L)$), and hence $G_s(L/K)$ is normal in G.

We have a filtration for $s \in \mathbb{Z}_{\geq 1}$:

$$\ldots \subseteq G_s \subseteq G_{s-1} \subseteq \ldots \subseteq G_{-1} = \mathrm{Gal}(L/K)$$

We have defined G_s for s real, but in fact G_s only changes at the integers. We'll use this definition in terms of real numbers later though.

Theorem 16.2.

1. *Let $\pi_L \in \mathcal{O}_L$ be a uniformizer. For $s \geq 1$, $G_s = \{\sigma \in G_0 : v_L(\sigma(\pi_L) - \pi_L) \geq s + 1\}$.*
2. *$\bigcap_{n=0}^{\infty} G_n = \{1\}$.*
3. *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 the map $\sigma \mapsto \sigma(\pi_L)/\pi_L$. This map is independent of the choice of π_L.

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

1. By **14.8**, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Suppose $v_L(\sigma(\pi_L) - \pi_L) \geq s + 1$. Now let $x \in \mathcal{O}_L$, then $x = f(\pi_L)$ for $t \in \mathcal{O}_K[t]$.

   Then $\sigma(x) - x = \sigma(f(\pi_L)) - f(\pi_L) = f(\sigma(\pi_L)) - f(\pi_L) = (\sigma(\pi_L) - \pi_L)g(\pi_L)$ where $g \in \mathcal{O}_K[t]$, as $\sigma(\pi_L) = \pi_L$ is a root.

   So $v_L(\sigma(x) - x) = v_L(\sigma(\pi_L) - \pi_L) + v_L(g(\pi_L)) \geq s + 1$.
2. Suppose that $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \neq 1$. Then $\sigma(\pi_L) \neq \pi_L$ because $L = K(\pi_L)$, and hence $v_L(\sigma(\pi_L) - \pi_L) < \infty$. Thus $\sigma \notin G_s$ for $s \gg 0$.
3. Note that, for $\sigma \in G_s, s \geq 0$, we have $\sigma(\pi_L) \in \pi_L + \pi_L^{s+1}\mathcal{O}_L$. So then

$$\sigma(\pi_L)/\pi_L \in 1 + \pi_L^s \mathcal{O}_L$$

   We claim that $\varphi : G_s \to U_L^{(s)}/U_L^{(s+1)}$, $\sigma \mapsto \sigma(\pi_L)/\pi_L$ is a group homomorphism with kernel G_{s+1}.

   For the homomorphism part, take $\sigma, \tau \in G_s$, and let $\tau(\pi_L) = u\pi_L, u \in \mathcal{O}_L^\times$. Then:

$$\begin{aligned}\frac{\sigma\tau(\pi_L)}{\pi_L} &= \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)} \cdot \frac{\tau(\pi_L)}{\pi_L} \\ &= \frac{\sigma(u)}{u} \cdot \frac{\sigma(\pi_L)}{\pi_L} \cdot \frac{\tau(\pi_L)}{\pi_L}\end{aligned}$$

   But $\sigma(u) \in u + \pi_L^{s+1}\mathcal{O}_L$ since $\sigma \in G_s$, and thus $\frac{\sigma(u)}{u} \in U_L^{(s+1)}$, and hence

$$\frac{\sigma\tau(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \cdot \frac{\tau(\pi_L)}{\pi_L} \mod U_L^{(s+1)}$$

   so φ is a group homomorphism.

   Moreover, $\ker \varphi = \{\sigma \in G_s : \sigma(\pi_L) \equiv \pi_L \mod \pi_L^{s+2}\} = G_{s+1}$.

   If $\pi_L' = a\pi_L$ is another uniformizer, and $a \in U_L$, then $\sigma(\pi_L')/\pi_L' = \frac{\sigma(a)}{a}\frac{\sigma(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \mod U_L^{(s+1)}$.

□

Corollary 16.3. Gal(L/K) *is solvable.*

Proof. By **15.2**, **16.2**, and **14.4**, for $s \in \mathbb{Z}_{\geq -1}$, $G_s/G_{s+1} \cong$ a subgroup of one of $\begin{cases} \mathrm{Gal}(k_L/k) & s = -1 \\ (k_L^\times, \times) & s = 0 \\ (k_l, +) & s \geq 1 \end{cases}$.

These are all cyclic groups, and hence G_s/G_{s+1} is cyclic for $s \geq -1$.

We thus conclude via **16.2.2** that Gal(L/K) is solvable. □

Let char $K = p$. 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 it is normal) Sylow-p subgroup of $G_0 = I_{L/K}$.

Definition 16.4. *The group G is called the* **wild inertia group** *and G_0/G_1 is the* **tame quotient**.

We say L/K (not necessarily Galois) is **tamely ramified** *if* char $k = p \nmid e_{L/K}$, *which, in the case when L/K is Galois, is equivalent to $G_1 = \{1\}$. Otherwise it is* **wildly ramified**.

