# Local Fields *

Zhiyuan Bai

Compiled on May 31, 2023

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part III course *Local Fields* in Michaelmas 2022. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

## Contents



*Based on the lectures under the same name taught by Dr. R. Zhou in Michaelmas 2022.

# 0 Introduction

Number theorists have been studying Diophantine equations since the dawn of time. They are integer polynomial equations, possibly in several variables. And what we're interested in are the integer solutions to these kinds of equations, which are notoriously hard to study. What's easier to study are the solutions of the equation modulo an integer, usually a prime or a prime power, which (at the very worst case) one can solve by enumeration. The theory of local fields package these kind of information together.

# 1 Basic Theory

## 1.1 Absolute Values

**Definition 1.1.** Let $K$ be a field. An absolute value on $K$ is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying:
(i) $|x| = 0$ iff $x = 0$.
(ii) $|xy| = |x||y|$ for all $x, y \in K$.
(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.
A field equipped with an absolute value is called a valued field.

**Example 1.1.** 1. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $|\cdot|$ the usual absolute value $|a + ib| = \sqrt{a^2 + b^2}$. We write $|\cdot|_\infty$ to denote this absolute value.
2. For any field $K$, we can define the trivial absolute value given by $|x| = 1$ if $x \in K^\times$ and $|0| = 0$. It's clear that this is the only absolute value on a finite field, since every nonzero element has a positive power equals to 1.
We henceforth only consider nontrivial absolute values.
3. For a prime $p$, we can define the $p$-adic absolute value on $\mathbb{Q}$ in the following way: For $0 \neq x \in \mathbb{Q}$, we can write $x = p^n a/b$ where $a, b \in \mathbb{Z}, p \nmid a, b$. We then define the $p$-adic absolute value as $|x|_p = p^{-n}$. And of course we still have $|0|_p = 0$.
The axioms are mostly easy to check. As for the triangle inequality, suppose we have another rational number $y = p^m c/d$ written in the form as described. WLOG $m \geq n$, then $|x + y|_p = |p^n(ad + p^{m-n}bc)/(bd)|_p \leq p^{-n} = \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$. The inequality $|x + y| \leq \max\{|x|, |y|\}$ is called the ultrametric inequality, which we'll come back later.

Needless to say, an absolute value on $K$ induces a metric topology via $d(x,y) = |x-y|$.

**Definition 1.2.** Two absolute values $|\cdot|, |\cdot|'$ on a field $K$ are equivalent iff they induce the same topology on $K$. An equivalence class of absolute values on $K$ is called a place of $K$.

Bad definition calls for equivalent forms.

**Proposition 1.1.** *For two absolute values $|\cdot|, |\cdot|'$ on a field $K$, the followings are equivalent:*
*(i) $|\cdot|, |\cdot|'$ are equivalent.*
*(ii) $|x| < 1$ iff $|x|' < 1$.*
*(iii) There is some $c > 0$ such that $|x|' = |x|^c$ for all $x \in K$.*

*Proof.* (i) $\implies$ (ii): $|x| < 1$ iff $(x^n)_n$ converges to 0 in $|\cdot|$ iff $(x^n)_n$ converges to 0 in $|\cdot|'$ iff $|x|' < 1$.
(ii) $\implies$ (iii): Let $a \in K^\times$ be such that $|a| > 1$ (exists since our absolute values are nontrivial). For every $x \in K^\times$, we want to show that $\log|x|/\log|a| = \log|x|'/\log|a|'$. Suppose to the contrary that this is not the case, then WLOG $\log|x|/\log|a| < \log|x|'/\log|a|'$, so we can choose some $m, n \in \mathbb{Z}, n > 0$ such that $\log|x|/\log|a| < m/n < \log|x|'/\log|a|'$. Rearranging, we have $n\log|x| < m\log|a|$ and $n\log|x|' > m\log|a|'$ and therefore $|x^n/a^m| < 1$ yet $|x^n/a^m|' > 1$, contradiction.
(iii) $\implies$ (i): Transparent. □

*Remark.* $|\cdot|_\infty^2$ is not an absolute value in our definition. Some authors replace the triangle inequality with $\exists \beta > 0, |x+y|^\beta \le |x|^\beta + |y|^\beta$ to circumvent this problem for whatever reason.

This course mainly focuses on non-Archimedean absolute values.

**Definition 1.3.** An absolute value is non-Archimedean if it satisfies the ultrametric inequality, i.e. $|x+y| \le \max\{|x|, |y|\}$. We say it is Archimedean if it is not non-Archimedean.

**Example 1.2.** Over $\mathbb{Q}$, $|\cdot|_\infty$ is Archimedean whereas $|\cdot|_p$ is non-Archimedean.

**Lemma 1.2** ("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.* $|x-y| \le \max\{|x|, |y|\} = |y|$. On the other hand, $|y| = |y-x+x| \le \max\{|x|, |x-y|\}$. If $|x| \ge |x-y|$ then $|y| \le \max\{|x|, |x-y|\} \le |x|$ which is not true, so $|x| < |x-y|$ and $|y| \le \max\{|x|, |x-y|\} = |x-y|$. □

Convergence is very easy to study over non-Archimedean fields.

**Proposition 1.3.** *Let $(K, |\cdot|)$ be non-Archimedean and $(x_n)_n$ a sequence in $K$. Then $(x_n)_n$ is Cauchy iff $|x_n - x_{n+1}| \to 0$ as $n \to \infty$.*

In particular, if $K$ happens to be complete, then $(x_n)_n$ converges in this case.

*Proof.* Suppose $|x_n - x_{n+1}| \to 0$ as $n \to \infty$ For $\epsilon > 0$, we choose large enough $N$ such that $|x_n - x_{n+1}| < \epsilon$ for all $n \geq N$. Then any $m, n \geq N$ (say $m > n$) would have

$$|x_n - x_m| = \left| \sum_{i=0}^{m-1} x_{n+i} - x_{n+i+1} \right| \leq \max_{0 \leq i \leq m-1} |x_{n+i} - x_{n+i+1}| < \epsilon$$

as desired. □

**Example 1.3.** Let $p = 5$. We shall construct a sequence $(x_n)_n$ with $x_n^2 + 1 \equiv 0 \pmod{5^n}$ and $x_n \equiv x_{n+1} \pmod{5^n}$. We do ths as follows: Starting with $x_1 = 2$. Once $x_n$ is constructed, we consider $x = x_n + b5^n$. Then $x^2 + 1 \equiv x_n^2 + 2bx_n 5^n + 1 \equiv a5^n + 2bx_n 5^n \pmod{5^{n+1}}$ for some integer $a$. Solving $a + 2bx_n \equiv 0 \pmod 5$ (which is possible since we must have $5 \nmid x$) gives some $b$ with $x^2 + 1 \equiv 0 \pmod{5^{n+1}}$. Setting $x_{n+1} = x$ finishes the construction.
By the preceding proposition, $(x_n)_n$ is $|\cdot|_5$-Cauchy. Suppose it converges to some $l \in \mathbb{Q}$, then we must have $x_n^2 \to l^2$ as $n \to \infty$. But our construction means that $x_n^2 \to -1$, contradiction. Hence $(\mathbb{Q}, |\cdot|_5)$ is not complete.

**Definition 1.4.** The $p$-adic numbers $\mathbb{Q}_p$ is the metric completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Fix a non-Archimedean valued field $(K, |\cdot|)$. For $x \in K$ and $r > 0$, we define $B(x, r) = \{y \in K : |x - y| < r\}$ and $\bar{B}(x, r) = \{y \in K : |x - y| \leq r\}$.

**Lemma 1.4.** *(i) ("open balls don't have centres') If $z \in B(x, r)$, then $B(z, r) = B(x, r)$.*
*(ii) ("closed balls don't have centres') If $z \in \bar{B}(x, r)$, then $\bar{B}(z, r) = \bar{B}(x, r)$.*
*(iii) ("open balls are closed") $B(x, r)$ is closed.*
*(iv) ("closed balls are open") $\bar{B}(x, r)$ is open.*

*Proof.* (i) Let $y \in B(x, r)$, then $|x - y| < r$, so $|z - y| \leq |z - x + x - y| \leq \max\{|z - x|, |x - y|\} < r$, so $B(x, r) \subset B(z, r)$. Similarly $B(z, r) \subset B(x, r)$.
(ii) Essentially the same as (i).
(iii) Suppose $y \notin B(x, r)$. If $z \in B(x, r) \cap B(y, r)$, then by (i) we have $B(x, r) = B(z, r) = B(y, r)$, contradiction. Hence $B(x, r) \cap B(y, r) = \varnothing$, so $B(x, r)$ has open complement, therefore $B(x, r)$ is closed.
(iv) For $y \in \bar{B}(x, r)$, we have $y \in B(y, r) \subset \bar{B}(y, r) = \bar{B}(x, r)$ by (i) and (ii). □

## 1.2 Valuations

**Definition 1.5.** Let $K$ be a field. A valuation on $K$ is a function $K^\times \to \mathbb{R}$ such that:
(i) $v(xy) = v(x) + v(y)$.
(ii) $v(x + y) \geq \min\{v(x), v(y)\}$.

Fix $0 < \alpha < 1$, if $v$ is a valuation on $K$, then

$$|x| = \begin{cases} \alpha^{v(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

determines a non-Archimedean absolute value on $K$. Conversely, every non-Archimedean absolute value on $K$ determines a valuation $v(x) = \log_\alpha |x|$.

*Remark.* 1. The trivial valuation $v \equiv 0$ is ignored, since it gives the trivial absolute value.
2. We say valuations $v_1, v_2$ are equivalent if $\exists c > 0, v_1 = cv_2$. This of course corresponds to equivalence of absolute values.

**Example 1.4.** 1. For $K = \mathbb{Q}$, the $p$-adic valuation $v_p(x) = -\log_p |x|_p$.
2. For a field $k$, $K = k(t)$ has a valuation given by $v(t^n f(t)/g(t)) = n$ where $f, g \in k[t]$ have nonzero constant terms. This could be called the $t$-adic, or $(t)$-adic, valuation.
3. Consider the field $K = k((t))$ of formal Laurent series over $k$. We can define the $(t)$-adic valuation in this case by setting $v(\sum_i a_i t^i)$ to be the smallest $i$ such that $a_i \neq 0$. This is in fact the completion of the previous example.

**Definition 1.6.** Let $(K, |\cdot|)$ be a non-Archimedean valued field. The valuation ring $\mathcal{O}_K$ is essentially the open unit ball $\bar{B}(0,1) = \{x \in K : |x| \leq 1\} = \{x \in K : v(x) \geq 0\}$.

**Proposition 1.5.** *(i) $\mathcal{O}_K$ is an open subring of $K$.*
*(ii) For $r \leq 1$, the subsets $\{x \in K : |x| \leq r\}$ and $\{x \in K : |x| < r\}$ are open ideals in $\mathcal{O}_K$.*
*(iii) $\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$.*

*Proof.* (i) We already know that it is open. It suffices to check that it's a ring, which follows from the ultrametric inequality.
(ii) Again we know that they are open. The fact that they are ideals again follows from the ultrametric inequality.
(iii) For $u \neq 0$, $u \in \mathcal{O}_K^\times$ iff $u, 1/u \in \mathcal{O}_K$ iff $|u|, |1/u| \leq 1$ iff $|u| = 1$. □

**Corollary 1.6.** *$\mathcal{O}_K$ is a local ring with unique maximal ideal $\mathfrak{m} = \{x \in \mathcal{O}_K : |x| < 1\}$.*

It's clear that $\mathcal{O}_K(x^{-1}) = K$ for any $x \in \mathfrak{m}$. In particular, the fraction field of $\mathcal{O}_K$ is simply $K$.
The field $k = \mathcal{O}_K/\mathfrak{m}$ is called the residue field of $K$.

**Example 1.5.** For $K = \mathbb{Q}$ with the $p$-adic absolute value $|\cdot|_p$, $\mathcal{O}_K = \mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z}, p \nmid b\}$ and $\mathfrak{m} = p\mathbb{Z}_{(p)}$.

**Definition 1.7.** A valuation $v$ on a field $K$ is discrete if $v(K^\times) \cong \mathbb{Z}$ (or, equivalently, $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$). If $v$ is discrete, then we say $K$ is discretely valued.
Suppose $K$ is discretely valued, then $\pi \in \mathcal{O}_K$ is a uniformiser if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$.

**Example 1.6.** The $p$-adic valuation on $\mathbb{Q}$ and the $t$-adic valuation on $k(t)$ are both discrete.

*Remark.* For a discretely valued field $K$, we can always replace its valuation by an equivalent one such that $v(K^\times) = \mathbb{Z}$. We say $v$ is normalised if $v(K^\times) = \mathbb{Z}$.

**Lemma 1.7.** *Let $v$ be a valuation on $K$, then the followings are equivalent:*
*(i) $v$ is discrete.*
*(ii) $\mathcal{O}_K$ is a PID.*
*(iii) $\mathcal{O}_K$ is Noetherian.*
*(iv) $\mathfrak{m}$ is principal.*

*Proof.* (i) $\implies$ (ii): $\mathcal{O}_K$ is clearly an integral domain. Let $I \subset \mathcal{O}_K$ be a nonzero ideal and $x \in I$ such that $v(x) = \min_{y \in I}\{v(y)\}$. $x$ exists since $v$ is discrete. Then $I = (x) = \{a \in \mathcal{O}_K : v(a) \geq x\}$.
(ii) $\implies$ (iii): Well-known.
(iii) $\implies$ (iv): If $\mathcal{O}_K$ is Noetherian, then $\mathfrak{m} = (x_1, \ldots, x_k)$ for some $x_1, \ldots, x_k \in \mathcal{O}_K$ with WLOG $x_1 \leq x_2 \leq \cdots \leq x_k$. Then we just have $\mathfrak{m} = (x_1)$.
(iv) $\implies$ (i): Let $\mathfrak{m} = (\pi)$ for some $\pi \in \mathcal{O}_K$ and let $c = v(\pi)$. Then for any $x \in \mathfrak{m}$, we must already have $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \varnothing$, which implies the discreteness of $v$. □

**Definition 1.8.** A ring $R$ is called a discrete valuation ring (DVR) if it is a PID and has exactly one nonzero prime ideal (which is then necessarily maximal).

**Lemma 1.8.** *(i) Suppose $v$ is a discrete valuation on a field $K$, then its valution ring is a DVR.*
*(ii) Given a DVR $R$, there exists a valuation $v$ on the fraction field $K$ of $R$ such that $R = \mathcal{O}_K$.*

*Proof.* (i) We know that $\mathcal{O}_K$ is a PID by the preceding lemma. Any nonzero prime ideal is then maximal, but there is only one maximal ideal since $\mathcal{O}_K$ is a local ring, so there is only one prime ideal, namely $\mathfrak{m}$.
(ii) We define $v$ as follows: Suppose $\mathfrak{m} = (\pi)$ is the unique prime ideal of $R$. Since $R$ is an UFD, given any $x \in R$, we can write $x = u\pi^m$ for some nonnegative integer $n$ and unit $u \in R^\times$. Then any $y \in K$ has an unique expression of the form $y = u\pi^m$ for some $m \in \mathbb{Z}$ and $u \in R^\times$. Furthermore, $m \geq 0$ iff $y \in R$. Taking $v(y) = m$ gives the desired valuation. □

**Example 1.7.** $\mathbb{Z}_{(p)}, k[[t]]$ are DVRs.

## 1.3 The $p$-adic Numbers

Recall that $\mathbb{Q}_p$ is the field of $p$-adic numbers, which is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. In example sheet, you'll show that the $p$-adic absolute value extends to a discrete valuation on $\mathbb{Q}_p$.

**Definition 1.9.** The valuation ring of $\mathbb{Q}_p$ is called the ring of $p$-adic integers $\mathbb{Z}_p$.

So $\mathbb{Z}_p$ is a DVR.z Its maximal ideal is just $p\mathbb{Z}_p$. Its nonzero ideals are then given by $p^n\mathbb{Z}_p$ for $n \geq 0$ an integer.

**Proposition 1.9.** *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. In particular, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ under the $p$-adic absolute value.*

*Proof.* We need to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. But $\mathbb{Q}$ is dense inside $\mathbb{Q}_p$ and $\mathbb{Z}_p$ is open, so $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ is dense in $\mathbb{Z}_p$. So it suffices to show $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. For $a \in \mathbb{Z}, b \in \mathbb{Z}_{>0}$, $p \nmid b$, we construct $(y_n)_n \in \mathbb{Z}$ with $by_n \equiv a \pmod{p^n}$ (exists as $p \nmid b$), which has $y_n \to a/b$ under $|\cdot|_p$. □

We want a nicer description of $\mathbb{Z}_p$, so let's think about inverse limits.

**Definition 1.10.** Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets (groups, rings, topological spaces, etc.) equipped with transition maps (homomorphisms, continuous maps etc.) $\phi_n : A_{n+1} \to A_n$. The inverse limit of this sequence of objects is the set (group, ring, topological spaces, etc.)

$$\varprojlim_n A_n = \{(a_n)_n : a_n \in A_n, \phi_n(a_{n+1}) = a_n\} \subset \prod_{n=1}^{\infty} A_n$$

where, if the sequence consists of something more complicated than sets, then we let $\varprojlim_n A_n$ inherit the structure from the product.

If we let $\theta_m : \varprojlim_n A_n \to A_m$ be the natural projection maps, then the inverse limit is characterised by the following universal property:

**Proposition 1.10.** *For any set (group, ring, etc.) $B$ together with homomorphisms $\psi_m : B \to A_m$ such that the diagram*

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

*commutes for all $n$, there exists a unique homomorphism $\psi : B \to \varprojlim_n A_n$ with $\theta_m \circ \psi = \psi_m$.*

*Proof.* We define $\psi : B \to \prod_n A_n$ by $\psi(b) = (\psi_1(b), \psi_2(b), \ldots)$. This lands in $\varprojlim_n A_n$ since the said diagrams commute. And it's clear that $\theta_m \circ \psi = \psi_m$. It is also unique by this condition. □

**Definition 1.11.** Let $I \leq R$ be an ideal of the ring $R$. We define the $I$-adic completion of $R$ to be $\hat{R} = \hat{R}_I = \varprojlim_n R/I^n$ with the obvious transition homomorphisms (i.e. projections).

There is a natural map $i : R \to \hat{R}$ from the projections $R \to R/I^n$ by the universal property. It's easy to see that $\ker i = \bigcap_n I^n$.

**Definition 1.12.** We say $R$ is $I$-adically complete if $i$ is an isomorphism.

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

**Proposition 1.11.** *If $K$ is complete, then $\mathcal{O}_K$ is $(\pi)$-adically complete, i.e. $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/(\pi^n)$. Furthermore, for a fixed set $A$ of coset representatives for $\mathcal{O}_K/\pi\mathcal{O}_K$, every $x \in \mathcal{O}_K$ can be written uniquely as a power series*

$$x = \sum_{i=0}^{\infty} a_i \pi^i$$

*for some $a_i \in A$. Moreover, any such power series converges, hence defines an element of $\mathcal{O}_K$.*

*Proof.* $K$ is complete and $\mathcal{O}_K$ is closed, so $\mathcal{O}_K$ too is complete. Suppose $x \in \ker i$, then $x \in (\pi^n)$ for all $n$, which means that if $x$ is nonzero then $\pi(x) \geq nv(\pi)$ for all $n$, a contradiction. So $x = 0$, which means that $\ker i = 0$.
As for surjectivity, let $x = (x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$. Lift each $x_n$ to $y_n \in \mathcal{O}_K$, then $y_n - y_{n+1} \in (\pi^n)$, so $|y_n - y_{n+1}| \to 0$ as $n \to \infty$. By completeness of $\mathcal{O}_K$, $y_n \to y$ for some $y \in \mathcal{O}_K$ and we have $i(y) = x$ by construction.
The rest is in example sheet. □

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

**Corollary 1.12.** *As in part (ii) of the preceding proposition, every $x \in K$ can be written uniquely as a Laurent series*

$$x = \sum_{i=n} a_i \pi^i$$

*for some $n$, possibly negative. conversely, every such expression converges to an element of $K$.*

*Proof.* Choose $n$ such that $\pi^{-n}x \in \mathcal{O}_K$. □

**Corollary 1.13.** *(i) $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.*
*(ii) Every element of $\mathbb{Q}_p$ can be written uniquely as a Laurent series*

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

*where $0 \leq a_i \leq p-1$.*

*Proof.* (i) We already know that $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p$. So it suffices to show that $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ canonically. Indeed, we have a natural map $\mathbb{Z} \to \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$. Its kernel is $\{n \in \mathbb{Z} : |x|_p \leq p^n\} = p^n\mathbb{Z}$, so it remains to show that the map is surjective. Let $c \in \mathbb{Z}_p$ (with reduction $\bar{c} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$). Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there exists $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$. Then $c$ is the image of $x$.
(ii) $\{0, \ldots, p-1\}$ is a set of representatives for $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. □

**Example 1.8.**

$$\frac{1}{1-p} = 1 + p + p^2 + \cdots$$

in $\mathbb{Q}_p$.

# 2 Complete Valued Fields

## 2.1 Hensel's Lemma

**Theorem 2.1** (Hensel's Lemma)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(X) \in \mathcal{O}_K[X]$ and assume that there is some $a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$. Then there is a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $|x - a| < |f'(a)|$.*

*Proof.* Let's assume WLOG that the valuation is normalised. Let $\pi \in \mathcal{O}_K$ be a uniformiser and let $r = v(f'(a))$. We'll construct a sequnece $(x_n)_{n=1}^{\infty}$ satisfying $f(x_n) \equiv 0 \pmod{\pi^{n+2r}}$ and $x_n \equiv x_{n+1} \pmod{\pi^{n+r}}$.
This is done this by taking $x_1 = a$ and, once $x_1, \ldots, x_n$ are constructed with the said properties, we define $x_{n+1} = x_n - f(x_n)/f'(x_n)$. Since $x_n \equiv x_1 \pmod{\pi^{r+1}}$, we have $v(f'(x_n)) = r$ and hence $f(x_n)/f'(x_n) \equiv 0 \pmod{\pi^{n+r}}$ Therefore $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$. If we now write $f(X+Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \cdots$ (indeed $f_0 = f, f_1 = f'$, etc.), then $f(x_{n+1}) = f(x_n) + f'(x_n)c + f_2(x_n)c^2 + \cdots$ where $c = -f(x_n)/f'(x_n)$. Since $c \equiv 0 \pmod{\pi^{n+r}}$ and $v(f_i(x_n)) \geq 0$, we have $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \pmod{\pi^{n+1+2r}}$.
This sequence is Cauchy and $\mathcal{O}_K$ is complete since it's closed, so there is some $x \in \mathcal{O}_K$ with $x_n \to x$. By continuity of $f$, we have $f(x) = 0$. Moreover, $a = x_1 \equiv x_n \pmod{\pi^{r+1}}$ for all $n$, so $a \equiv x \pmod{\pi^{r+1}}$, which means that $|x - a| < |f'(a)|$.
As for uniqueness, suppose $x' \in \mathcal{O}_K$ is another solution satisfying $f(x') = 0$ and $|x' - a| < |f'(a)|$. Let $\delta = x' - x$. Suppose for the sake of contradiction that $\delta \neq 0$, then $|\delta| < |f'(a)|$ by the ultrametric inequality. On the other hand, $0 = f(x') = f(x+\delta) = f'(x)\delta + f_2(x)\delta^2 + \cdots$. This tells us that $|f'(x)\delta| \leq |\delta^2|$, so $|f'(a)| = |f'(x)| \leq |\delta|$, contradiction. □

**Corollary 2.2.** *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(X) \in \mathcal{O}_K[X]$ and $\bar{c} \in k = \mathcal{O}_K/\mathfrak{m}$ a simple root of its reduction $\bar{f}(X) \in k[X]$, then there is some unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $x \equiv \bar{c} \pmod{\mathfrak{m}}$.*

*Proof.* Apply the preceding theorem to a lift $c \in \mathcal{O}_K$ of $c$, then $|f(c)| < |f'(c)|^2 = 1$ since $c$ is a simple root. □

**Example 2.1.** $f(X) = X^2 - 2$ has a simple root modulo 7, so $\mathbb{Z}_7$ contains a square root of 2.

**Corollary 2.3.** *$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ when $p > 2$ and $(\mathbb{Z}/2\mathbb{Z})^3$ when $p = 2$.*

*Proof.* Suppose first that $p > 2$. Take $b \in \mathbb{Z}_p^\times$. Applying the preceding corollary to $f(X) = X^2 - b$ shows that $b \in (\mathbb{Z}_p)^2$ iff $\bar{b} \in (\mathbb{F}_p)^2$. We therefore have an isomorphism $(\mathbb{Z}_p)^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$. The isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \cong \mathbb{Q}_p^\times, (u, n) \mapsto up^n$ of (multiplicative) groups shows that $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \oplus \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
Now suppose $p = 2$. Again consider $f(X) = X^2 - b$. The problem here is that $f'(X) = 2X \equiv 0 \pmod 2$, so $\bar{f}$ cannot ever have a simple root, so we need to look at a deeper congruence. As $3, 5, 7$ are not squares modulo 8, let's take $b \equiv 1 \pmod 8$, then $|f(1)|_2 \leq 2^{-3} < |f'(1)|_2^2$. So Hensel's lemma gives a root of $f(X)$ in $\mathbb{Z}_p$. Hence $b \in (\mathbb{Z}_2^\times)^2$ iff $b \equiv 1 \pmod 8$, thus $(\mathbb{Q}_2^\times)/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}_2^\times)/(\mathbb{Z}_2^\times)^2 \oplus \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z})^\times \oplus \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^3$. □

*Remark.* The iteration we used in proving Theorem 2.1 are essentially the same as the one used in the Newton-Raphson approximation scheme for solving real-valued functions. This is probably how it's motivated.

**Theorem 2.4** (Hensel's Lemma but better)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(X) \in \mathcal{O}_K[X]$. Suppose $\bar{f}$ is the reduction of $f$ modulo $\mathfrak{m}$ which*

*factorises as $\bar{f} = \bar{g}\bar{h}$ in $k[X]$ with $\bar{g}, \bar{h}$ coprime, then there is a factorisation $f = gh$ in $\mathcal{O}_K[X]$ such that $g$ reduces to $\bar{g}$ and $h$ reduces to $\bar{h}$.*

**Corollary 2.5.** *Let $f(X) = a_n X^n + \cdots + a_0, a_n \neq 0$ be an irreducible polynomial in $K[X]$ with $(K, |\cdot|)$ a complete discretely valued field. Then $|a_i| \leq \max\{|a_0|, |a_n|\}$ for all $i$.*

*Proof.* WLOG $f(X) \in \mathcal{O}_K[X]$ with $\max_i |a_i| = 1$. Let's show $\max\{|a_0|, |a_n|\} = 1$. Let $r$ be the minimal such that $|a_r| = 1$. If $r = 0$ then we are done. Otherwise, $0 < r \leq n$. Therefore we have $\bar{f}(X) = X^r \bar{g}(X)$ for some $\bar{g}(X) \in k[X]$, which lifts to a nontrivial factorisation unless $r = n$. □

## 2.2 Teichmüller Lifts

Let $p$ be a prime.

**Definition 2.1.** A ring $R$ of characteristic $p$ is perfect if the Frobenius $x \mapsto x^p$ is a bijection.

We also say a field is perfect if it is perfect as a ring.

*Remark.* The Frobenius is a ring homomorphism since $\operatorname{char} R = p$.

**Example 2.2.** 1. $\mathbb{F}_p, \bar{\mathbb{F}}_p$ are perfect.
2. (non-example) $\mathbb{F}_p[t]$ is not perfect, as $t$ is not in the image of the Frobenius.
3. $\mathbb{F}_p(t)$ is not perfect, but $\mathbb{F}_p(t^{1/p^\infty}) = \mathbb{F}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$ is perfect (we call it the perfection of $\mathbb{F}_p(t)$).

It's an easy fact that a field of characteristic $p$ is perfect iff any finite extension of it is separable.

**Theorem 2.6.** *Let $(K, |\cdot|)$ be a complete discretely valued field with perfect residue field $k$ of characteristic $p$, then there exists a unique map $[-] : k \to \mathcal{O}_K$ such that:*
*(i) $a$ is the reduction of $[a]$ modulo $\mathfrak{m}$.*
*(ii) $[ab] = [a][b]$.*
*(iii) If the characteristic of $K$ is also $p$, then $[a+b] = [a] + [b]$ and $[-]$ is a ring homomorphism.*

**Definition 2.2.** $[-]$ is called the Teichmüller lift of $K$.

**Lemma 2.7.** *Let $(K, |\cdot|)$ be a complete discretely valued field whose residue field $k$ has characteristic $p$. Fix $\pi \in \mathcal{O}_K$ a uniformiser and let $x, y \in \mathcal{O}_K$. Suppose $x \equiv y \pmod{\pi^k}, k \geq 1$. Then $x^p \equiv y^p \pmod{\pi^{k+1}}$.*

*Proof.* Write $x = y + u\pi^k$ for some $u \in \mathcal{O}_K$. Note that $p \in \mathfrak{m}$ as $\operatorname{char} k = p$. So we can compute

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

as desired. □

*Proof of 2.6.* Let $a \in k$. Keep taking $p^{th}$ root gives me a (unique) sequence of roots $a, a^{1/p}, a^{1/p^2}, \ldots$ as $k$ is perfect. To each $i \geq 0$, we choose a lift $y_i \in \mathcal{O}_K$ of $a^{1/p^i}$. We claim that $x_i = y_i^{p^i}$ is a Cauchy sequence, and its limit is independent of the choice of $y_i$.
By construction, $y_i \equiv y_{i+1}^p \pmod{\pi}$. By the preceding lemma, this gives $x_i \equiv x_{i+1} \pmod{\pi^{i+1}}$. So the sequence is Cauchy and converges to some $x \in K$.
If we have another choice $y_i'$ which gives us another sequence $x_i' \to x'$, then we let

$$x_i'' = \begin{cases} x_i & \text{for } i \text{ even} \\ x_i' & \text{for } i \text{ odd} \end{cases}$$

which comes from the liftings

$$y_i'' = \begin{cases} y_i & \text{for } i \text{ even} \\ y_i' & \text{for } i \text{ odd} \end{cases}$$

and hence is Cauchy, and its limit must equal to $x, x'$ simultaneously, thus we have $x = x'$.
We define $[a] = x$, then $x_i = y_i^{p^i} \equiv (a^{1/p^i})^{p^i} \equiv a \pmod{\pi}$ shows that $[a]$ reduces to $a$ modulo $\mathfrak{m}$. Let $b \in k$ and we choose $u_i \in \mathcal{O}_K$ a lift of $b^{1/p^i}$, and $z_i = u_i^{p^i}$. Then $[ab]$ is the limit of $x_i z_i$, which is $[a][b]$.
If $K$ also has characteristic $p$, then $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$. Then $[a+b]$ is the limit of $(y_i + u_i)^{p^i} = y_i^{p^i} + u_i^{p^i}$, which is $[a] + [b]$.
As for uniqueness, suppose $\phi : k \to \mathcal{O}_K$ satisfies (i) and (ii). Then for $a \in k$, $\phi(a^{1/p^i})$ is a lift of $a^{1/p^i}$. It follows that $[a]$ is the limit of $\phi(a^{1/p^i})^{p^i} = \phi(a)$. □

**Example 2.3.** Suppose $K = \mathbb{Q}_p$. Let's see what happens to $[-] : \mathbb{F}_p \to \mathbb{Z}_p$. For $a \in \mathbb{F}_p^\times$, then $[a]^{p-1} = [a^{p-1}] = [1] = 1$, so $[a]$ is a $(p-1)$-th root of unity, which in some sense is a more natural choice of lifting (than $0, \ldots, p-1$). This also tells us that $\mathbb{Z}_p$ contains all $(p-1)$-th roots of unity.

**Lemma 2.8.** *Suppose $(K, |\cdot|)$ is a complete discretely valued field. If the residue field is a subfield of $\bar{\mathbb{F}}_p$, then $[a] \in \mathcal{O}_K^\times$ are roots of unity.*

*Proof.* Given $a \in k$, there is some $n$ such that $a \in \mathbb{F}_{p^n}$. So $[a]^{p^n-1} = [a^{p^n-1}] = [1] = 1$. □

**Theorem 2.9.** *Suppose $(K, |\cdot|)$ is a complete discretely valued field with characteristic $p > 0$ and perfect residue field. Then $K \cong k((t))$.*

*Proof.* Note that since $K = \mathrm{FF}(\mathcal{O}_K)$, it suffices to show that $\mathcal{O}_K \cong k[[t]]$ as rings.
Fix a uniformiser $\pi \in \mathcal{O}_K$ and $[-] : k \to \mathcal{O}_K$ be the Teichmüller lift. Consider $\phi : k[[t]] \to \mathcal{O}_K, \sum_i a_i t^i \mapsto \sum_i [a_i]\pi^i$. This is a ring homomorphism as $[-]$ is, and is a bijection by Proposition 1.11. □

## 2.3 Extensions of Complete Valued Fields

We're looking to prove the following theorem.

**Theorem 2.10.** *Given a complete discretely valued field $(K, |\cdot|)$ and a finite extension $L/K$, then there is a unique absolute value $|\cdot|_L$ on $L$ extending the absolute value on $K$. Moreover, this absolute value is given by*

$$|y|_L = |N_{L/K}(y)|^{1/[L:K]}$$

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

Let's be reminded that, for a finite extension $L/K$, the norm of $y \in L$ is the determinant of the $K$-linear map $\mathrm{mult}_y : L \to L, x \mapsto xy$. The following facts are straightforward.