We can thus break up L/K into $L/K'/K_0/K$, where L/K' is totally wildly ramified, K'/K_0 is totally tamely ramified, and K_0/K is unramified.

Example. $K = \mathbb{Q}_p$. Let ζ_{p^n} be a primitive $p^{n\text{th}}$ root of unity. Let $L = \mathbb{Q}_p(\zeta_{p^n})$.

Then the $p^{n\text{th}}$ cyclotomic polynomial

$$\Phi_{p^n}(x) = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \ldots + 1$$

is the minimal polynomial of ζ_{p^n}. The following 3 facts are exercises on sheet 3:

- $\Phi_{p^n}(x)$ is irreducible.
- $L/\mathbb{Q}_p$ is Galois and totally ramified of degree $p^{n-1}(p-1)$.
- $\pi := \zeta_{p^n} - 1$ is a uniformizer of $\mathcal{O}_L$, and hence $\mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^n} - 1]$.

Now Gal$(L/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ given by sending $(\sigma_m : \zeta_{p^n} \mapsto \zeta_{p^n}^m) \leftarrow\!\shortmid m$.

Let k be maximal such that $p^k | m-1$. Then $\zeta_{p^n}^{m-1}$ is a primitive $p^{n-k\text{th}}$ root of unity, and so $\zeta_{p^n}^{m-1} - 1$ is a uniformizer π' in $L' := \mathbb{Q}_p(\zeta_{p^n}^{m-1})$.

So $v_L(\sigma(\pi) - \pi) = v_L(\pi') = e_{L/L'} = \frac{e_{L/\mathbb{Q}_p}}{e_{L'/\mathbb{Q}_p}} = \frac{[L:\mathbb{Q}_p]}{[L':\mathbb{Q}_p]} = \frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k$

By **16.2.1**, $\sigma \in G_i \iff p^k \geq i+1$. Thus:

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

These are reminiscent of $U_{\mathbb{Q}_p}^{(k)}$.

16.1 Upper Numbering of Ramification Groups

These ramification groups behave well with respect to taking subgroups:

Proposition 16.5. *Let $L/F/K$ be finite extensions of non-archimedean local fields, with L/K Galois. Then for $s \in \mathbb{R}_{\geq -1}$,*

$$G_s(L/F) = G_s(L/K) \cap \mathrm{Gal}(L/F)$$

Proof. $G_s(L/F) = \{\sigma \in \mathrm{Gal}(L/F) : v_L(\sigma(x) - x) \geq s + 1 \ \forall x \in \mathcal{O}_L\} = \mathrm{Gal}(L/F) \cap G_s(L/K)$ □

However, G_s behave badly with respect to taking quotients. We fix this by renumbering.

Let L/K be finite and Galois. Define a function $\phi := \phi_{L/K} : \mathbb{R}_{\geq -1} \to \mathbb{R}$ by

$$\phi(s) = \int_0^s \frac{1}{[G_0 : G_t]} dt$$

As a convention, we write, for $t \in [-1, 0]$, $\frac{1}{[G_0:G_t]} = [G_t : G_0]$.

We have for $m \leq s < m + 1$,

$$\phi(s) = \begin{cases} s & m = -1 \\ \frac{1}{|G_0|}(|G_1| + \ldots + |G_m| + (s - m)|G_{m+1}|) & m \geq 0 \end{cases}$$

Thus ϕ is continuous, piecewise linear, and strictly increasing.

Fix notation: $L/F/K$ are finite extensions of non-archimedean local fields with L/K and F/K Galois. Take $G := \mathrm{Gal}(L/K)$ and $H := \mathrm{Gal}(L/F)$, and so $G/H = \mathrm{Gal}(F/K)$.

Then for $s \in \mathbb{R}_{\geq -1}$, we will write $G_s, H_s, (G/H)_s$ for the s^{th} higher ramification groups for $G, H, (G/H)$ respectively.

Theorem 16.6 (Herbrand's Theorem)**.** *Let $L/F/K$ be as above. Then for $s \in \mathbb{R}_{\geq -1}$, we have*

$$\frac{G_s H}{H} = (G/H)_{\phi_{L/F}(s)}$$

Proof. Next lecture. □

As $\phi_{L/K}$ is continuous and strictly increasing, we may define $\psi_{L/K} := \phi_{L/K}^{-1}$.

Definition 16.7 (Upper Numbering)**.** *Let L/K be a finite Galois extension of non-archimedean local fields. The higher ramification groups in upper numbering is defined by*

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

We can thus rephrase **16.6** as follows:

Lemma 16.8. *Let $L/F/K$ be as above.*

1. $\phi_{L/K} = \phi_{F/K} \circ \phi_{L/F}$
2. $\psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}$

Proof. Since $\psi = \phi^{-1}$, it suffices to just prove *1*.