**Proposition 2.11.** *(i) $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}$.*
*(ii) Let $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ be the minimal polynomial of $y \in L$, then $N_{L/K}(y) = \pm a_0^m$ for some $m \geq 1$. In particular, $N_{L/K}(y) = 0$ iff $y = 0$.*

We'll first prove the uniqueness part of Theorem 2.10.

**Definition 2.3.** 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:
(i) For any $x \in V$, $\|x\| = 0$ iff $x = 0$.
(ii) $\|\lambda x\| = |\lambda|\|x\|$ for all $\lambda \in K, x \in V$.
(iii) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$ for all $x, y \in V$.

**Example 2.4.** If $V$ is finite-dimensional and $e_1, \ldots, e_n$ is a basis of $V$, then the sup norm on $V$ with respect to this basis is defined by $\|x\|_{\sup} = \max_i |x_i|$ where $x = \sum_i x_i e_i$.

**Definition 2.4.** Two norms $\|\cdot\|_1, \|\cdot\|_2$ are equivalent if there are some $C, D > 0$ such that $C\|x\|_1 \leq \|x\|_2 \leq D\|x\|_1$.

Equivalently, two norms are equivalent iff they induce the same topology.

**Proposition 2.12.** *Let $(K, |\cdot|)$ be a complete non-Archimedean valued field and $V$ a finite dimensional vector space over $K$. Then $V$ is complete with respect to $\|\cdot\|_{\sup}$ (for any choice of basis).*

*Proof.* Let $(x_n)_n$ be a Cauchy sequence in $V$ and $e_1, \ldots, e_n$ a basis of $V$ with respect to which $\|\cdot\|_{\sup}$ is defined. Write $v_i = \sum_{j=1}^n x_j^i e_j$, then $(x_j^i)_i$ is a Cauchy sequencce in $K$, hence converges to some $x_j \in K$. Then $v_i \to v = \sum_j x_j e_j$. □

**Theorem 2.13.** *Let $(K, |\cdot|)$ be a complete non-Archimedean valued field and $V$ a finite-dimensional vector space over $K$. Then any two norms on $V$ are equivalent. In particular, $V$ is complete with respect to any of these norm.*

*Proof.* Since equivalence of norms is an equivalence relation (as one can check), it suffices to show that they are equivalent to the sup norm with respect to a chosen basis $e_1, \ldots, e_n$.
Let $\|\cdot\|$ be a norm. $D = \max_i \|e_i\|$ has $\|x\| \leq \max_i |x_i|\|e_i\| \leq D\|x\|_{\sup}$.
To find $C$, we do induction on $n = \dim V$. The case $n = 1$ is clear. Assume now that $n > 1$ and such $C$ can be found for $n - 1$ (say with value $C_{n-1}$). Let $V_i = \langle e_1, \ldots, \hat{e}_i, \ldots, e_n \rangle$. Each $V_i$ is complete, hence closed. Then $e_i + V_i$ is also closed for all $i$, so $S = \bigcup_i (e_i + V_i)$ is also closed, and it doesn't contain 0. So we can find some $C$ such that $B(0, C) \cap S = \varnothing$. We shall show that this $C$ works. Take $x \in V$. Suppose $x_j = \max_i |x_i|$, then $\|x\|_{\sup} = |x_j|$ and $x_j^{-1}x \in S$, thus $\|x_j^{-1}x\| \geq C$ and therefore $\|x\| \geq C|x_j| = C\|x\|_{\sup}$. □

The uniqueness part of Theorem 2.10 follows due to Proposition 1.1.
As for the existence, we shall show that the expression $|y|_L = |N_{L/K}(y)|^{1/[L:K]}$ does give rise to an absolute value on $L$ extending that on $K$. Proposition 2.11 implies that $|\cdot|_L$ is multiplicative and $|x|_L = 0$ iff $x = 0$. We need a little bit more work for the ultrametric inequality.

**Definition 2.5.** Let $R \subset S$ be (commutative unital) rings, then $s \in S$ is integral over $R$ if it solves a monic polynomial with coefficients in $R$. The integral closure $R^{\mathrm{int}(S)}$ of $R$ inside $S$ is the set of integral elements of $S$ over $R$. We say $R$ is integrally closed in $S$ if $R^{\mathrm{int}(S)} = R$.

**Proposition 2.14.** *$R^{\mathrm{int}(S)}$ is an integrally closed subring of $S$.*

*Proof.* Example sheet. □

**Lemma 2.15.** *Let $(K, |\cdot|)$ be a non-Archimedean valued field, then $\mathcal{O}_K$ is integrally closed in $K$.*

*Proof.* Pick an integral element $x \in K^\times$ over $\mathcal{O}_K$, so there is some $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with $a_i \in \mathcal{O}_K$ and $f(x) = 0$. So $x = -a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0x^{1-n}$. If $|x| > 1$ (i.e. $x \notin \mathcal{O}_K$), then $|-a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0x^{1-n}| \leq 1$, contradiction. □

Consider the set $\mathcal{O}_L = \{y \in L : |y|_L \leq 1\}$. Now we add back in the condition that $K$ is discretely valued.

**Lemma 2.16.** *$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in $L$.*

This implies the ultrametric inequality (hence Theorem 2.10, since $|\cdot|_L$ clearly extends $|\cdot|$), since if $x, y \in L$ and $|x|_L \leq |y|_L$ then $x/y \in \mathcal{O}_L$. But since $1 \in \mathcal{O}_L$ and $\mathcal{O}_L$ is a ring, we have $1 + x/y \in \mathcal{O}_L$, so $|x+y|_L \leq |y| = \max\{|x|, |y|\}$.

*Proof.* Take integral $y \in L$ and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the minimal polynomial of $y$ over $K$.
We claim that $y$ is integral over $\mathcal{O}_K$ iff $f(X) \in \mathcal{O}_K[X]$. The "if" part is by definition. Conversely, suppose $y$ is integral over $\mathcal{O}_K$, then there is some $g(X) \in \mathcal{O}_K[X]$ be monic and such that $g(y) = 0$. Since $f \mid g$, every root of $f$ is a root of $g$, but every root of $g$ in $L$ is integral over $\mathcal{O}_K$. As the coefficients of $f$ are integer polynomials over its roots, they must be integral over $\mathcal{O}_K$. Since $\mathcal{O}_K$ is integrally closed, this gives $f(X) \in \mathcal{O}_K[X]$.
We know that $|a_i| \leq \max\{|a_0|, 1\}$ by Corollary 2.5, but by the properties of $N_{L/K}$, we have $N_{L/K}(y) = \pm a_0^m \in \mathcal{O}_K$ for some $m$. Hence $y \in \mathcal{O}_L$ iff $|N_{L/K}(y)| \leq 1$ iff $|a_0| \leq 1$ iff $\forall i, |a_i| \leq 1$ iff $f(X) \in \mathcal{O}_K[X]$ iff $y$ is integral over $\mathcal{O}_K$. □

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

**Corollary 2.17.** *Let $L/K$ be a finite extension, then $L$ is also discretely valued with respect to $|\cdot|_L$ and $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in $L$.*

*Proof.* The second part follows from the preceding lemma. As for the first part, let $v$ be a valuation on $K$, then it extends uniquely to a valuation $v_L$ on $L$. For $y \in L^\times$, we have $|y| = |N_{L/K}(y)|^{1/n}$ where $n = [L : K]$, so after taking logarithm we obtain $v_L(y) = n^{-1}v(N_{L/K}(y))$, therefore $v_L(L^\times) \subset n^{-1}v(K^\times)$ which is discrete. □

**Corollary 2.18.** *Let $\bar{K}/K$ be an algebraic closure of $K$, then the absolute value on $K$ extends uniquely to an absolute value on $\bar{K}$.*

*Proof.* Let $x \in \bar{K}^\times$, then $x \in L$ for some $L/K$ finite. Define $|x|_{\bar{K}} = |x|_L$. This is independent of the choice of $L$ by the uniqueness part of Theorem 2.10. All axioms can be checked by passing to a suitable finite extension.
Uniqueness of $|\cdot|_{\bar{K}}$ again follows from the uniqueness part of Theorem 2.10. □

*Remark.* Unlike the case of a finite extension, $|\cdot|_{\bar{K}}$ is never discrete. This can be seen by adjoining roots of uniformisers.
Not only that, it may not even be complete, e.g. $\bar{\mathbb{Q}}_p$ isn't complete. But if we take $\mathbb{C}_p$ (the "$p$-adic complex numbers") to be the metric completion of $\bar{\mathbb{Q}}_p$, then it can be shown that $\mathbb{C}_p$ is algebraically closed (and in fact abstractly isomorphic to $\mathbb{C}$).

**Proposition 2.19.** *Let $L/K$ be a finite extension of complete discretely valued fields. Assume that $\mathcal{O}_K$ is compact and the corresponding extension $k_L/k$ of residue fields is finite and separable, then there is some $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.*

Later, we'll see that the compactness of $\mathcal{O}_K$ in fact implies the finiteness and separability of the residue field extension.

*Proof.* By the primitive element theorem, $k_L = k(\bar{\alpha})$ for some $\bar{\alpha} \in k_L$. Pick a lift $\alpha \in \mathcal{O}_L$ of $\bar{\alpha}$ and take $g(X) \in \mathcal{O}_K[X]$ a monic lift of the minimal polynomial of $\bar{\alpha}$. Fix $\pi_L \in \mathcal{O}_L$ a uniformiser, then $\bar{g}(X) \in k[X]$ is irreducible and separable, so $g(\alpha) \equiv 0 \pmod{\pi_L}$ and $g'(\alpha) \not\equiv 0 \pmod{\pi_L}$.
Now, if $g(\alpha) \equiv 0 \pmod{\pi_L^2}$, then $g(a + \pi_L) \equiv \pi_L g'(\alpha) \pmod{\pi_L^2}$ and therefore $v_L(g(\alpha+\pi_L)) = 1$ (WLOG $v_L$ is normalised). This means that either $v_L(g(\alpha)) = 1$ or $v_L(g(\alpha + \pi_L)) = 1$. Since they are both lifts of $\bar{\alpha}$, by possibly replacing $\alpha$ by $\alpha + \pi_L$ we may assume that $v_L(g(\alpha)) = 1$, i.e. $\beta = g(\alpha)$ is a uniformiser in $L$.
Consider the map $\phi : \mathcal{O}_K^n \to L, (x_0, \ldots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_i \alpha^i$ where $n = [K(\alpha) : K]$. The image of this map is $\mathcal{O}_K[\alpha]$, and is also compact as $\mathcal{O}_K$ is. As metric topologies are Hausdorff, this means that $\mathcal{O}_K[\alpha]$ is closed.
Since $k_L = k(\bar{\alpha})$, $\mathcal{O}_K[\alpha]$ contains a set of coset representatives for $k_L = \mathcal{O}_L/\mathfrak{m} = \mathcal{O}_L/(\beta)$. So any $y \in \mathcal{O}_L$ is a power series $y = \sum_i \lambda_i \beta^i$ for $\lambda_i \in \mathcal{O}_K[\alpha]$. The partial sums are in $\mathcal{O}_K[\alpha]$, so the closedness of $\mathcal{O}_K[\alpha]$ implies $y \in \mathcal{O}_K[\alpha]$. □

# 3 Local Fields

## 3.1 Definition and Classification

**Definition 3.1.** A valued field $(K, |\cdot|)$ is a local field if it is complete and locally compact (i.e. each point has a open neighbourhood contained in a compact set).

**Example 3.1.** $\mathbb{R}$ and $\mathbb{C}$ are local fields.

**Proposition 3.1.** *Let $(K, |\cdot|)$ be a non-Archimedean complete valued field. Then the followings are equivalent:*
*(i) $K$ is locally compact.*
*(ii) $\mathcal{O}_K$ is compact.*
*(iii) The valuation is discrete and the residue field is finite.*

*Proof.* (i) $\implies$ (ii): Let $U \ni 0$ be a compact neighbourhood of 0 (i.e. a compact set containing an open neighbourhood of 0). Then there is some $x \in \mathcal{O}_K$ such that $x\mathcal{O}_K \subset U$. Since $x\mathcal{O}_K$ is closed, it is compact, so $\mathcal{O}_K$ is compact.
(ii) $\implies$ (i): If $\mathcal{O}_K$ is compact, then $a + \mathcal{O}_K$ is a compact neighbourhood of $a$.
(ii) $\implies$ (iii): Let $x \in \mathfrak{m}$ and fix $A_x \subset \mathcal{O}_K$ a set of coset representatives for $\mathcal{O}_K/x\mathcal{O}_K$. Then $\mathcal{O}_K$ is a disjoint union of the open sets $y + x\mathcal{O}_K, y \in A_x$. By compactness, $A_x$ must be finite, so $\mathcal{O}_K/(x)$ is finite, therefore $\mathcal{O}_K/\mathfrak{m}$ is finite.
To see that the valuation is discrete, suppose it is not discrete, then we can find a sequence $x_1, x_2, \ldots$ such that $v(x_1) > v(x_2) > \cdots > 0$. Then $(x_1) \subsetneq (x_2) \subsetneq \cdots$, but this must be a contradiction due to the finiteness of their quotients.
(iii) $\implies$ (ii): It suffices to show that $\mathcal{O}_K$ is sequentially compact. Let $(x_n)_n$ be a sequence in $\mathcal{O}_K$. Fix a uniformser $\pi \in \mathcal{O}_K$. Since $(\pi^i)/(\pi^{i+1}) \cong k$, we have the finiteness of $\mathcal{O}_K/(\pi^i)$ for all $i$.
Choose a subsequence $(x_k^{(1)})_k$ of $(x_n)$ such that the terms of $(x_k^{(1)})_k$ have the same residue modulo $\pi$, which is possible by finiteness of $\mathcal{O}_K/(\pi)$. Once $(x_k^{(m)})_k$ is chosen, we choose a subsequence $(x_k^{(m+1)})_k$ of it so that the terms of $(x_k^{(m+1)})_k$ have the same residue modulo $\pi^{m+1}$. Then $(x_m^{(m)})_m$, which is a subsequence of $(x_n)_n$, is a Cauchy sequence by construction, therefore converges. □

**Example 3.2.** $\mathbb{Q}_p, \mathbb{F}_p((t))$ are local fields.

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

**Definition 3.2.** Suppose each $A_n$ is finite. The profinite topology on $A = \varprojlim_n A_n$ is the weakest topology on $A$ such that the projection maps $A \to A_n$ are continuous, where each $A_n$ is equipped with the discrete topology.

It's a fact that the profinite topology is always compact, Hausdorff, and totally disconnected.

**Proposition 3.2.** *Let $K$ be a non-Archimedean local field. Recall the isomorphism of rings $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/(\pi^n)$ with $\pi$ a uniformiser. It is, in fact, an isomorphism of topological rings with the latter equipped with the profinite topology.*

*Proof.* It's not hard to check that the sets $B = \{a + \pi^n\mathcal{O}_K : n \in \mathbb{Z}_{>0}\}$ form a basis for both topologies. □

**Lemma 3.3.** *Let $K$ be a non-Archimedean local field and $L/K$ a finite extension, then $L$ is also a local field.*

*Proof.* We already know that $L$ is still complete and discretely valued. It remains to show the finiteness of its residue field $k_L = \mathcal{O}_L/\mathfrak{m}_L$. Pick a basis $\alpha_1, \ldots, \alpha_n$ for $L$ over $K$. We know that $\|\cdot\|_{\sup}$ with respect to this basis is equivalent to the absolute value on $L$. So there is some $r > 0$ such that $\mathcal{O}_L \subset \{x \in L : \|x\|_{\sup} \leq r\}$. Take $a \in K$ be such that $|a| > r$. Then $\mathcal{O}_L \leq \bigoplus_{i=1}^n a\alpha_i\mathcal{O}_K$, so $\mathcal{O}_L$ is a finite $\mathcal{O}_K$-module since $\mathcal{O}_K$ is Noetherian, therefore $k_L$ is a finitely generated $k$-module, i.e. a finite field extension. □

**Definition 3.3.** Suppose $(K, |\cdot|)$ is a non-Archimedean valued field. We say it has equal characteristic if $\operatorname{char} K = \operatorname{char} k$; mixed characteristic otherwise.

**Example 3.3.** $\mathbb{Q}_p$ has mixed characteristic, but $\mathbb{F}_p((t))$ has equal characteristic.

**Theorem 3.4.** *Any equal characteristic, non-Archimedean local field (necessarily with positive characteristic $p > 0$) is isomorphic to $\mathbb{F}_{p^m}((t))$ for some $m$.*

*Proof.* The residue field is finite, hence perfect. So the theory of Teichmüller lift tells us the result. □

**Lemma 3.5.** *An absolute value $|\cdot|$ on a field $K$ is non-Archimedean iff $|n|$ is bounded for all integers $n$.*

*Proof.* The "only if" part follows straight from the ultrametric inequality. Conversely, suppose $|n|$ is bounded by some constant $B > 0$, we show the ultrametric inequality using the tensor power trick. Let $x, y \in K$ and WLOG $|x| \leq |y|$. Then

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

Take $m^{th}$ roots gives $|x+y| \leq (m+1)^{1/m} B^{1/m} |y|$. Sending $m \to \infty$ gives the inequality. □

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

*Proof.* Let's first assume that $|\cdot|$ is Archimedean.
Fix $b > 1$ an integer such that $|b| > 1$ (possible by the preceding lemma). Let $a > 1$ be another integer. We write $b^n$ in base $a$, i.e. $b^n = c_m a^m + c_{m-1} a^{m-1} + \cdots + c_0$ with $c_i \in \{0, \ldots, a-1\}$ and $c_n \neq 0$. Let $B = \max_i |c_i|$. Then $|b^n| = |b|^n \leq (m+1)B \max\{|a|^m, 1\}$. So $|b| \leq ((n \log_a b + 1)B)^{1/n} \max\{|a|^{\log_a b}, 1\}$ (note that $m \leq n \log_a b$ since $a^m \leq b^n$). Taking $n \to \infty$ gives $|b| \leq \max\{|a|^{\log_a b}, 1\}$. But $|b| > 1$, so $|a| > 1$ and $|b| \leq |a|^{\log_a b}$.
Switching the roles of $a, b$ gives $|a| \leq |b|^{\log_b a}$. Combining this with the earlier inequality gives $\log|a| / \log a = \log|b| / \log b$. Say $\log|b| / \log b = \lambda$, then we know from this that $|a| = a^\lambda$ for all integers $a > 1$, which forces $|\cdot| = |\cdot|_\infty^\lambda$.
Now suppose that $|\cdot|$ is non-Archimedean. Since $|n| \leq |1| = 1$ for all positive integer $n$, there must be some prime $p$ with $|p| < 1$. Suppose there is some other prime $q$ such that $|q| < 1$, we choose integers $r, s$ such that $1 = rp + sq, r, s \in \mathbb{Z}$. Then $1 \leq \max\{|rp|, |sq|\} < 1$, contradiction. We therefore have $|\cdot| \sim |\cdot|_p$. □

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

*Proof.* Since $|k| < \infty$ (hence $\operatorname{char} k > 0$), we must have $\operatorname{char} K = 0$, so $\mathbb{Q} \subset K$. The restriction of $|\cdot|$ to $\mathbb{Q}$ is non-Archimedean. It is also nontrivial as $\operatorname{char} k$ must have positive valuation. The preceding theorem then shows that the restricted absolute value is equivalent to $|\cdot|_p$ for some prime $p$.
Since $K$ is also complete, $\mathbb{Q}_p \subset K$. The only thing left to show is that this field extension is finite. It suffices to prove that $\mathcal{O}_K$ is a finite $\mathbb{Z}_p$-module.
Let $\pi \in \mathcal{O}_K$ be a uniformiser and $v$ a normalised valuation on $K$. Set $e = v(p)$. Then $\mathcal{O}_K / p\mathcal{O}_K = \mathcal{O}_K / \pi^e \mathcal{O}_K$ is finite (due to the filtration $\pi^e \mathcal{O}_K \leq \pi^{e-1} \mathcal{O}_K \leq \cdots \leq \mathcal{O}_K$ whose factors are $\pi^i \mathcal{O}_K / \pi^{i+1} \mathcal{O}_K \cong \mathcal{O}_K / \pi \mathcal{O}_K$). So $\mathcal{O}_K / p\mathcal{O}_K$ is a finite-dimensional $\mathbb{F}_p$-vector space. Let $x_1, \ldots, x_n \in \mathcal{O}_K$ be a set of coset representatives for a $\mathbb{F}_p$-basis of $\mathcal{O}_K / p\mathcal{O}_K$.

Then $\{\sum_i a_i x_i : a_i \in \{1, \dots, p-1\}\}$ is a set of coset representative for $\mathcal{O}_K/p\mathcal{O}_K$. Any $y \in \mathcal{O}_K$ has a power series

$$y = \sum_{i=0}^{\infty} \sum_{j=1}^{n} a_{ij} x_n p^i = \sum_{j=1}^{n} b_j x_j, b_j = \sum_{i=0}^{\infty} a_{ij} p^i$$

for some $a_{ij} \in \{0, \dots, p-1\}$. This shows that $x_j$'s form a $\mathbb{Z}_p$-basis for $\mathcal{O}_K$. □

On example sheet, you'll show that if $K$ is a complete Archimedean field, then $K$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.
To summarise, any local field is isomorphic to one of $\mathbb{R}, \mathbb{C}, \mathbb{F}_{p^m}((t))$, or a finite extension of $\mathbb{Q}_p$ for some prime $p$ and integer $m \geq 1$.

## 3.2 Global Fields

**Definition 3.4.** A global field is a field isomorphic to either a number field or a global function field, i.e. a finite extension of $\mathbb{F}_p(t)$ for a prime $p$.

**Lemma 3.8.** *Let $K = |\cdot|$ be a complete discretely valued field and $L/K$ a finite Galois extension with absolute value $|\cdot|_L$ extending $|\cdot|$. Then for any $x \in L$ and $\sigma \in \mathrm{Gal}(L/K)$, we have $|\sigma(x)|_L = |x|_L$.*

*Proof.* Note that $|x|'_L = |\sigma(x)|_L$ is again an absolute value on $L$ extending $|\cdot|$. So we are done by the uniqueness of extension. □

**Lemma 3.9** (Krasner's Lemma)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(X) \in K[X]$ be separable and irreducible, with roots $\alpha_1, \dots, \alpha_n \in K^{\mathrm{sep}}$, the separable closure of $K$.*
*Suppose $\beta \in \bar{K}$ is such that $|\beta - \alpha_1| < |\beta - \alpha_i|$ for $i = 2, \dots, n$, then $K(\alpha_1) \subset K(\beta)$.*

*Proof.* Let $L = K(\beta)$ and $L' = L(\alpha_1, \dots, \alpha_n)$. Then $L'/L$ is Galois since it's the splitting field of $f$ viewed as a polynomial with coefficients in $L$. Let $\sigma \in \mathrm{Gal}(L'/L)$, then $|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1|$ by the preceding lemma.. In light of the inequality we are given, $\sigma$ must fix $\alpha_1$, i.e. $\alpha_1 \in K(\beta)$. □

**Proposition 3.10** ("Nearby polynomials give the same extension")**.** *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(X) = \sum_{i=0}^{m} a_i X^i \in \mathcal{O}_K[X]$ is separable, irreducible, and monic of degree $m$. Let $\alpha \in K^{\mathrm{sep}}$ be a root of $f$, then there is some $\epsilon > 0$ such that for any $g(X) = \sum_{i=0}^{m} b_i X^i$ monic of degree $m$ with $|a_i - b_i| < \epsilon$, there is a root $\beta$ of $g$ such that $K(\alpha) = K(\beta)$.*

*Proof.* Suppose $\alpha = \alpha_1, \dots, \alpha_n \in K^{\mathrm{sep}}$ are the roots of $f$, necessarily distinct. Then $f'(\alpha_1) \neq 0$. Choose $\epsilon$ sufficiently small such that for any $g$ satisfying the said conditions have $|g(\alpha_1)| < |f'(\alpha)|^2$ and $|f'(\alpha_1) - g'(\alpha_1)| \leq |f'(\alpha_1)|$. Then $|g(\alpha_1)| < |g'(\alpha_1)|^2$, so we get $\beta \in K(\alpha_1)$ from Theorem 2.1 with the property that $g(\beta) = 0$ and

$$|\beta - \alpha_1| < |g'(\alpha_1)| = |f'(\alpha_1)| = \prod_{i=2}^{n} |\alpha_1 - \alpha_i| \leq |\alpha_1 - \alpha_i|$$

for all $i = 2, \dots, n$ (noting the integrality of $\alpha_1$). Since $|\beta - \alpha_1| < |\alpha_1 - \alpha_i| = |\beta - \alpha_i|$, Krasner's lemma gives $\alpha_1 \in K(\beta)$, so $K(\alpha_1) = K(\beta)$. □

**Theorem 3.11.** *Let $K$ be a local field, then $K$ is the completion of a global field.*

*Proof.* Case 1: $K$ is Archimedean. Then $K$ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. The former is the completion of $\mathbb{Q}$ and the latter that of $\mathbb{Q}(i)$.
Case 2: $K$ is non-Archimedean and of equal characteristic. Then we know that $K \cong \mathbb{F}_{p^m}((t))$ for some prime $p$ and $m \geq 1$, which is the completion of $\mathbb{F}_{p^m}(t)$.
Case 3: $K$ is non-Archimedean and of mixed characteristic. So $K$ is a finite extension of $\mathbb{Q}_p$. As it is separable, $K = \mathbb{Q}_p(\alpha)$ for some $\alpha \in K$. WLOG $\alpha$ is integral over $\mathbb{Q}_p$. Let $f(X) \in \mathbb{Z}_p(X)$ be its minimal polynomial. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we can choose $g(X) \in \mathbb{Z}[X]$ as in the preceding proposition. Then $K = \mathbb{Q}_p(\beta)$ for a root $\beta$ of a suitable $g$. Since $\mathbb{Q}(\beta)$ (which is a number field) is dense in $K = \mathbb{Q}_p(\beta)$, $K$ must be the completion of it. □

# 4 Dedekind Domains

## 4.1 Dedekind Domains and DVRs

**Definition 4.1.** A Dedekind domain $R$ is a ring satisfying the following properties:
(i) $R$ is a Noetherian integral domain.
(ii) $R$ is integrally closed.
(iii) Every nonzero prime ideal of $R$ is maximal.

**Example 4.1.** 1. The ring of integers of a number field is a Dedekind domain.
2. Any PID (hence any DVR) is a Dedekind domain.

**Theorem 4.1.** *A ring $R$ is a DVR if and only if $R$ is a Dedekind domain with exactly one nonzero prime ideal.*

**Lemma 4.2.** *Let $R$ be a Noetherian ring and $I \subset R$ is nonzero, then there are nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I$.*

*Proof.* Suppose not. Since $R$ is Noetherian, we can always find a counterexample $I$ which is maximal among all the counterexamples. Then $I$ is not prime, so there are $x, y \notin R \backslash I$ such that $xy \in I$. Let $I_1 = I + (x) \supsetneq I, I_2 = I + (y) \supsetneq I$. By maximality of $I$, we can choose nonzero primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I_1, \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I_2$, so $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I_1 I_2 \subset I$, contradiction. □

**Lemma 4.3.** *Let $R$ be an integral domain which is integrally closed. Suppose $I \subset R$ is a nonzero finitely generated ideal and $x \in K = \mathrm{FF}(R)$. Then $xI \subset I$ implies $x \in R$.*

*Proof.* Suppose $I = (c_1, \ldots, c_n)$. Since $xI \subset I$, $xc_i = \sum_j a_{ij} c_j$ for some $a_{ij} \in R$. Let $A = (a_{ij})_{i,j}$ and set $B = x\,\mathrm{id} - A$. Then $\det(B)(c_1, \ldots, c_n)^\top = \mathrm{adj}(B)B(c_1, \ldots, c_n)^\top = 0$ which shows that $\det B = 0$. So $x$ is a root of the characteristic polynomial of $A$, which is monic and has coefficients in $R$. Hence $x$ is integral over $R$, therefore $x \in R$. □

*Proof of Theorem 4.1.* The "only if" part is clear.
Conversely, suppose $R$ is a Dedekind domain with exactly one nonzero prime ideal. To show that $R$ is a DVR in this case, it suffices to show that $R$ is a PID.

Since $R$ has only one prime, $R$ is local and the prime $\mathfrak{m}$ has to be maximal.
Let's first show that $\mathfrak{m}$ is principal. Pick $x \in \mathfrak{m} \setminus \{0\}$. Then $(x) \supset \mathfrak{m}^n$ for some $n \geq 1$ by Lemma 4.2 Choose $n$ minimal such that this containment holds. Then there is some $y \in \mathfrak{m}^{n-1} \setminus (x)$. We let $\pi = x/y$. As $y\mathfrak{m} \subset \mathfrak{m}^n \subset (x)$ we know $\pi^{-1}\mathfrak{m} \subset R$. if $\pi^{-1}\mathfrak{m}$ is a proper ideal, then $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$, so $\pi \in R$ by the preceding lemma and therefore $y \in (x)$, contradiction. So $\pi^{-1}\mathfrak{m} = R$, i.e. $\mathfrak{m} = (\pi)$.
To see that $R$ is a PID, let $I$ be any nonzero ideal. Consider the sequence of fractional ideals $I \subset \pi^{-1}I \subset \pi^{-2}I \subset \cdots$, and the containments are all strict since $\pi^{-1} \notin R$. It eventually contains $R$ since $R$ is Noetherian. Choose a maximal $n$ such that $\pi^{-n}I \subset R$. If $\pi^{-n}I \neq R$, then $\pi^{-n}I \subset \mathfrak{m} = (\pi)$ and $\pi^{-(n+1)}I \subset R$, contradicting maximality of $n$. So $\pi^{-n}I = R$, i.e. $I = (\pi^n)$. □

Let $R$ be an integral domain and $S$ a subset of $R$ which contains 1, is multiplicatively closed, and doesn't contain 0. The localisation $S^{-1}R$ of $R$ at $S$ is the ring $S^{-1}R = \{r/s : r \in R, s \in S\} \subset \mathrm{FF}(R)$. We have a natural map (called the localisation map) $R \to S^{-1}R, r \mapsto r/1$ which is an inclusion in our case.

**Example 4.2.** If $\mathfrak{p}$ is a prime ideal in $R$, we write $R_{(\mathfrak{p})}$ to denote the localisation of $R$ at $R \setminus \mathfrak{p}$ (also known as the localisation of $R$ at the prime $\mathfrak{p}$). For example, if $\mathfrak{p} = (0)$, then $R_{(\mathfrak{p})} = \mathrm{Frac}(R)$. If $R = \mathbb{Z}$ and $p$ is a prime, then $\mathbb{Z}_{((p))} = \{a/b : a, b \in \mathbb{Z}, \gcd(b, p) = 1\}$.

**Proposition 4.4.** *(i) If $R$ is Noetherian, so are its localisations.*
*(ii) Localisation induces a bijection between prime ideals of $S^{-1}R$ and prime ideals of $R$ avoiding $S$.*

*Proof.* Standard. □

**Corollary 4.5.** *Localisations of a Dedekind domain at a nonzero prime is a DVR.*

*Proof.* Let $R$ be a Dedekind domain and $\mathfrak{p} \leq R$ a nonzero prime. Then $R_{(\mathfrak{p})}$ is a Noetherian integral domain with a unique nonzero prime ideal, which is necessarily maximal. In light of Theorem 4.1, it suffices to show that $R_{(\mathfrak{p})}$ is integrally closed in $K = \mathrm{FF}(R)$.
Let $x \in K$ be integral over $R_{(\mathfrak{p})}$, then there are some $a_{n-1}, \ldots, a_0 \in R$ such that $sx^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for some $s \notin \mathfrak{p}$. Then $(sx)^n + sa_{n-1}(sx)^{n-1} + \cdots + s^n a_0 = 0$, so $sx$ is integral over $R$ and hence in $R$, therefore $x \in R_{(\mathfrak{p})}$. □

**Definition 4.2.** If $R$ is a Dedekind domain and $\mathfrak{p} \leq R$ is a nonzero prime ideal, we write $v_\mathfrak{p}$ for the normalised valuation on $\mathrm{FF}(R) = \mathrm{FF}(R_{(\mathfrak{p})})$ induced by the valuation on the DVR $R_{(\mathfrak{p})}$.

**Example 4.3.** For $R = \mathbb{Z}, \mathfrak{p} = (p)$ where $p$ is a prime number, $v_\mathfrak{p}$ is simply the $p$-adic valuation on $\mathbb{Q}$.

**Theorem 4.6.** *Let $R$ be a Dedekind domain. Then every nonzero ideal in $R$ can be written in the form $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, unique up to permutation of indices, where $\mathfrak{p}_i$ are distinct primes and $e_i > 0$.*

*Proof.* From commutative algebra, we know that two ideals $I, J \leq R$ are equal iff $IR_{(\mathfrak{p})} = JR_{(\mathfrak{p})}$ for all primes $\mathfrak{p}$ of $R$, and that (when $R$ is a Dedekind domain) for any distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of $R$, we always have $\mathfrak{p}_1 R_{(\mathfrak{p}_2)} = R_{(\mathfrak{p}_2)}$.
Back to the proof, let $I \leq R$ be a nonzero ideal. We know that $\mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_r^{\beta_r} \subset I$ for some $\beta_i > 0$ and $\mathfrak{p}_i$ distinct nonzero primes.
For any other nonzero prime $\mathfrak{p}$, we must have $\mathfrak{p}_i R_{(\mathfrak{p})} = R_{(\mathfrak{p})}$ for all $i$, so $IR_{(\mathfrak{p})} = R_{(\mathfrak{p})}$. On the other hand, since localisations of Dedekind domains are DVRs, there is some $\alpha_i$ such that $IR_{(\mathfrak{p}_i)} = \mathfrak{p}_i^{\alpha_i} R_{(\mathfrak{p}_i)}$.
Hence $IR_{(\mathfrak{p})} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} R_{(\mathfrak{p})}$ for any prime $\mathfrak{p} \leq R$, which means that $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$. Uniqueness is also clear from this. □

## 4.2 Extensions of Dedekind Domains

Let $L/K$ be a finite field extension. For $x \in L$, we write $\mathrm{Tr}_{L/K}(x) \in K$ to denote the trace of the $K$-linear map $L \to L, y \mapsto xy$. If $L/K$ is separable and has degree $n$, then

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

where $\sigma_1, \ldots, \sigma_n : L \to \bar{K}$ are distinct embeddings of $L$ in $\bar{K}$.