$\phi_{L/K}$ and $\phi_{F/K} \circ \phi_{L/F}$ are piecewise linear and $\phi_{L/K}(0) = \phi_{F/K} \circ \phi_{L/F}(0) = 0$. Then it suffices to show that their derivatives are equal.

Let $r = \phi_{L/F}(s)$. Then

$$\begin{aligned}(\phi_{F/K} \circ \phi_{L/F})'(s) &= \phi'_{L/F}(s)\phi'_{F/K}(r) \\ &= \frac{|H_s|}{|H_0|}\frac{|(G/H)|_r}{|G/H|_0} \\ &= \frac{|H_s|}{e_{L/F}}\frac{|(G/H)_r|}{e_{F/K}}\end{aligned}$$

Now **16.6** implies that $(G/H)_r = \frac{G_s H}{H} = \frac{G_s}{G_s \cap H} = \frac{G_s}{H_s}$ by **16.3**.

So $\phi'_{L/K}(s) = \frac{|G_s|}{|G_0|} = \frac{|H_s||(G/H)_R|}{e_{L/K}}$, and $e_{L/K} = e_{L/F}e_{F/K}$, so we are done. □

Corollary 16.9. *For $t \in [-1, \infty]$, we have*

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

Proof. Let $r = \psi_{F/K}(t)$. Then

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

. □

17 Proof of Herbrand's Theorem

Let $L/F/K$ be finite extensions of non-archimedean local fields, with $L/K, F/K$ Galois, with $G = \mathrm{Gal}(L/K), H = \mathrm{Gal}(L/F)$.

Recall Herbrand's theorem:

Theorem 16.6 (Herbrand's Theorem).

$$G_s H/H = (G/H)_{\phi_{F/L}(s)}$$

We introduce an auxiliary function:

Definition 17.1. *Let L/K be finite and Galois, with $\sigma \in \mathrm{Gal}(L/F)$. Then we define:*

$$\begin{aligned}i_{L/K} &: \mathrm{Gal}(L/K) \to \mathbb{Z} \\ i_{L/K}(\sigma) &= \min_{x \in \mathcal{O}_L} v_L(\sigma(x) - x) \\ &= \max\{i \in \mathbb{Z} : \sigma \in G_{i-1}\}\end{aligned}$$

By convention, $i_{L/K}(1) = \infty$.

Note that $G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : i_{L/K}(\sigma) \geq s + 1\}$.

Lemma 17.2. *Let L/K be finite and Galois. Let $x \in \mathcal{O}_L$ such that $\mathcal{O}_K[x] = \mathcal{O}_L$. Then:*

1. $i_{L/K}(\sigma) = v_L(\sigma(x) - x)$.
2. $G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(x) - x) \geq s + 1\}$.

Proof. Let $y \in \mathcal{O}_L$, then $y = f(x)$ for some polynomial $f \in \mathcal{O}_K[X]$. The same argument as in **15.6.1** shows that $\sigma(x) - x | \sigma(y) - y$ in $\mathcal{O}_L$.

Hence $v_L(\sigma(y) - y) \geq v_L(\sigma(x) - x)$, and we have both parts. □

Proposition 17.3. *Let $L/F/K$ be as above, and let $\sigma \in G$. Then we have*

$$i_{F/K}(\sigma H) = e_{L/F}^{-1} \sum_{\tau \in H} i_{L/K}(\sigma\tau)$$

Proof. When $\sigma = 1$, we interpret this as "$\infty = \infty$".

When $\sigma \neq 1$, let v_L and v_F denote the normalised valuations on L and F. Let $x \in \mathcal{O}_F, y \in \mathcal{O}_L$, such that $\mathcal{O}_F = \mathcal{O}_K[x]$, and $\mathcal{O}_L = \mathcal{O}_K[y]$.

Define $a := \sigma(x) - x \in \mathcal{O}_L$, and $b := \prod_{\tau \in H}(\sigma\tau(y) - y) \in \mathcal{O}_L$.

Then $e_{L/F} i_{F/K}(\sigma H) = e_{L/F} v_F(\sigma(x) - x) = v_L(\sigma(x) - x) = v_L(a)$.

And $\sum_{\tau \in H} i_{L/K}(\sigma\tau) = \sum_{\tau \in H} v_L(\sigma\tau(y) - y) = v_L(\prod_{\tau \in H}(\sigma\tau(y) - y)) = v_L(b)$.

We need to show that $v_L(a) = v_L(b)$. We will show this by showing that $a|b$ and $b|a$ in $\mathcal{O}_L$.

For $a|b$, let $f \in \mathcal{O}_F[X]$ be the minimal polynomial for y over $\mathcal{O}_F$. Then

$$f(x) = \prod_{\tau \in H}(X - \tau(y))$$

and $\sigma(f)(X) = \prod_{\tau \in H}(X - \sigma\tau(y))$.

Since $\mathcal{O}_F = \mathcal{O}_K[x]$, $a = \sigma(x) - x$ divides $\sigma(z) - z$ for all $z \in \mathcal{O}_F$.

Thus a divides all coefficients of $\sigma(f)(X) - f(X)$, and so $a|\sigma(f)(y) - f(y) = \sigma(f)(y) = \pm b$.

For $b|a$, let $g \in \mathcal{O}_K[X]$ be such that $x = g(y)$. Then $g(X) - x \in \mathcal{O}_F[X]$ has y as a root, and so $g(X) - x = f(X)h(X)$ for some $h \in \mathcal{O}_F[X]$.

Applying σ and evaluating at y gives:

$$\sigma(g)(y) - \sigma(x) = \sigma(f)(y)\sigma(h)(y) = b\sigma(g)(y)$$

But $\sigma(h)(y) \in \mathcal{O}_L$, and $\sigma(g)(y) = g(y) = x$, and $b|a$. □

Lemma 17.4. *Let L/K be a finite Galois extension of non-archimedean local fields, and $\sigma \in G = \mathrm{Gal}(L/K)$. Then*

$$\phi_{L/K}(s) = -1 + \frac{1}{|G_0|} \sum_{\sigma \in G} \min\{i_{L/K}(\sigma), s + 1\}$$

for any $s \in \mathbb{R}_{\geq 1}$.

Proof. Since both sides are piecewise linear and continuous. Let $\theta(s) = \text{RHS}$. Then $\phi_{L/K}(-1) = -1 = \theta(-1)$.

Thus it suffices to show $\theta' = \phi'_{L/K}$.

$\theta'(u) = \frac{1}{|G_0|} \cdot \#\{\sigma \in G : i_{L/K}(\sigma) \geq s+1\} = \frac{|G_s|}{|G_0|} = \phi'_{L/K}$ by the fundamental theorem of calculus. $\square$

Proof of Herbrand's Theorem. Define a function $j : G/H \to \mathbb{Z} \cup \{\infty\}$ by

$$j(\sigma H) = \max_{\tau \in H}\{i_{L/K}(\sigma\tau)\}$$

for $\sigma \in G$.

Then we have $\sigma H \in G_s H/H \iff j(\sigma H) - 1 \geq s \iff \phi_{L/F}(j(\sigma H) - 1) \geq \phi_{L/F}(s)$, as ϕ is strictly increasing.

On the other hand, we have $\sigma H \in (G/H)_{\phi_{L/F}(s)} \iff i_{F/K}(\sigma H) - 1 \geq \phi_{L/F}(s)$

Thus it suffices to show

$$\phi_{L/F}(j(\sigma H) - 1) = i_{F/K}(\sigma H) - 1 \tag{$*$}$$

We can assume $\sigma \notin H$, as then this just say "$\infty = \infty$". Upon replacing σ by another element in σH, we may assume

$$j(\sigma H) = i_{L/K}(\sigma) =: m$$

i.e. $\sigma \in G_{m-1} \setminus G_m$.

Now if $\tau \in H_{m-1} = G_{m-1} \cap H$, then $\sigma\tau \in G_{m-1} \implies i_{L/K}(\sigma\tau) \geq m$, and so $i_{L/K}(\sigma\tau) = m$, by maximality of m.

On the other hand, if $\tau \notin H_{m-1}$, then $\sigma\tau \notin G_{m-1}$, and so $i_{L/K}(\sigma\tau) < m$, and $i_{L/K}(\sigma\tau) = i_{L/K}(\tau)$.

In either case, we have, for any $\tau \in H$, we have $i_{L/K}(\sigma\tau) = \min(i_{L/K}(\tau), m)$.

By **17.3**, we have

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

But $i_{L/K}(\tau) = i_{L/F}(\tau)$ and $e_{L/F} = |H_0|$.

Thus **17.4** gives us that

$$\begin{aligned} i_{F/K}(\sigma H) &= \frac{1}{|H_0|} \sum_{\tau \in H} \min(i_{L/F}(\tau, m)) \\ &= \phi_{L/F}(m-1) + 1 \\ &= \phi_{L/F}(j(\sigma H) - 1) + 1 \end{aligned}$$

and so we have $(*)$. $\square$

For example, take $K = \mathbb{Q}_p, L = \mathbb{Q}_p(\zeta_{p^n})$. Then $G \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Let $k \in \mathbb{Z}, 1 \leq k \leq n-1$. For $p^{k-1} - 1 < s \leq p^k - 1$, we have

$$G_s \cong \{m \in (\mathbb{Z}/p^n\mathbb{Z})^\times : m \equiv 1 \mod p^k\}$$

Let's compute $\phi_{L/K}$. Since G_s jumps at p^{k-1}, we have $\phi_{L/K}$ linear on $[p^{k-1} - 1, p^k - 1]$.

It suffices to determine $\phi_{L/K}(p^k - 1)$.

We claim $\phi_{L/K}(p^k - 1) = k$. This follows as $[G_0 : G_k] = p^k(p-1)$.