**Lemma 4.7.** *Let $L/K$ be a finite separable field extension, then the symmetric bilinear pairing $(,); L \times L \to Y, (x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ (the "trace form") is non-degenerate.*

*Proof.* As $L/K$ is finite and separable, there is some $\alpha \in L$ such that $L = K(\alpha)$. Let $A$ be the matrix for the pairing under the basis $1, \alpha, \ldots, \alpha^{n-1}$, then $A_{ij} = \mathrm{Tr}_{L/K}(\alpha^{i+j}) = [BB^\top]_{ij}$ where

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

Then

$$\det A = (\det B)^2 = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \neq 0$$

by separability. □

*Remark.* In fact, the separability of $L/K$ is equivalent to the nondegeneracy of the trace form (example sheet).

**Theorem 4.8.** *Let $\mathcal{O}_K$ be a Dedekind domain, $K = \mathrm{FF}(\mathcal{O}_K)$ and $L/K$ is a finite field extension. Then the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in $L$ is also a Dedekind domain.*

*Remark.* We'll prove the theorem in the situation where $L/K$ is separable. The general case is true but will not concern us that much since the situations we're most interested in have characteristic 0.

*Proof.* $\mathcal{O}_L$ is certainly an integral domain since it's a subring of a field, and it is integrally closed since it's an integral closure (example sheet).
To see that $\mathcal{O}_L$ is Noetherian, let $e_1, \dots, e_n \in L$ be a $K$-basis for $L$. Rescale if needed, we may assume that $e_i \in \mathcal{O}_L$ for all $i$. Let $f_1, \dots, f_n \in L$ be the its dual basis with respect to the trace form, then $(e_i, f_i) = \delta_{ij}$.
For $x \in \mathcal{O}_L$, we can write $x = \sum_i \lambda_i f_i$ for $\lambda_i \in K$ with $\lambda_i = \mathrm{Tr}_{L/K}(xe_i)$. But the trace of an element in $\mathcal{O}_L$ must be in $\mathcal{O}_K$, for it's a sum of elements in $\bar{K}$ all of which must be integral over $\mathcal{O}_K$ (and therefore in $\mathcal{O}_K$). In particular, $\lambda_i \in \mathcal{O}_K$. So $\mathcal{O}_L \subset \mathcal{O}_K f_1 + \cdots + \mathcal{O}_K f_n$, forcing $\mathcal{O}_L$ to be finitely generated as a $\mathcal{O}_K$-module (as $\mathcal{O}_K$ is Noetherian), so it must itself be Noetherian.
It remains to show that every nonzero prime of $\mathcal{O}_L$ is maximal. Let $\mathfrak{P}$ be a nonzero prime of $\mathcal{O}_L$, then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime in $\mathcal{O}_K$. It is nonzero. Indeed, choose any $x \in \mathfrak{P} \setminus \{0\}$, then $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for some $a_i \in \mathcal{O}_K, a_0 \neq 0$. But then $a_0 \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, hence $\mathfrak{p} \neq (0)$. So $\mathfrak{p}$ must be maximal.
$\mathcal{O}_L/\mathfrak{P}$ is a domain and a finite-dimensional $\mathcal{O}_K/\mathfrak{p}$-algebra, hence is itself a field, which means that $\mathfrak{P}$ is maximal. □

**Corollary 4.9.** *The ring of integers of a number field is a Dedekind domain.*

**Definition 4.3.** Suppose $K$ is a number field with ring of integers $\mathcal{O}_K$. Let $\mathfrak{p}$ be a nonzero prime of $\mathcal{O}_K$. The $\mathfrak{p}$-adic absolute value on $K$ is defined by $|x|_\mathfrak{p} = (N\mathfrak{p})^{-v_\mathfrak{p}(x)}$ where $N\mathfrak{p} = \#(\mathcal{O}_K/\mathfrak{p})$.

Suppose $\mathcal{O}_K$ is a Dedekind domain, $K$ its fraction field and $L/K$ a finite separable extension. We write $\mathcal{O}_L$ to denote the integral closure of $\mathcal{O}_K$ in $L$.

**Lemma 4.10.** *Let $x \in \mathcal{O}_K \setminus \{0\}$, then*

$$x\mathcal{O}_K = \prod_{\mathfrak{p} \leq \mathcal{O}_K \text{ nonzero prime}} \mathfrak{p}^{v_\mathfrak{p}(x)}$$

*Proof.* This follows from the fact that $x(\mathcal{O}_K)_{(\mathfrak{p})} = (\mathfrak{p}(\mathcal{O}_K)_{(\mathfrak{p})})^{v_\mathfrak{p}(x)}$. □

**Definition 4.4.** Suppose $\mathfrak{P} \leq \mathcal{O}_L, \mathfrak{p} \leq \mathcal{O}_K$ be nonzero prime ideals. We say $\mathfrak{P} \mid \mathfrak{p}$ ("$\mathfrak{P}$ divides $\mathfrak{p}$") if $\mathfrak{P}$ appears in the factorisation of $\mathfrak{p}\mathcal{O}_L$.

**Theorem 4.11.** *Suppose $\mathfrak{p} \leq \mathcal{O}_K$ is prime and we have a factorisation $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, e_i > 0$. Then the absolute values on $L$ extending $|\cdot|_\mathfrak{p}$ are precisely $|\cdot|_{\mathfrak{P}_1}, \dots, |\cdot|_{\mathfrak{P}_r}$.*

*Proof.* By the preceding lemma, for any nonzero $x \in \mathcal{O}_K$ we have $v_{\mathfrak{P}_i}(x) = e_i v_{\mathfrak{p}_i}(x)$, hence each $|\cdot|_{\mathfrak{P}_i}$ does extend $|\cdot|_\mathfrak{p}$ up to equivalence.
Now suppose $|\cdot|$ is any absolute value on $L$ extending $|\cdot|_\mathfrak{p}$, then $|\cdot|$ is bounded on $\mathbb{Z}$ and hence non-Archimedean. Let $R = \{x \in L : |x| \leq 1\}$ be the valuation ring of $|\cdot|$. Then $\mathcal{O}_K \subset R$ and $R$ is integrally closed in $L$, so $\mathcal{O}_L \subset R$. Let $\mathfrak{P} = \{x \in \mathcal{O}_L : |x| < 1\} = \mathcal{O}_L \cap \mathfrak{m}_R$ where $\mathfrak{m}_R$ is the unique maximal ideal in $R$. Then $\mathfrak{P}$ must be prime, and also nonzero as it contains $\mathfrak{p}$. So we can localise.
We know $(\mathcal{O}_L)_{(\mathfrak{P})} \subset R$ and $(\mathcal{O}_L)_{(\mathfrak{P})}$ is a DVR, hence a maximal subring of $L$. But this means that $(\mathcal{O}_L)_{(\mathfrak{P})} = R$, which means that $|\cdot|$ is equivalent to $|\cdot|_\mathfrak{P}$.
As $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, we have $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subset \mathfrak{P}$, so $\mathfrak{P} = \mathfrak{P}_i$ for some $i$ by unique factorisation. □

Let $K$ be a number field. If $\sigma : K \to \mathbb{R}$ (resp. $\sigma : K \to \mathbb{C}$) is a real (resp. complex) embedding, then $x \mapsto |\sigma(x)|_\infty$ defines an absolute value on $K$ (example sheet), which we'll denote by $|\cdot|_\sigma$.

**Corollary 4.12.** *Let $K$ be a number field with ring of integers $\mathcal{O}_K$, then any absolute value on $K$ is equivalent to one of the following:*
*(i) $|\cdot|_\mathfrak{p}$ for some nonzero prime ideal $\mathfrak{p} \leq \mathcal{O}_K$.*
*(ii) $|\cdot|_\sigma$ for some real or complex embedding $\sigma$ of $K$.*

*Proof.* Any non-Archimedean absolute value must restrict to $|\cdot|_p$ on $\mathbb{Q}$ for some prime $p$ by Theorem 3.6. So it must be equivalent to some $|\cdot|_\mathfrak{p}$ by the preceding theorem. The Archimedean case is on the example sheet. □

## 4.3 Completions of Dedekind Domains

As usual let $\mathcal{O}_K$ be a Dedekind domain with fraction field $K$, $L/K$ finite separable. Let $\mathfrak{p} \in \mathcal{O}_K$ and $\mathfrak{P} \leq \mathcal{O}_L$ be prime ideals with $\mathfrak{P} \mid \mathfrak{p}$. We write $K_\mathfrak{p}$ and $L_\mathfrak{P}$ to denote their completions with respect to the absolute values $|\cdot|_\mathfrak{p}, |\cdot|_\mathfrak{P}$ respectively.

**Lemma 4.13.** *(i) The natural map $\pi_\mathfrak{P} : L \otimes_K K_\mathfrak{p} \to L_\mathfrak{P}$ is surjective.*
*(ii) $[L_\mathfrak{P} : K_\mathfrak{p}] \leq [L : K]$.*

*Proof.* Let $M = LK_\mathfrak{p} \subset L_\mathfrak{P}$ which is essentially the image of $\pi_\mathfrak{P}$. As $L/K$ is finite and separable, $L = K(\alpha)$ for some $\alpha \in L$. Then $M = K_\mathfrak{p}(\alpha)$ and hence $M$ is a finite extension of $K_\mathfrak{p}$ and $[M : K_\mathfrak{p}] \leq [L : K]$.
$M$ is complete since it's a finite extension of a complete valued field, and it lies between $L$ and $L_\mathfrak{P}$, so we must have $M = L_\mathfrak{P}$. □

**Lemma 4.14** (Chinese Remainder Theorem)**.** *Let $R$ be a ring and $I_1, \dots, I_n \leq R$ be ideals such that $I_i + I_j = R$ whenever $i \neq j$. Then $\bigcap_i I_i = \prod_i I_i$. Moreover, if we call this intersection $I$, then $R/I \cong \prod_i R/I_i$.*

*Proof.* Example sheet. □

**Theorem 4.15.** *The natural map $L \otimes_K K_\mathfrak{p} \to \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$ is an isomorphism.*

*Proof.* Write $L = K(\alpha)$ as usual. Let $f \in K[X]$ be the minimal polynomial of $\alpha$. Factorise $f(X) = f_1(X) \cdots f_r(X)$ into irreducibles $f_i \in K_\mathfrak{p}[X]$. Then they are distinct by separability. Since $L \cong K[X]/(f(X))$, we have $L \otimes_K K_\mathfrak{p} \cong K_\mathfrak{p}[X]/(f(X)) \cong \prod_{i=1}^r K_\mathfrak{p}[X]/(f_i(X))$. Set $L_i = K_\mathfrak{p}[X]/(f_i(X))$, which is a finite extension of $K_\mathfrak{p}$.
Each of these $L_i$ contains $K_\mathfrak{p}$. It also contains $L$ since the map $K[X]/(f(x)) \to K_\mathfrak{p}[X]/(f_i(X))$ is a morphism of fields, hence injective.
$L$ is moreover dense in $L_i$. Indeed, since $K$ is dense in $K_\mathfrak{p}$, we can approximate elements of $K_\mathfrak{p}[X]/(f_i(X))$ with elements of $K[X]/(f(X))$.
We claim the followings:
(i) For every $i$, $L_i \cong L_\mathfrak{P}$ for some $\mathfrak{P} \in \mathcal{O}_L$ dividing $\mathfrak{p}$.
(ii) Each prime ideal appears at most once in (i).
(iii) Each prime ideal appears at least once in (i).
(i) As $L_i/K_\mathfrak{p}$ is finite, there is a unique absolute value on $L_i$ extending $|\cdot|_\mathfrak{p}$. But this can only restrict to some $|\cdot|_\mathfrak{P}$ on $L$ by Theorem 4.11. Since $L$ is dense in $L_i$ and $L_i$ is complete, we must have $L_i \cong L_\mathfrak{P}$.

(ii) Suppose not, then there is an isomorphism $\phi : L_i \to L_j$ for some $i \neq j$ preserving both $L$ and $K_\mathfrak{p}$. Then $\phi : K_\mathfrak{p}[X]/(f_i(X)) \to K_\mathfrak{p}[X]/(f_j(X))$ must send $X$ to $X$, which can only happen when $f_i = f_j$, so $i = j$.
(iii) This follows from Lemma 4.13: The natural map $\pi_\mathfrak{P}$ is surjective and hence must factor through $L_i$ for some $i$, which means that $L_i \cong L_\mathfrak{P}$. □

**Example 4.4.** Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Then we can take $f(X) = X^2 + 1$ as in the theorem. By Hensel's lemma, $f$ has a root in $\mathbb{Q}_5$, hence (5) must split into two primes when extended to $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$.

**Corollary 4.16.** *For $x \in L$,*

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

*Proof.* Suppose $\mathfrak{P}_1, \dots \mathfrak{P}_r$ are the primes dividing $\mathfrak{p}$. Let $B_1, \dots, B_r$ be bases for $L_{\mathfrak{P}_i}/K_\mathfrak{p}$. Then $B = \bigcup_i B_i$ is a basis for $L \otimes_K K_\mathfrak{p}$ over $K_\mathfrak{p}$ by the preceding theorem. Let $[\mathrm{mult}(x)]_B$ (resp. $[\mathrm{mult}(x)]_{B_i}$) be the matrix for $\mathrm{mult}(x) : L \otimes_K K_\mathfrak{p} \to L \otimes_K K_\mathfrak{p}$ (resp. $L_{\mathfrak{P}_i} \to L_{\mathfrak{P}_i}$) with respect to the basis $B$ (resp. $B_i$). Then

$$[\mathrm{mult}(x)]_B = \begin{pmatrix} [\mathrm{mult}(x)]_{B_1} & & 0 \\ & \ddots & \\ 0 & & [\mathrm{mult}(x)]_{B_r} \end{pmatrix}$$

Computing the determinant of this gives the result. □

## 4.4 Decomposition Groups

Suppose $\mathfrak{p}$ is a nonzero prime of $\mathcal{O}_K$ and $\mathcal{O}_L$ is an extension of $\mathcal{O}_K$, both Dedekind domains. Suppose also that $L/K$ is finite and separable. We write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where $e_i > 0$ and $\mathfrak{P}_i$ are distinct primes in $\mathcal{O}_L$.
For any $i$, $\mathfrak{p} \leq \mathcal{O}_K \cap \mathfrak{P}_i \lneq \mathcal{O}_K$, so the maximality of $\mathfrak{p}$ implies $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$.

**Definition 4.5.** $e_i$ is called the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$. We say $\mathfrak{p}$ is ramified in $L$ if $e_i > 1$ for some $i$.

**Example 4.5.** Let $\mathcal{O}_K = \mathbb{C}[t]$ and $\mathcal{O}_L = \mathbb{C}[T]$. Consider $\mathcal{O}_K \to \mathcal{O}_L, t \mapsto T^n$. Then the ramification index of $(T)$ over $(t)$ is $n$. Geometrically, this corresponds to a covering of $\mathbb{A}^1$ by raising to the $n$-th power, which (in the sense of algebraic geometry) ramifies at 0 with ramification index $n$.

**Definition 4.6.** $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is called the residue class degree (or inertia degree) of $\mathfrak{P}_i$ over $\mathfrak{p}$.

**Theorem 4.17.** $\sum_i e_i f_i = [L : K]$.

*Proof.* Let $S = \mathcal{O}_K \setminus \mathfrak{p}$. Then from commutative algebra we know that $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K = (\mathcal{O}_K)_{(\mathfrak{p})}$ in $L$. Moreover, $(S^{-1}\mathfrak{p})S^{-1}\mathcal{O}_L \cong S^{-1}\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and $S^{-1}\mathcal{O}_L/S^{-1}\mathfrak{P}_i \cong \mathcal{O}_L/\mathfrak{P}_i$ and $S^{-1}\mathcal{O}_K/S^{-1}\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$.
The point of these is that we can essentially replace $\mathcal{O}_K$ with $S^{-1}\mathcal{O}_K$ and $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_L$, therefore assume WLOG that $\mathcal{O}_K$ is a DVR.
We have an isomorphism $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_i \mathcal{O}_L/\mathfrak{P}_i^{e_i}$. Let's count dimensions of both sides as $k = \mathcal{O}_K/\mathfrak{p}$-vector spaces.