Thus $G^s \cong \begin{cases} (\mathbb{Z}/p^n\mathbb{Z})^\times & s \le 0 \\ (1+p^k\mathbb{Z})/p^n\mathbb{Z} & k-1 < s \le k \\ \{1\} & s > n-1 \end{cases}$. Note that $\phi(p^k - 1)$ is an integer - this is a priori not clear.

Definition 17.5. *We say i is a* **jump in a the filtration** $(G^s)_{s\in R_{\ge -1}}$ *if $G^i \neq G^j$ for all $j > i$.*

Theorem 17.6 (Hasse-Arf). *If* $\mathrm{Gal}(L/K)$ *is abelian, then the jumps of the filtration* $(G^s)_{s\in\mathbb{R}_{\ge -1}}$ *can be only be at integers.*

Proof. Omitted. See Serre: Local Fields, chapter 4, section 7. □

18 Local Class Field Theory

18.1 Infinite Galois Theory

Let L/K be an algebraic extension of fields.

Definition 18.1. *L/K is* **separable** *if, for every $\alpha \in L$, the minimal polynomial $f_\alpha(x) \in K[x]$ for α is separable. It is* **normal** *if $f_\alpha(x)$ splits in L for all $\alpha \in K$.*

We then say that L/K is Galois if it is separable and normal. In this case, we write

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$$

If L/K is finite and Galois, then the Galois correspondence tells us that there is a bijection:

$$\begin{array}{ccc} \{\text{subextensions } K \subseteq K' \subseteq L\} & \longleftrightarrow & \{\text{subgroups of } \mathrm{Gal}(L/K)\} \\ K' & \longmapsto & \mathrm{Gal}(L/K') \end{array}$$

For L/K infinite, we need to introduce a topology. Let $(I \le)$ be a partially ordered set. We say that I is ***directed*** if, for all $i, j \in I$, there is some $k \in I$ such that $i \le k, j \le k$. For example:

- Any total ordered set (e.g. $(\mathbb{N}, \le)$)/
- $(\mathbb{N}_{\ge 1}, |)$ ordered by divisibility.

Definition 18.2. *Let $(I, \le)$ be a directed set and $(G_i)_{i\in I}$ a collection of groups together with transition maps $\varphi_{ij} : G_j \to G_i$ for $i \le j$ such that $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ whenever $i \le j \le k$, and $\varphi_{ii} = \mathrm{id}$.*

We then say that $((G_i)_{i\in I}, \varphi_{ij})$ is an **inverse system**, *and we can define the* **inverse limit** *of $((G_i)_{i\in I}, \varphi_{ij})$ as*

$$\varprojlim_{i\in I} G_i = \{(G_i)_{i\in I} \in \prod_{i\in I} G_i | \varphi_{ij}(g_j) = g_i\}$$

For $I = (\mathbb{N}, \le)$, this is just our previous definition. There are projection maps $\psi_j : \varprojlim_{i\in I} G_i \to G_j$, and this inverse limit satisfies a universal property.

If all the G_i are finite, then we can define the profinite topology on $\varprojlim_{i\in I} G_i$ as the weakest topology such that the ψ_j are continuous for all j.

Proposition 18.3. *Let L/K be Galois. Then*

1. *The set $I = \{F/K \text{ finite } : F \subseteq L, L/K \text{ Galois}\}$ is a directed set under $\subseteq$.*
2. *For $F, F' \in I, F \subseteq F'$, there is a restriction map $res_{F,F'} : \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$, and the natural map*
$$\mathrm{Gal}(L/K) \to \varprojlim_{F \in I} \mathrm{Gal}(F/K)$$
is an isomorphism.

Proof. Example sheet 4. □

We say that $\mathrm{Gal}(L/K)$ packages all the information of $\mathrm{Gal}(F/K)$ for all finite Galois subextensions.

For example, if $K = \mathbb{F}_q, L = \bar{\mathbb{F}}_q$, then we have a bijection between the finite Galois extensions of $\mathbb{F}_q$ and $\mathbb{N}_{\geq 1}$, namely $\mathbb{F}_{q^n} \mapsto n$.

We then have $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ if and only if $m|n$. The restriction map looks something like:

$$\begin{tikzcd}
\mathrm{Frob}_q \arrow[r, hook, "\text{generates}"] \arrow[d, leftrightarrow] & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \arrow[r, two heads, "\text{res}"] \arrow[d, leftrightarrow, "\cong"] & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \arrow[d, leftrightarrow, "\cong"] & \mathrm{Frob}_q \arrow[l, hook', "\text{generates}"'] \arrow[d, leftrightarrow] \\
1 \arrow[r, hook, "\text{generates}"] & \mathbb{Z}/n\mathbb{Z} \arrow[r, two heads, "\text{proj}"] & \mathbb{Z}/m\mathbb{Z} & 1 \arrow[l, hook', "\text{generates}"']
\end{tikzcd}$$

So $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim_{n \in (N_{\geq 1}, |)} \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}$, generated by the Frobenius automorphism.

On example sheet 3, we show that $\widehat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p$.