For the right hand side, observe that there is an increasing sequence of $k$-subspaces $0 \leq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e^i} \leq \cdots \leq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \leq \mathcal{O}_L/\mathfrak{P}_i^{e_i}$. But each successive quotients $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is generated by any element of $\mathfrak{P}_i^j \setminus \mathfrak{P}_i^{j+1}$ as an $\mathcal{O}_L/\mathfrak{P}_i$-module, therefore $\dim_k \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1} = \dim_k \mathcal{O}_L/\mathfrak{P}_i = f_i$. So $\dim_k \mathcal{O}_L/\mathfrak{P}_i^{e_i} = e_i f_i$. It remains to show that $\dim_k \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = [L:K]$. Since $\mathcal{O}_K$ is a DVR hence a PID, the structure theorem of finite modules over PIDs imply that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module. Its rank can be no other than $n = [L:K]$. So $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_K/\mathfrak{p})^n$ as an $\mathcal{O}_K/\mathfrak{p}$-module, hence the result. □

What's the geometric intuition behind this? It actually corresponds to the valency theorem of Riemann surfaces: Recall that if $\phi : X \to Y$ is a degree $n$ cover of Riemann surfaces, then $n = \sum_{x \in \phi^{-1}(y)} e_x$ for every $y \in Y$ (the residue class degree is always 1 since $\mathbb{C}$ is algebraically closed). This can actually be implied by the theorem we just proved.
Back to algebra. Suppose $L/K$ is Galois. For any $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(\mathfrak{P}_i) \cap \mathcal{O}_K = \mathfrak{p}$, so $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some other $j$. So $\mathrm{Gal}(L/K)$ acts on $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$.

**Proposition 4.18.** *The action of* $\mathrm{Gal}(L/K)$ *on* $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ *is transitive.*

*Proof.* Suppose not, then there is some $i \neq j$ such that $\sigma(\mathfrak{P}_i)$ never equals $\mathfrak{P}_j$ for every $\sigma \in \mathrm{Gal}(L/K)$. We can choose an element $x \in \mathfrak{P}_i$ congruent to 1 modulo $\sigma(\mathfrak{P}_j)$ for every $\sigma \in \mathrm{Gal}(L/K)$. Since $L/K$ is Galois, we have $N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathcal{O}_K \cap \mathfrak{P}_i = \mathfrak{p} \subset \mathfrak{P}_j$. As $\mathfrak{P}_j$ is prime, there is some $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(x) \in \mathfrak{P}_j$, which means that $x \in \tau^{-1}(\mathfrak{P}_j)$, i.e. $x$ is congruent to 0 modulo $\tau^{-1}(\mathfrak{P}_j)$, contradiction. □

**Corollary 4.19.** *If $L/K$ is Galois, then $e_1 = \cdots = e_r, f_1 = \cdots = f_r$. In particular, $n = efr$ where $e = e_1, f = f_1$.*

*Proof.* All the ramification indices equal since $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L)$. The residue class degree are also the same since $\mathcal{O}_L/\mathfrak{P}_i \cong \mathcal{O}_L/\sigma(\mathfrak{P}_i)$. □

**Corollary 4.20.** *Suppose now that $L/K$ is a finite separable extension of complete discretely valued field with normalised valuations $v_L, v_K$ and uniformisers $\pi_L, \pi_K$. Then the ramification index of the extension is just $e = e_{L/K} = v_L(\pi_K)$, the residue class degree is $f = f_{L/K} = [k_L : k]$, and we have $[L:K] = ef$.*

*Remark.* This corollary holds even without the separability assumption on $L/K$.

Back to the case where $\mathcal{O}_K$ is a Dedekind domain and $L/K$ is finite and Galois.

**Definition 4.7.** The decomposition group $G_{\mathfrak{P}}$ of at a prime $\mathfrak{P}$ of $\mathcal{O}_L$ is the stabiliser of $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$.

Then $G_{\mathfrak{P}}$ is conjugate to $G_{\mathfrak{P}'}$ if $\mathfrak{P}, \mathfrak{P}'$ lie over the same prime of $\mathcal{O}_K$.

**Proposition 4.21.** *Suppose $L/K$ is Galois and $\mathfrak{P} \leq \mathcal{O}_L$ is a prime lying over $\mathfrak{p} \leq \mathcal{O}_K$, then $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois and the restriction map $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$ is injective and has image $G_{\mathfrak{P}}$.*

*Proof.* Suppose $L$ is the splitting field of $f \in K[X]$. Then $L_{\mathfrak{P}}$ is the splitting field of $f$ over $K_{\mathfrak{p}}$, hence Galois.
Let $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, then $\sigma$ fixes $L$ since $L/K$ is normal. So the restriction map is well-defined, necessarily injective since $L$ is dense in $L_{\mathfrak{P}}$. As for its image, observe that $|\sigma(x)|_{\mathfrak{P}} = |x|_{\mathfrak{P}}$ for any $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ and $x \in L_{\mathfrak{P}}$. This means that $\sigma$ fixes $\mathfrak{P}$, therefore the image is contained in $G_{\mathfrak{P}}$.
To see that it surjects onto $G_{\mathfrak{P}}$, let's count dimensions. It suffices to show that $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef = \#G_{\mathfrak{P}}$. The first equality follows from the preceding corollary applied to $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ (note that $e, f$ don't change under taking completions). The second equality follows from Proposition 4.18 and Corollary 4.19. □

# 5 Ramification Theory

Let $p$ be a prime number. We know that it factors as $p = p_1 p_2$ into primes in $\mathbb{Z}[i]$ iff it is the sum of two squares. Let's extend this idea.

## 5.1 Different and Discriminant

Suppose $L/K$ is an extension of algebraic number fields with $[L : K] = n$.

**Definition 5.1.** Let $x_1, \dots, x_n \in L$. Their discriminant is $\Delta(x_1, \dots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j))_{i,j} \in K$.

It's easy to show that $\Delta(x_1, \dots, x_n) = (\det(\sigma_i(x_j))_{i,j})^2$, where $(\sigma_i)$ are distinct embeddings $L \to \bar{K}$. Note that if $y_i = \sum_j A_{ij} x_j$, then $\Delta(y_1, \dots, y_n) = (\det A)^2 \Delta(x_1, \dots, x_n)$.
It's also clear that $\Delta(x_1, \dots, x_n) \in \mathcal{O}_K$ whenever $x_1, \dots, x_n \in \mathcal{O}_K$.

**Lemma 5.1.** *Let $k$ be a perfect field and $R$ a finite-dimensional $k$-algebra. The trace form $(,) : R \times R \to k$ defined via $(x, y) = \mathrm{Tr}_{R/k}(xy) = \mathrm{Tr}_R(\mathrm{mult}_{xy})$ is nondegenerate iff $R \cong k_1 \times \cdots \times k_n$ where $k_1, \dots, k_n$ are finite (hence separable) field extensions of $k$.*

*Proof.* Example sheet. □

**Theorem 5.2.** *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$.*
*(i) If $\mathfrak{p}$ ramifies in $L$, then $\mathfrak{p} \mid (\Delta(x_1, \dots, x_n))$ for any $x_1, \dots, x_n \in \mathcal{O}_L$.*
*(ii) If $\mathfrak{p}$ is unramified in $L$, then $\mathfrak{p} \nmid (\Delta(x_1, \dots, x_n))$ for some $x_1, \dots, x_n \in \mathcal{O}_L$.*

*Proof.* (i) Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where $\mathfrak{P}_i \leq \mathcal{O}_L$ are distinct and $e_i > 0$. By Lemma 4.14, we have $R = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_i \mathcal{O}_L/\mathfrak{P}_i^{e_i}$. If some $e_i$ is strictly greater than 1, then $R$ contains nonzero nilponents so the preceding lemma forces the trace form on $R$ to be degenerate. So $\Delta(x_1, \dots, x_n) \in \mathfrak{p}\mathcal{O}_L$ for all $x_i \in \mathcal{O}_L$. But this discriminant is always in $\mathcal{O}_K$, so $\Delta(x_1, \dots, x_n) \in \mathfrak{p}$.
(ii) Again with the preceding lemma we know that the trace form on $R$ is nondegenerate in this case, so we can just pick a basis $\bar{x}_1, \dots, \bar{x}_n$ of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. Then their lifts $(x_i)$ would have $\Delta(x_1, \dots, x_n) \notin \mathfrak{p}\mathcal{O}_L$, hence $\Delta(x_1, \dots, x_n) \notin \mathfrak{p}$. □

**Definition 5.2.** The discriminant of $L$ is the ideal $d_{L/K} \leq \mathcal{O}_K$ generated by $\Delta(x_1, \dots, x_n), x_1, \dots, x_n \in \mathcal{O}_L$.

**Corollary 5.3.** $\mathfrak{p} \leq \mathcal{O}_K$ *ramifies in* $L$ *iff* $\mathfrak{p} \mid d_{L/K}$. *In particular, only finitely many prime ideals ramify.*

**Definition 5.3.** The inverse different ideal is the set $D_{L/K}^{-1} = \{y \in L : \forall x \in \mathcal{O}_L, \operatorname{Tr}_{L/K}(xy) \in \mathcal{O}_K\}$.

It's immediate that $D_{L/K}^{-1}$ is an $\mathcal{O}_L$-submodule of $L$ containing $\mathcal{O}_L$.

**Lemma 5.4.** $D_{L/K}^{-1}$ *is a fractional ideal in* $L$.

*Proof.* Let $x_1, \ldots, x_n \in \mathcal{O}_L$ be a $K$-basis for $L$. Set $d = \Delta(x_1, \ldots, x_n) = \det A \in \mathcal{O}_K$, where $A = (\operatorname{Tr}_{L/K}(x_i x_j))_{i,j}$. For any $x \in D_{L/K}^{-1}$, we can write $x = \sum_j \lambda_j x_j$ for some $\lambda_j \in K$. Then $\operatorname{Tr}_{L/K}(xx_i) = \sum_j \lambda_j \operatorname{Tr}_{L/K}(x_j x_i)$.
Note that $\operatorname{Adj} A$ has coefficients in $\mathcal{O}_K$, so

$$d \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \operatorname{Adj}(A) \begin{pmatrix} \operatorname{Tr}_{L/K}(xx_1) \\ \vdots \\ \operatorname{Tr}_{L/K}(xx_n) \end{pmatrix}$$

Therefore $\lambda_i \in d^{-1}\mathcal{O}_K$, so $x \in d^{-1}\mathcal{O}_L$ and hence $D_{L/K}^{-1} \subset d^{-1}\mathcal{O}_L$, which means that $D_{L/K}^{-1}$ must be a fractional ideal. □

Since $D_{L/K}^{-1}$ contains $\mathcal{O}_L$, its inverse is an ideal of $\mathcal{O}_L$.

**Definition 5.4.** The inverse $D_{L/K} \leq \mathcal{O}_L$ of $D_{L/K}^{-1}$ is called the different ideal of $L$ over $K$.

Set $\mathscr{I}_L, \mathscr{I}_K$ to be the groups of fractional ideals in $L, K$. They are both freely generated over their respective prime ideals by unique factorisation. Let $N_{L/K} : \mathscr{I}_L \to \mathscr{I}_K$ be the group homomorphism taking a prime $\mathfrak{P}$ to $\mathfrak{p}^f$ where $f = f_{\mathfrak{P}|\mathfrak{p}}$ is the residue class degree of $\mathfrak{P}$ over $\mathfrak{p}$. The diagram

$$\begin{array}{ccc} L^\times & \longrightarrow & \mathscr{I}_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K^\times & \longrightarrow & \mathscr{I}_K \end{array}$$

commutes since $v_{\mathfrak{p}}(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x)) = f_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(x)$ for $x \in L_{\mathfrak{P}}^\times$.

**Theorem 5.5.** $N_{L/K}(D_{L/K}) = d_{L/K}$.

*Proof.* First assume that $\mathcal{O}_K, \mathcal{O}_L$ are PIDs. Let $x_1, \ldots, x_n$ be an $\mathcal{O}_K$-basis for $\mathcal{O}_L$ and $y_1, \ldots, y_n$ be its dual basis with respect to the trace form. Then $y_1, \ldots, y_n$ form a basis for $D_{L/K}^{-1}$. Let $\sigma_1, \ldots, \sigma_n \to \bar{K}$ be distinct embeddings of $L$. Then

$$\sum_{i=1}^{n} \sigma_i(x_j)\sigma_i(y_k) = \operatorname{Tr}_{L/K}(x_j y_k) = \delta_{jk}$$

We also know that $\Delta(x_1, \ldots, x_n) = (\det(\sigma_i(x_j))_{i,j})^2$. Putting them together gives us $\Delta(x_1, \ldots, x_n)\Delta(y_1, \ldots, y_n) = 1$.
Write $D_{L/K}^{-1} = \beta\mathcal{O}_L$ (allowed since we've assumed that $\mathcal{O}_L$ is a PID). Then

$$\Delta(x_1, \ldots, x_n)^{-1} = \Delta(y_1, \ldots, y_n) = \Delta(\beta x_1, \ldots, \beta x_n) = N_{L/K}(\beta)^2 \Delta(x_1, \ldots, x_n)$$

Thus $d_{L/K}^{-1} = N_{L/K}(\beta)^2 d_{L/K}$, so $(N_{L/K}(\beta)) = N_{L/K}(D_{L/K}^{-1}) = d_{L/K}^{-1}$.
For the general case, we localise at $S = \mathcal{O}_K \setminus \mathfrak{p}$ and observe that $S^{-1}D_{L/K} = D_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$ and that $S^{-1}d_{L/K} = d_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$. □

**Theorem 5.6.** *If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$ and $\alpha$ has minimal polynomial $g(X) \in \mathcal{O}_K[X]$. Then $D_{L/K} = (g'(\alpha))$.*

*Proof.* Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of $g$. $g(X)/(X-\alpha) = \beta_{n-1}X^{n-1} + \beta_{n-2}X^{n-2} + \cdots + \beta_0, \beta_{n-1} = 1$ is a polynomial with coefficients in $\mathcal{O}_L$. We claim that

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

for $0 \leq r \leq n-1$. Indeed, the difference of the two sides has degree strictly less than $n$ but vanishes at each $\alpha_i$.
Equating the coefficients, we obtain $\mathrm{Tr}_{L/K}(\alpha^r \beta_s / g'(\alpha)) = \delta_{rs}$. $1, \alpha, \ldots, \alpha^{n-1}$ form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$, $D_{L/K}^{-1}$ is spanned by $\beta_0/g'(\alpha), \ldots, \beta_{n-1}/g'(\alpha)$ over $\mathcal{O}_K$. But $\beta_{n-1} = 1$. So $D_{L/K}^{-1} = (1/g'(\alpha))$, which means that $D_{L/K} = (g'(\alpha))$. □

Let $\mathfrak{P} \leq \mathcal{O}_L$ be a prime lying over $\mathfrak{p}$. $D_{L_\mathfrak{P}/K_\mathfrak{p}}$ can be defined similarly using $\mathcal{O}_{K_\mathfrak{p}}, \mathcal{O}_{L_\mathfrak{P}}$.

**Theorem 5.7.** $D_{L/K} = \prod_{\mathfrak{P}|\mathfrak{p}} D_{L_\mathfrak{P}/K_\mathfrak{p}}$.

We'll later show that this is a finite product. For now, we'll just assume it.

*Proof.* Let $x \in L$ and $\mathfrak{p} \leq \mathcal{O}_K$ prime. Then

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

Let $r(\mathfrak{P}) = v_\mathfrak{p}(D_{L/K}), s(\mathfrak{P}) = v_\mathfrak{p}(D_{L_\mathfrak{P}/K_\mathfrak{p}})$. Let's first show that $r(\mathfrak{P}) \geq s(\mathfrak{P})$. Suppose $x \in L$ is such that $v_\mathfrak{P}(x) \geq -s(\mathfrak{P})$ for all $\mathfrak{P}$. Then $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_L$ and all $\mathfrak{P}$. Therefore $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_L$ and $\mathfrak{p}$. So $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K$ for all $y \in \mathcal{O}_L$, which means that $x \in D_{L/K}^{-1}$.
Conversely, we shall show that $r(\mathfrak{P}) \leq s(\mathfrak{P})$. Fix $\mathfrak{P}$ and let $x \in \mathfrak{P}^{-r(\mathfrak{P})}$. Then $v_\mathfrak{P}(x) = r(\mathfrak{P})$ and $v_{\mathfrak{P}'}(x) \geq 0$ for all $\mathfrak{P}' \neq \mathfrak{P}$. So for any $y \in \mathcal{O}_L$,

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

which means that $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for any $y \in \mathcal{O}_{L_\mathfrak{P}}$ by continuity. This means that $x \in D_{L_\mathfrak{P}/K_\mathfrak{p}}^{-1}$, i.e. $-v_\mathfrak{P}(x) = r(\mathfrak{P}) \leq s(\mathfrak{P})$. □

**Corollary 5.8.** $d_{L/K} = \prod_{\mathfrak{P}|\mathfrak{p}} d_{L_\mathfrak{P}/K_\mathfrak{p}}$.

*Proof.* Take norms. □

## 5.2 Unramified and Totally Ramified Extensions

Let $L/K$ be a finite separable extension of non-Archimedean local fields (we'll just call them local fields from now on). Recall that $[L:K] = e_{L/K} f_{L/K}$.

**Lemma 5.9.** *Let $M/L/K$ be finite separable extensions of local fields. Then:*
*(i) $f_{M/K} = f_{M/L} f_{M/K}$.*
*(ii) $e_{M/K} = e_{M/L} e_{L/K}$.*

*Proof.* (i) follows from the tower law for residue fields, and (ii) follows from (i) and the tower law for the fields themselves. □

**Definition 5.5.** A finite separable extension $L/K$ of local fields is unramified if $e_{L/K} = 1$ (equivalently $f_{L/K} = [L:K]$), ramified if $e_{L/K} > 1$ (equivalently $f_{L/K} < [L:K]$), and totally ramified if $e_{L/K} = [L:K]$ (equivalently $f_{L/K} = 1$).

**Proposition 5.10.** *There exists a field $K_0$ between $K$ and $L$ such that $K_0/K$ is unramified and $L/K_0$ is totally ramified. Moreover, $[K_0:K] = f_{L/K}, [L:K_0] = e_{L/K}$ and $K_0/K$ is Galois.*

$K_0$ is known as the maximal unramified extension of $K$ in $L$.

*Proof.* Let $k = \mathbb{F}_q$ be the residue field of $K$. So the residue field $k_L$ of $L$ is $\mathbb{F}_{q^f}$ where $f = f_{L/K}$. Set $m = q^f - 1$ and let $[-] : \mathbb{F}_{q^f} \to L$ be the Teichmüller lift for $L$. Let $\zeta_m = [\alpha]$ where $\alpha$ is a generator for $\mathbb{F}_{q^f}^\times$. Then $\zeta_m$ is a primitive $m$-th root of unity.
Set $K_0 = K[\zeta_m]$, which is cyclotomic and hence Galois over $K$. As $K_0$ has residue field $k_0 = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^f}$. Let res : $\mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_0/k)$ be the restriction map. This is injective: For $\sigma \in \mathrm{Gal}(K_0/K)$, $\sigma(\zeta_m)$ is determined by its reduction to the residue field since $\mathcal{O}_{K_0}^\times \to k_0^\times$ induces a bijection between the $m$-th roots of unity (by Theorem 2.1).
Therefore $[K_0:K] = \#\,\mathrm{Gal}(K_0/K) \le \#\,\mathrm{Gal}(k_0/k) = f_{K_0/K}$, so we must have $f_{K_0/K} = [K_0:K]$, which in turn means that res is an isomorphism, so $K_0/K$ is unramified. Since $k_0 = k_L$, $f_{L/K} = f_{K_0/K} = [K_0:K]$, and $L/K_0$ has to be totally ramified with degree $e_{L/K}$ by tower law. □

**Theorem 5.11.** *Suppose $k = \mathbb{F}_q$ is the residue field of $K$. For any $n \ge 1$, there exists a unique unramified extension $L/K$ of degree $n$. Moreover, $L/K$ is Galois and the natural restriction map* res : $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ *is an isomorphism. In particular,* $\mathrm{Gal}(L/K)$ *is cyclic and is generated by an element* $\mathrm{Frob}_{L/K}$ *restricting to the Frobenius* $(x \mapsto x^q) \in \mathrm{Gal}(k_L/k)$.

*Proof.* We take $L = K(\zeta_m)$ where $m = q^n - 1$ and $\zeta_m$ is a primitive $m$-th root of unity. As in the proof of the preceding theorem, res : $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is an isomorphism. This shows existence.
As for uniqueness, suppose $L/K$ is any degree $n$ unramified extension. Then using Teichmüller lift we can show that $\zeta_m \in L$ for some primitive $m$-th root of unity $\zeta_m$, where $m = p^n - 1$. But then $L = K(\zeta_m)$. □

**Corollary 5.12.** *Suppose $L/K$ is a finite Galois extension of local fields. Then* res : $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ *is surjective.*

*Proof.* The restriction map factors through $\mathrm{Gal}(K_0/K)$. □

**Definition 5.6.** The kernel of the restriction map as in the corollary is called the inertia subgroup $I_{L/K}$ associated with the field extension $L/K$.

Then $I_{L/K} = \mathrm{Gal}(L/K_0)$ and $\#I_{L/K} = e_{L/K}$ by what we've discussed.

**Definition 5.7.** A polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ is Eisenstein if $v_K(a_i) \geq 1$ for all $i$ and $v_K(a_0) = 1$, where $v_K$ is the normalised valuation on $K$.

It's easy to generalise Eisenstein's criterion and show that all Eisenstein polynomials are irreducible.

**Theorem 5.13.** *(i) Let $L/K$ be a finite, totally ramified extension of local fields and $\pi_L \in \mathcal{O}_L$ a uniformiser. Then the minimal polynomial of $\pi_L$ is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. In particular, $L = K(\pi_L)$.*
*(ii) Conversely, if $f(X) \in \mathcal{O}_K[X]$ is Eisenstein and $\alpha$ is a root of $f$, then $K(\alpha)$ is totally ramified and $\alpha$ is a uniformiser in $L$.*

*Proof.* (i) Write $[L : K] = e$. Write $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ be the minimal polynomial of $\pi_L$. Then $m \leq e$. Let $v_L$ be the normalised valuation on $L$. Then $v_L(K^\times) = e\mathbb{Z}$, we have $v_L(a_i\pi_L^i) \equiv i \pmod{e}$ for all $i < n$. So all these terms have distinct valuations. As $\pi_L^m = -\sum_{i=0}^{m-1} a_i\pi_L^i$, we have $m = \min_{0\leq i\leq m-1}\{i + ev_K(a_i)\}$, so $v_K(a_i) \geq 1$ for all $i$ and hence $v_K(a_0) = 1$ (so $f$ is Eisenstein) and $m = e$ (so $L = K(\pi_L)$).
For $y \in L$, we write $y = \sum_{i=0}^{e-1} b_i\pi_L^i, b_i \in K$. Then $v_L(y) = \min_{0\leq i\leq l-1}(i + ev_k(b_i))$. Therefore $y \in \mathcal{O}_L$ iff $v_K(b_i) \geq 0$ iff $y \in \mathcal{O}_K[\pi_L]$.
(ii) Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ be an Eisenstein polynomial and $\alpha$ a root of it. Let $e = e_{L/K}$ where $L = K(\alpha)$. Thus $v_L(a_i) \geq e$ and $v_L(a_0) = e$. If $v_L(\alpha) \leq 0$, we have $v_L(\alpha^n) < v_L(-\sum_{i=0}^{n-1} a_i\alpha^i)$, contradiction. Hence $v_L(\alpha) > 0$. For $i \neq 0$, we have $v_L(a_i\alpha^i) > e = v_L(a_0)$, therefore

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

But $n = [L : K] \geq e$, so $n = e$ and $v_L(\alpha) = 1$. □

## 5.3 Units in Local Fields

Consider first the mixed characteristic case, where $K$ is a finite extension of $\mathbb{Q}_p$. Set $e = e_{K/\mathbb{Q}_p}$ (the "absolute ramification index") and let $\pi$ be a uniformiser.

**Proposition 5.14.** *If $r > e/(p-1)$, then*

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

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

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

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

Since $r > e/(p-1)$, $v_K(x^n/n!) \to \infty$ as $n \to \infty$, so $\exp(x)$ always converges. The computation also shows that we always have $v_K(x^n/n!) \geq r$ for any $n \geq 1$, so $\exp(x) \in 1 + \pi^r \mathcal{O}_K$. Similarly, we can consider

$$\log : 1 + \pi^r \mathcal{O}_K \to \pi^r \mathcal{O}_K, \log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n$$

which converges as one can check very easily.
But $\exp(X+Y) = \exp(X)\exp(Y), \log(\exp(X)) = X, \exp(\log(1+X)) = 1+X$ are true in $\mathbb{Q}[[X,Y]]$, so they are also true for the functions defined by them in this case, hence the result. □

What about a general local field $K$ (not necessarily of mixed characteristic)? Write $U_K = \mathcal{O}_K^\times$ and fix a uniformiser $\pi \in \mathcal{O}_K$.

**Definition 5.8.** For $s \in \mathbb{Z}$, the $s$-th unit group is $U_K^{(s)} = 1 + \pi^s \mathcal{O}_K$, which is a group under multiplication. Set $U_K^{(0)} = U_K$.

We have the filtration $\cdots \subset U_k^{(s)} \subset U_k^{(s-1)} \subset \cdots \subset U_K^{(0)} = U_K$.

**Proposition 5.15.** *(i)* $U_K^{(0)}/U_K^{(1)} \cong (k^\times, \times)$ *where* $k = \mathcal{O}_K/(\pi)$.
*(ii)* $U_K^{(s)}/U_K^{(s+1)} \cong (k, +)$ *for* $s \geq 1$.

*Proof.* (i) The reduction map $U_K \to k^\times$ is surjective with kernel $U_K^{(1)}$.
(ii) The map $f : U_K^{(s)} \to k$ via $1 + \pi^s x \mapsto x \bmod \pi$ is a surjective group homomorphism with kernel $U_K^{(s+1)}$. □

**Corollary 5.16.** *Back to the case where $K$ has mixed characteristic. Then there is a finite index subgroup of $\mathcal{O}_K^\times$ isomorphic to $(\mathcal{O}_K, +)$.*

*Proof.* Take $r > e/(p-1)$. We already know that $U_K^{(r)} \cong (\mathcal{O}_K, +)$ by exp and log. The preceding proposition shows that it indeed has finite index in $\mathcal{O}_K$. □

*Remark.* This does not necessarily hold in equal characteristic, mainly because exp is ill-defined.

**Example 5.1.** The exponential map is quite useful. Let $p > 2$ be prime and consider $K = \mathbb{Q}_p$. Then we can take $r = 1$. We always have $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p), x \mapsto (x \bmod p, x/[x \bmod p])$, which in turn is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. What if $p = 2$? Then we can't take $r = 1$, but we can take $r = 2$. We have $\mathbb{Z}_2^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + 4\mathbb{Z}_2), x \mapsto (x \bmod 4, x/\epsilon(x))$ where $\epsilon(x) = 1$ if $x \equiv 1 \pmod 4$ and $-1$ if $x \equiv 3 \pmod 4$. So the result on exponential gives $\mathbb{Z}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.
These give an alternative proof of the fact that

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

## 5.4 Higher Ramification Groups

Suppose $L/K$ is a finite Galois extension of local fields and let $\pi_L \in \mathcal{O}_L$ be a uniformiser. Let $v_L$ be the normalised valuation on $L$.

**Definition 5.9.** For $s \in \mathbb{R}_{\geq -1}$, the $s$-th ramification group is $G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \forall x \in \mathcal{O}_L, v_L(\sigma(x) - x) \geq s+1\}$.

**Example 5.2.** $G_{-1}(L/K) = \mathrm{Gal}(L/K)$. $G_0(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \forall x \in \mathcal{O}_L, \sigma(x) \equiv x \pmod{\pi}\} = \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)) = I_{L/K}$.

*Remark.* When $s \in \mathbb{Z}_{\geq 0}$, $G_s(L/K) = \ker(\mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{O}_L/\pi_L^{s+1}\mathcal{O}_L))$. In particular, $G_s(L/K)$ is a normal subgroup of $\mathrm{Gal}(L/K)$.
We also have a filtration $\cdots \subset G_s \subset G_{s-1} \subset \cdots \subset G_{-1}$.

$G_s$ only changes at integer values of $s$, so why did we ask $s \in \mathbb{R}_{\geq -1}$ instead of $s \in \mathbb{Z}_{\geq -1}$? It's so that it'll be compatible with the upper-numbering of these groups.

**Theorem 5.17.** *(i) For $s > 1$, $G_s = \{\sigma \in G_0 : v_L(\sigma(\pi_L) - \pi_L) \geq s+1\}$.*
*(ii) We have*

$$\bigcap_{s=0}^{\infty} G_s = \{1\}$$

*(iii) Let $s \in \mathbb{Z}_{\geq 0}$, then there is an injective group homomorphism $G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$ induced by $\sigma \mapsto \sigma(\pi_L)/\pi_L$. Moreover, this homomorphism is independent of the choice of $\pi_L$.*

*Proof.* Replacing $K$ by the maximal unramified extension $K_0 \subset L$ of it in $L$, we may assume WLOG that $L/K$ is totally ramified.
(i) We know that $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Suppose $v_L(\sigma(\pi_L) - \pi_L) \geq s+1$. For any $x \in \mathcal{O}_L$, we can write $x = f(\pi_L)$ for some $f(X) \in \mathcal{O}_K[X]$. So $\sigma(x) - x = \sigma(f(\pi_L)) - f(\pi_L) = f(\sigma(\pi_L)) - f(\pi_L) = (\sigma(\pi_L) - \pi_L)g(\pi_L)$ for some $g(\pi_L) \in \mathcal{O}_L$, so $v_L(\sigma(x) - x) \geq s+1$.
(ii) Suppose $\sigma \in \mathrm{Gal}(L/K), \sigma \neq 1$. Then $\sigma(\pi_L) \neq \pi_L$ since $L = K(\pi_L)$. But then $\sigma \notin G_{1+v_L(\sigma(\pi_L)-\pi_L)}$.
(iii) For $\sigma \in G_s, s \in \mathbb{Z}_{\geq 0}$, we have $\sigma(\pi_L) \in \pi_L + \pi_L^{s+1}\mathcal{O}_L$, so $\sigma(\pi_L)/\pi_L \in 1 + \pi_L^s\mathcal{O}_L = U_L^{(s)}$. This means that $G_s \to U_L^{(s)}/U_L^{(s+1)}$ is a well-defined map. It is a group homomorphism: For $\sigma, \tau \in G_s$, we can write $\tau(\pi_L) = u\pi_L$ for some $u \in \mathcal{O}_L^\times$. Then

$$\frac{(\sigma\tau)(\pi_L)}{\pi_L} = \frac{(\sigma\tau)(\pi_L)}{\tau(\pi_L)}\frac{\tau(\pi_L)}{\pi_L} = \frac{\sigma(u)}{u}\frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L}$$

But $\sigma(u) \in u + \pi_L^{s+1}\mathcal{O}_L$ since $\sigma \in G_s$. Therefore $\sigma(u)/u \in 1 + \pi_L^{s+1}\mathcal{O}_L = U_L^{(s+1)}$, so the map is a group homomorphism. It's clear that the kernel is exactly $G_{s+1}$, so we get an injective homomorphism $G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$.
If $\pi_L' = u\pi_L, u \in \mathcal{O}_L^\times$ is another uniformiser, the same computation as above shows that the homomorphism doesn't change at all. □

**Corollary 5.18.** *Given a finite Galois extension $L/K$ of local fields,* $\mathrm{Gal}(L/K)$ *is solvable.*

*Proof.* For $s \in \mathbb{Z}_{\geq -1}$, $G_s/G_{s+1}$ is isomorphic to either a subgroup of $\mathrm{Gal}(k_L/k)$ (when $s = -1$) or a subgroup of $(k_L^\times, \times)$ (when $s = 0$) or a subgroup of $(k_L, +)$ (when $s \geq 1$). These are all abelian groups. □

Suppose $\mathrm{char}\, k = p > 0$. Then $p \nmid \#(G_0/G_1)$ and $\#G_1$ is a power of $p$. So $G_1$ is the unique $p$-Sylow subgroup of $G_0$.

**Definition 5.10.** $G_1$ is called the wild inertia group and $G_0/G_1$ is called the tame quotient.

**Definition 5.11.** Suppose $L/K$ is finite and separable. It is tamely ramified if $\mathrm{char}\, k \nmid e_{L/K}$ (if $L/K$ is Galois, this is to say $G_1 = \{1\}$). Otherwise it is wildly ramified.