Now we then have $\mathrm{Gal}(L/K)$ endowed with the profinite topology, and:

Theorem 18.4 (Fundamental Theorem of Galois Theory)**.** *Let L/K be Galois. Then there is a bijection*
$$\{F/K \text{ subextensions of } L/K\} \leftrightarrow \{\text{closed subgroups of } \mathrm{Gal}(L/K)\}$$
given by $F \mapsto \mathrm{Gal}(L/F)$, $L^H \hookleftarrow H$.

Moreover, F/K is finite if and only if $\mathrm{Gal}(L/F)$ is open, and F/K is Galois if and only if $\mathrm{Gal}(L/F)$ is normal in $\mathrm{Gal}(L/K)$.

Proof. Omitted. □

18.2 Weil Group

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

Definition 18.5.

1. *L/K is unramified if F/K is unramified for all F/K finite subextensions.*
2. *L/K is totally ramified if F/K is totally ramified for all F/K finite subextensions.*

Proposition 18.6. *Let L/K be unramified. Then L/K is Galois, and*
$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$$

Proof. Every finite subextension F/K is unramified, hence Galois, and so L/K is normal and separable hence Galois.

Moreover, there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(L/K) \arrow[r, "\mathrm{res}"] \arrow[d, "\cong"] & \mathrm{Gal}(k_L/k) \arrow[d, "i"] \\
\varprojlim_{\substack{F/K \text{finite} \\ F\subseteq L}} \mathrm{Gal}(F/K) \arrow[r] & \varprojlim_{\substack{F/K \text{finite} \\ F\subseteq L}} \mathrm{Gal}(k_F/k)
\end{tikzcd}$$

Now $\varprojlim_{\substack{F/K \text{finite} \\ F\subseteq L}} \mathrm{Gal}(k_F/k) \cong \varprojlim_{\substack{L/k \text{finite} \\ L\subseteq k_L}} \mathrm{Gal}(L/k) \cong \mathrm{Gal}(k_L/k)$, where first isomorphism comes from **14.4** and the second by **18.4**. Hence i is an isomorphism. $\square$

On example sheet 3, we will show $L_1/K, L_2/K$ finite unramified implies that L_1L_2/K unramified.

Thus, for any L/K, there is a maximal unramified subextension K_0/K. There is a surjection

$$\mathrm{res} : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K_0/K) \cong \mathrm{Gal}(k_l/k)$$

and we write $I_{L/K}$ for the kernel of res, and call the ***inertia subgroup***.

Finally, we let $\mathrm{Frob}_{k_L/k} \in \mathrm{Gal}(k_L/k)$ be the Frobenius map $x \mapsto x^{|k|}$, and we let $\langle \mathrm{Frob}_{k_L/k}\rangle$ be the subgroup generated by $\mathrm{Frob}_{k_L/k}$.

Definition 18.7. *Let L/K be Galois. Then the* **Weil group** *$W(L/K)$ is the subgroup of* $\mathrm{Gal}(L/K)$ *which maps to $\langle \mathrm{Frob}_{k_L/k}\rangle \subseteq \mathrm{Gal}(k_L/k)$, i.e. $\mathrm{res}^{-1}(\langle \mathrm{Frob}_{k_L/k}\rangle)$.*

Note that if k_L/k is finite, then $W(L/K) = \mathrm{Gal}(L/K)$. There is a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & I_{L/K} \arrow[r] \arrow[d, leftrightarrow] & W(L/K) \arrow[r] \arrow[d, hook] & \langle \mathrm{Frob}_{k_L/k}\rangle \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & I_{L/K} \arrow[r] & \mathrm{Gal}(L/K) \arrow[r] & \mathrm{Gal}(k_L/K) \arrow[r] & 0
\end{tikzcd}$$

with exact rows.

We endow $W(L/K)$ with the weakest topology such that $I_{L/K}$ is an open subgroup of $W(L/K)$ equipped with its subspace $I_{L/K} \subseteq \mathrm{Gal}(L/K)$.

Warning: If k_L/k is infinite, this is not the subspace topology on $W(L/K) \subseteq \mathrm{Gal}(L/K)$.

Proposition 18.8. *If L/K is a Galois extension of local fields, then:*

1. *$W(L/K)$ is dense in* $\mathrm{Gal}(L/K)$.
2. *If F/K is a finite subextension of L/K, then $W(L/F) = W(L/K) \cap \mathrm{Gal}(L/F)$.*
3. *If F/K is a finite Galois subextension, then*

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

Proof.

1. $W(L/K)$ is dense in $\mathrm{Gal}(L/K)$ if and only if, for all finite Galois subextensions F/K, $W(L/K)$ intersects every coset of $\mathrm{Gal}(L/F)$, which occurs if and only if $W(L/K)$ surjects onto $\mathrm{Gal}(F/K)$.

   But note we have a diagram

$$\begin{tikzcd} 0 \arrow[r] & I_{L/K} \arrow[r] \arrow[d, "a"] & W(L/K) \arrow[r] \arrow[d, "b"] & \langle \mathrm{Frob}_{k_L/k} \rangle \arrow[r] \arrow[d, "c"] & 0 \\ 0 \arrow[r] & I_{F/K} \arrow[r] & \mathrm{Gal}(F/K) \arrow[r] & \mathrm{Gal}(k_F/K) \arrow[r] & 0 \end{tikzcd}$$

   Example sheet 4 tells us that a is then surjective.

   Since $\mathrm{Gal}(k_F/k)$ is generated by $\mathrm{Frob}_{k_F/k}$, c is surjective, and then a diagram chase gives b is surjective.

2. F/K is finite. There is a commutative diagram

$$\begin{tikzcd} \mathrm{Gal}(L/K) \arrow[r, two heads] & \mathrm{Gal}(k_L/K) & \langle \mathrm{Frob}_{k_L/k} \rangle \arrow[l, hook'] \\ \mathrm{Gal}(L/F) \arrow[r, two heads] \arrow[u, hook] & \mathrm{Gal}(k_L/k_F) \arrow[u, hook] & \langle \mathrm{Frob}_{k_L/k_F} \rangle \arrow[l, hook'] \arrow[u, hook] \end{tikzcd}$$

   Hence for $\sigma \in \mathrm{Gal}(L/F)$, $\sigma \in W(L/F) \iff \sigma|_{k_L} \in \langle \mathrm{Frob}_{k_L/k_F} \rangle \iff \sigma|_{k_L} \in \langle \mathrm{Frob}_{k_L/k} \rangle \iff \sigma \in W(L/K)$.

3. $\frac{W(L/K)}{W(L/F)} = \frac{W(L/K)}{W(L/K)\cap \mathrm{Gal}(L/F)} \cong \frac{W(L/K)\,\mathrm{Gal}(L/F)}{\mathrm{Gal}(L/F)} \cong \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)} \cong \mathrm{Gal}(F/K)$.

□

19 Local Class Field Theory

Let K be a non-archimedean local field.

Definition 19.1. *We say L/K is* **abelian** *if it is Galois and* $\mathrm{Gal}(L/K)$ *is an abelian group.*

If $L_1/K, L_2/K$ are abelian then it is a fact that

1. L_1L_2/K is abelian
2. If $L_1 \cap L_2 = K$, then there is a canonical isomorphism $\mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

We also have as a fact that there is a maximal abelian extension of K, which we denote as K^{ab}.

For example, let K^{ur} denote the maximal unramified extension of K inside K^{sep}. Then:

$$K^{ur} = \bigcup_{m=1}^{\infty} K(\zeta_{q^m-1})$$

where $|k| = q$, $k_{K^{ur}} \cong \bar{\mathbb{F}}_q$.

Then $\mathrm{Gal}(K^{ur}/K) \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$.

So K^{ur} is abelian, and hence contained in K^{ab}. Then we have an exact sequence:

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

For L/K unramified, let $\mathrm{Frob}_{L/K} \in \mathrm{Gal}(L/K)$ correspond to the Frobenius automorphism on k_L/k (as $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$).

Theorem 19.2.

1. *(Local Artin Reciprocity). There exists a unique topological isomorphism (i.e. an isomorphism of groups and a homeomorphism of topological spaces):*

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

   satisfying the properties:

   (a) $\mathrm{Art}_K(\pi)|_{K^{ur}} = \mathrm{Frob}_{K^{ur}/K}$ *for any uniformiser* $\pi \in K$.

   (b) For each finite subextension L/K in K^{ab}/K

$$\mathrm{Art}_K(N_{L/K}(L^\times))|_L = \{1\}$$

   Art_K *is called the Artin Reciprocity map.*

2. *Let L/K be finite abelian. Then* Art_K *induces an isomorphism:*

$$\frac{K^\times}{N_{L/K}(L^\times)} \cong \frac{W(K^{ab}/K)}{W(K^{ab}/L)} \cong \mathrm{Gal}(L/K)$$

Remark: $\mathrm{Frob}_{K^{ur}/K}$ lifts $x \mapsto x^q$ in $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F})$. This is called the "arithmetic Frobenius." It has an inverse, $(\mathrm{Frob}_{K^{ur}/K})^{-1}$, called the "geometric Frobenius." There is another normalisation of Art_K with $\mathrm{Art}_K(\pi)|_{K^{ur}} = (\mathrm{Frob}_{K^{ur}/K})^{-1}$.

19.1 Properties of the Artim map

- (Existence theorem). For $H \subseteq K^\times$ and open finite subgroup, there is 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

$$\begin{array}{rcl} \{\text{Open finite index subgroup of } K^\times\} & \longleftrightarrow & \{\text{finite abelian extensions } L/K\} \\ H & \longmapsto & (K^{ab})^{\mathrm{Art}_K(H)} \\ N_{L/K}(L^\times) & \longleftarrow\!\shortmid & L/K \end{array}$$

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

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

- (Compatibility with Higher ramification groups).

Definition 19.3. *Let L/K be Galois. For $s \in \mathbb{R}_{\geq -1}$, we define*

$$G^s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma|_F \in G^s(F/K) \text{ for all } F/K \text{ finite Galois subextensions}\}$$

Corollary **16.7** tells us that $G^s(L/K)$ is well defined.

Let $s \in \mathbb{Z}_{\geq 0}$. Then:

$$\mathrm{Art}_K(U_K^{(s)}) = G^s(K^{ab}/K)$$

Note that $G^s(K^{ab}/K) \subseteq I_{K^{ab}/K} \subseteq W(K^{ab}/K)$ for $s \geq 0$.

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

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

We also saw on example sheet 3 that $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ gives a totally ramified extension of degree $p^{n-1}(p-1)$, with

$$\theta_n : \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$$

For $n \geq m \geq 1$, there is a diagram

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \arrow[r] \arrow[d, "\theta_n"] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) \arrow[d, "\theta_m"] \\
(\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r] & (\mathbb{Z}/p^m\mathbb{Z})^\times
\end{tikzcd}$$

Now 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

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

We have $\mathbb{Q}_p(\zeta_{p^\infty}) \cap \mathbb{Q}_p^{ur} = \mathbb{Q}_p$.

It then follows that there is an isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times$$

Theorem 19.4 (Local Kronecker-Weber)**.**

$$\mathbb{Q}_p^{ab} = \mathbb{Q}_p^{ur}\mathbb{Q}_p(\zeta_{p^\infty})$$

Proof. Later. □

The Artin map can now be constructed as follows:

We have $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times; p^n u \mapsto (n, u)$. Then

$$\mathrm{Art}_{\mathbb{Q}_p}(p^n u) = ((\mathrm{Frob}_{\mathbb{Q}_p^{ur}/\mathbb{Q}_p})^n, \theta^{-1}(u))$$

This definition actually involves an arbitrary choice of a totally ramified extension $\mathbb{Q}_p(\zeta_{p^\infty})$, and there is no "maximal totally ramified extension" of $\mathbb{Q}_p$. For example, see example sheet 3 q6(b). We also make a choice of a uniformizer p, which determines the isomorphism

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$$

These choices are actually related, and in fact they "cancel out", so that $\mathrm{Art}_{\mathbb{Q}_p}$ is in fact canonical.

19.3 General Case

$\mathrm{Art}_{\mathbb{Q}_p}$ was constructed by constructing a totally ramified extension $\mathbb{Q}_p(\zeta_{p^n})$ with

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \cong U_{\mathbb{Q}_p}^{(0)}/U_{\mathbb{Q}_p}^{(s)}$$

In general, if K is a local field and π a uniformiser of K, then we construct for $n \geq 1$ a totally ramified extension $K_{\pi/n}/K$ satisfying the following:

1. $K \subseteq \ldots \subseteq K_{\pi,n} \subseteq K_{\pi,n+1} \subseteq \ldots$
2. For $n \geq m \geq 1$ there is a diagram

$$\begin{tikzcd} \mathrm{Gal}(K_{\pi,n}/K) \arrow[r, two heads] \arrow[d, hook, two heads, "\psi_n"] & \mathrm{Gal}(K_{\pi,m}/K) \arrow[d, hook, two heads, "\psi_m"] \\ O_K^\times/U_K^{(n)} \arrow[r, two heads, "\text{canon. proj.}"] & O_K^\times/U_K^{(m)} \end{tikzcd}$$

3. Setting $K_{\pi,\infty} := \bigcup_{n=1}^{\infty} K_{\pi,n}$, we have

$$K^{ab} = K^{ur} K_{\pi,\infty}$$

Since $O_K^\times = U_K^{(0)} \cong \varprojlim_n O_K^\times/U_K^{(n)}$, (2) gives an isomorphism $\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \cong O_K^\times$. We can define Art_K by

$$K^\times \cong \mathbb{Z} \times O_K^\times \to \mathrm{Gal}(K^{ur}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K)$$
$$(\pi^n, u) \mapsto ((\mathrm{Frob}_{K^{ur}/K})^n, \psi^{-1}(u))$$

We have the following picture:

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}_p^{(ab)} \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}_p^{ur} \arrow[dr, dash, "\widehat{\mathbb{Z}}"'] & & \mathbb{Q}_p(\zeta_{p^\infty}) \arrow[dl, dash, "\mathbb{Z}_p^\times"] \\ & \mathbb{Q}_p & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] & K^{ab} \arrow[dl, dash] \arrow[dr, dash] & \\ K^{ur} \arrow[dr, dash, "\widehat{\mathbb{Z}}"'] & & K_{\pi,\infty} \arrow[dl, dash, "O_K^\times"] \\ & K & \end{tikzcd}$$

The goal is then to construct these extensions $K_{\pi,n}$.