**Theorem 5.19.** *Suppose $K$ is a finite extension of $\mathbb{Q}_p$ and $L/K$ is a finite extension. Write $D_{L/K} = (\pi_L)^{\delta(L/K)}$. Then $\delta(L/K) \geq e_{L/K} - 1$ with equality iff $L/K$ is tamely ramified. In particular, $L/K$ is unramified if and only if $D_{L/K} = \mathcal{O}_L$.*

*Proof.* By example sheet, $D_{L/K} = D_{L/K_0} D_{K_0/K}$ holds for any intermediate field $K_0$ between $L$ and $K$. We are gonna take $K_0$ to be the maximal unramified extension, so it suffices to show the unramified and totally ramified cases.
Suppose $L/K$ is unramified, then $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$. Let $g \in \mathcal{O}_K[X]$ be the minimal polynomial for $\alpha$. Since $[L : K] = [k_L : k]$, the reduction $\bar{g} \in k[X]$ of $g$ modulo $\pi_K$ is the minimal polynomial of $\bar{\alpha} \in k_L$, the reduction of $\alpha$ modulo $\pi_L$. $\bar{g}$ is separable, so $g'(\alpha) \notin (\pi_L)$. Consequently $D_{L/K} = (g'(\alpha)) = \mathcal{O}_L$.
Now suppose $L/K$ is totally ramified. Then $[L : K] = e = e_{L/K}$ and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. The minimal polynomial of $\pi_L$ is an Eisenstein polynomial $g(X) = X^e + \sum_{i=0}^{e-1} a_i X^i \in \mathcal{O}_K[X]$. Then $g'(\pi_L) \equiv e\pi_L^{e-1} \pmod{\pi_L^e}$, hence $v_L(g'(\pi_L)) \geq e - 1$ with equality if and only if $p \nmid e$. □

**Corollary 5.20.** *Suppose $L/K$ is an extension of number fields and $\mathfrak{P} \leq \mathcal{O}_L, \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Then $e(\mathfrak{P} \mid \mathfrak{p}) > 1$ iff $\mathfrak{P} \mid D_{L/K}$.*

*Proof.* $D_{L/K} = \prod_{\mathfrak{P}} D_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ and $e(\mathfrak{P} \mid \mathfrak{p}) = e_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$. □

**Example 5.3.** Suppose $K = \mathbb{Q}_p$ and $\xi_{p^n}$ is a primitive $p^n$-th root of unity and $L = \mathbb{Q}_p(\xi_{p^n})$. Consider the $p^n$-th cyclotomic polynomial

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

By example sheet, we know that $\Phi_{p^n}(X)$ is irreducible in $\mathbb{Q}_p$ (hence the minimal polynomial of $\xi_{p^n}$), that $L/K$ is Galois, totally ramified of degree $p^{n-1}(p-1)$, that it has $\pi = \xi_{p^n} - 1$ to be a uniformiser (so $\mathcal{O}_L = \mathbb{Z}_p(\xi_{p^n})$) and that $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ via $\sigma_m \mapsto m$ where $\sigma_m : \xi_{p^n} \mapsto \xi_{p^n}^m$.
Let's compute its higher ramification groups. Note that we have $v_L(\sigma_m(\pi) - \pi) = v_L(\xi_{p^n}^{m-1} - 1)$. Let $k$ be the maximal such that $p^k \mid m - 1$, then $\xi_{p^n}^{m-1}$ is a primitive $p^{n-k}$-th root of unity and hence $\pi' = \xi_{p^n}^{m-1} - 1$ is a uniformiser in $L' = \mathbb{Q}_p(\xi_{p^n}^{m-1})$. Therefore

$$v_L(\xi_{p^n}^{m-1} - 1) = e_{L/L'} = \frac{e_{L/K}}{e_{L'/K}} = \frac{[L : K]}{[L' : K]} = \frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k$$

Therefore $\sigma_m \in G_i$ iff $p^k \geq i+1$, i.e.

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

Hey this looks like the quotients of unit groups!

# 6 Local Class Field Theory

## 6.1 Infinite Galois Theory

Let $L/K$ be an algebraic extension of fields.

**Definition 6.1.** $L/K$ is separable if for every $\alpha \in L$, the minimal polynomial of $\alpha$ in $K$ is separable. It is normal if the minimal polynomial of any $\alpha \in L$ splits completely in $L$. We say it is Galois if it is separable and normal. Write $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ in this case.

Recall that if $L/K$ is finite Galois, we have the correspondence bewteen subextensions $L/K'/K$ and subgroups of $\mathrm{Gal}(L/K)$ which is given by $K' \mapsto \mathrm{Gal}(L/K'), H \mapsto L^H$, We want to extend this to the infinite case, which requires the introduction of a topology on $\mathrm{Gal}(L/K)$. To do this, we need to generalise the notion of an inverse limit.

**Definition 6.2.** Let $(I, \leq)$ be a partially ordered set. $I$ is a directed set if for all $i, j \in I$, there is some $k \in I$ with $i \leq k, j \leq k$.

**Example 6.1.** Any totally ordered set is a directed set. $\mathbb{N}_{\geq 1}$ ordered by divisibility is also a directed set.

**Definition 6.3.** Let $(I, \leq)$ be a directed set. An inverse system $(G_i)_{i\in I}$ is a collection of groups $G_i$ together with a transition map $\phi_{ij} : G_j \to G_i$ for all $i \leq j$ such that $\phi_{ii} = \mathrm{id}_{G_i}$ and $\phi_{ik} = \phi_{ij}\phi_{jk}$ if $i \leq j \leq k$.
The inverse limit of the inverse system is

$$\varprojlim_{i\in I} G_i = \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i : \phi_{ij}(g_j) = g_i \right\}$$

*Remark.* 1. Taking $I$ to be $(\mathbb{N}, \leq)$ recovers our previous definition.
2. We also have natural projection maps $\phi_j : \varprojlim_{i\in I} G_i \to G_j$ for each $j$.

For $G_i$ finite, we can put a topology on $\varprojlim_{i\in I} G_i$ (the profinite topology) by taking the weakest topology making each projection map continuous.

**Proposition 6.1.** *Let $L/K$ be Galois, then $I = \{F \subset L : F/K$ finite Galois$\}$ is a directed set ordered under inclusion. For $F, F' \in I, F \subset F'$, there is a natural map $\mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$ by restriction, so we get an inverse system of groups $\{\mathrm{Gal}(F/K) : F \subset L, F/K$ finite Galois$\}$ indexed by $I$. Then the natural map from $\mathrm{Gal}(L/K)$ to the inverse limit of the system is an isomorphism.*

We endow $\mathrm{Gal}(L/K)$ with the profinite topology on the inverse limit. This is the discrete topology when $L/K$ is finite.

*Proof.* Example sheet. □

**Example 6.2.** Take $K = \mathbb{F}_q, L = \overline{\mathbb{F}}_q$. For each $n$, there is a unique extension $F/K$ of degree $n$, namely $F = \mathbb{F}_{q^n}$. We also know that $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ if and only if $m \mid n$.
We have $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ is generated by the Frobenius $\mathrm{Fr}_q : x \mapsto x^q$. So for $m \mid n$ the restriction map $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is just given by the projection $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Therefore $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. This group is also known as $\hat{\mathbb{Z}}$. It is also isomorphic to $\prod_{p \text{ prime}} \mathbb{Z}_p$.
The subgroup $\langle \mathrm{Fr}_q \rangle \subset \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ corresponds to the natural inclusion $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$.

**Theorem 6.2** (Fundamental Theorem of Galois Theory)**.** *Let $L/K$ be a Galois extension. Then there is a bijection between subextensions $F/K$ of $L/K$ and closed subgroups of $\mathrm{Gal}(L/K)$ given by $F \mapsto \mathrm{Gal}(L/F), H \mapsto L^H$. Moreover, $F/K$ is finite iff $\mathrm{Gal}(L/F)$ is open, and it is Galois iff $\mathrm{Gal}(L/F) \lhd \mathrm{Gal}(L/K)$, in which case $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.*

*Proof.* Example sheet. □

## 6.2 Weil Group

Let $K$ be a local field and $L/K$ is a separable algebraic (but not necessarily finite) extension.

**Definition 6.4.** $L/K$ is unramified (resp. totally ramified) if $F/K$ is unramified (resp. totally ramified) for any finite subextension $F/K$ of $L/K$.

**Proposition 6.3.** *Let $L/K$ be an unramified extension, then it is Galois and $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is an isomorphism of topological groups.*

*Proof.* Every finite subextension $F/K$ is unramified hence Galois, so $L/K$ is normal and separable, therefore Galois. The commutative diagram

$$\begin{array}{ccc}
\mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(k_L/k) \\
\cong\downarrow & & \downarrow\cong \\
\varprojlim_{L/F/K, F/K \text{ finite}} \mathrm{Gal}(F/K) & & \varprojlim_{k_L/k'/k, k'/k \text{ finite}} \mathrm{Gal}(k'/k) \\
\cong\downarrow & \swarrow\cong & \\
\varprojlim_{L/F/K, F/K \text{ finite}} \mathrm{Gal}(k_F/k) & &
\end{array}$$

gives the isomorphism. □

Suppose $L_1/K, L_2/K$ are finite unramified subextensions of $L/K$, then their compositum $L_1L_2/K$ is unramified by example sheet, so there exists a maximal unramified subextension $K_0/K$ in $L/K$. Suppose $L/K$ is Galois, then there is a restrction map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(K_0/K) \cong \mathrm{Gal}(k_L/k)$ which is surjective.

**Definition 6.5.** The inertia subgroup $I_{L/K}$ is the kernel of this restriction map.

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

**Definition 6.6.** Let $L/K$ be Galois. Then the Weil group $W(L/K)$ is a subgroup of $\mathrm{Gal}(L/K)$ which is the preimage of $\langle \mathrm{Fr}_{k_L/k} \rangle$ under the restriction map.

*Remark.* 1. In the case where $k_L/k$ is finite, we have $W(L/K) = \mathrm{Gal}(L/K)$. Otherwise, $W(L/K) \subsetneq \mathrm{Gal}(L/K)$.
2. We have the commutative diagram

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

with exact rows.

What should the topology on $W(L/K)$ be? We declare it to be the weakest topology such that it is a topological group and $I_{L/K}$, equipped with the topology inherited from $\mathrm{Gal}(L/K)$, is an open subgroup in $W(L/K)$. So open sets in $W(L/K)$ are supposed to be translations of open sets in $I_{L/K}$ by elements of $W(L/K)$.

*Remark.* When $k_L/k$ is infinite, this is not the same as (and is generally stronger than) the subspace topology inherited from $\mathrm{Gal}(L/K)$. Indeed, $I_{L/K}$ would not generally be open in $W(L/K)$ if we put the subspace topology on the latter.

**Proposition 6.4.** *Suppose $L/K$ is Galois, then:*
*(i) $W(L/K)$ is dense in $\mathrm{Gal}(L/K)$.*
*(ii) Suppose $F/K$ is a finite subextension of $L/K$, then we have $W(L/F) = W(L/K) \cap \mathrm{Gal}(L/F)$.*
*(iii) Suppose $F/K$ is a finite Galois subextention of $L/K$, then $W(L/F) \lhd W(L/K)$ and we have $W(L/K)/W(L/F) \cong \mathrm{Gal}(F/K)$.*

*Proof.* (i) This is equivalent to the statement that for any finite Galois subextensions $F/K$ of $L/K$, $W(L/K)$ intersects every coset of $\mathrm{Gal}(L/F)$. But this is just to say that $W(L/K)$ surjects into $\mathrm{Gal}(F/K)$ for finite Galois $F$. Let's look at the commutative diagram

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

Let $K_0$ be the maximal unramified subextension of $L/K$, then $K_0 \cap F$ is the maximal unramified subextension of $F/K$. Then $\mathrm{Gal}(L/K_0) \to \mathrm{Gal}(K_0F/K_0) \cong \mathrm{Gal}(F/(K_0 \cap F))$ is surjective. As $\mathrm{Gal}(k_F/k)$ is generated by $\mathrm{Fr}_{k_F/k}$, $c$ is surjective. Hence $b$ is surjective.
(ii) Consider the commutative diagram

$$\begin{array}{ccccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(k_L/k) & \hookleftarrow & \langle \mathrm{Fr}_{k_L/k} \rangle \\ \uparrow & & \uparrow & & \uparrow \\ \mathrm{Gal}(L/F) & \longrightarrow & \mathrm{Gal}(k_L/k_F) & \hookleftarrow & \langle \mathrm{Fr}_{k_L/k} \rangle \end{array}$$

from which the assertion is clear.
(iii) From (ii) we know that

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

which is isomorphic to $\mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K)$ by (i). □

## 6.3 Statements of Local Class Field Theory

Let $K$ be a local field.

**Definition 6.7.** An extension $L/K$ is abelian if it is Galois and $\mathrm{Gal}(L/K)$ is Galois.

**Proposition 6.5.** *If $L_1/K, L_2/K$ are abelian extensions, then:*
*(i) $L_1L_2/L$ is abelian.*
*(ii) If $L_1 \cap L_2 = K$, then there is a canonical isomorphism* $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Part (i) means that we have unique maximal abelian extension $K^{\mathrm{ab}}$ of $K$ in $K^{\mathrm{sep}}$, the separable closure of $K$.

**Example 6.3.** Let $K^{\mathrm{nr}}$ be the maximal unramified extension of $K$ in $K^{\mathrm{sep}}$. We know that $K^{\mathrm{nr}} = \bigcup_{m=1}^{\infty} K(\xi_{q^m-1})$ where $|k| = q$ and that $k_{K^{\mathrm{nr}}} = \bar{\mathbb{F}}_q$. As $\mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$. Hence $K^{\mathrm{nr}} \subset K^{\mathrm{ab}}$.

There is an exact sequence

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

where $\mathbb{Z} = \langle \mathrm{Fr}_{K^{\mathrm{nr}}/K} \rangle$ with $\mathrm{Fr}_{K^{\mathrm{nr}}/K} = \mathrm{Fr}_{k_{K^{\mathrm{nr}}}/k}$ the Frobenius element.

**Theorem 6.6.** *There exists a unique isomorphism* $\mathrm{Art}_K : K^\times \to W(K^{\mathrm{ab}}/K)$ *(the local Artin reciprocity) of topological groups such that:*
*(i)* $\mathrm{Art}_K(\pi)|_{K^{\mathrm{nr}}} = \mathrm{Fr}_{K^{\mathrm{nr}}/K}$ *for any uniformiser $\pi \in K$.*
*(ii) For each finite subextension $L/K$ of $K^{\mathrm{ab}}/K$,* $\mathrm{Art}_K(N_{L/K}(L^\times))|_L = \{1\}$.
*Moreover, for a finite abelian extension $L/K$,* $\mathrm{Art}_K$ *induces an isomorphism* $K^\times/N_{L/K}(L^\times) \cong W(K^{\mathrm{ab}}/K)/W(K^{\mathrm{ab}}/L) \cong \mathrm{Gal}(L/K)$.

*Remark.* 1. These are special cases of what's known as local Langlands correspondence.
2. There is a similar Artin reciprocity in global class field theory, which can be characterised using the local Artin reciprocity.

**Proposition 6.7.** *(i) (Existence theorem) For any open $H \leq K^\times$ of finite index, there is some finite abelian extension $L/K$ such that $N_{L/K}(L^\times) = H$. In particular,* $\mathrm{Art}_K$ *induces an inclusion-reversing isomorphism of partially order sets between the set of finite index open subgroups of $K^\times$ and finite abelian extensions $L/K$. More explicitly, the isomorphism is given by $H \mapsto (K^{\mathrm{ab}})^{\mathrm{Art}_K(H)}$ and $L/K \mapsto N_{L/K}(L^\times)$.*

*(ii) (Norm functoriality) Let $L/K$ be a finite separable extension, then there is a commutative diagram*

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

**Proposition 6.8.** *Suppose $L/K$ is a finite abelian extension of degree $n$, then $e_{L/K} = [\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$.*

*Proof.* For $x \in L^\times$, we have $v_K(N_{L/K}(x)) = f_{L/K} v_L(x)$ since $v_K = e v_L$. So $v_K$ induces a surjection $K^\times/N_{L/K}(L^\times) \to \mathbb{Z}/f_{L/K}\mathbb{Z}$ with kernel

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

But then $n = [K^\times : N_{L/K}(L^\times)] = f_{L/K}[\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$ by Theorem 6.6. □

**Corollary 6.9.** *A finite abelian extension $L/K$ is unramified if and only if $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$.*

## 6.4 Construction of Artin Reciprocity

Let's first construct $\mathrm{Art}_{\mathbb{Q}_p}$.
Recall that $\mathbb{Q}_p^{\mathrm{nr}} = \bigcup_{m=1}^\infty \mathbb{Q}_p(\xi_{p^m-1}) = \bigcup_{p\nmid m} \mathbb{Q}_p(\xi_m)$. On the other hand, $\mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$ with an isomorphism $\theta_n : \mathrm{Gal}(\mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. For $n \geq m \geq 1$, we have the diagram

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}_p(\xi_{p^m})/\mathbb{Q}_p) \\ {\scriptstyle \theta_n}\downarrow & & \downarrow{\scriptstyle \theta_m} \\ (\mathbb{Z}/p^n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p^m\mathbb{Z})^\times \end{array}$$

Set $\mathbb{Q}_p(\xi_{p^\infty}) = \bigcup_{n\geq 1} \mathbb{Q}_p(\xi_{p^n})$, then the diagram means that we have an isomorphism $\theta : \mathrm{Gal}(\mathbb{Q}_p(\xi_{p^\infty})/\mathbb{Q}_p) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$. Since $\mathbb{Q}_p(\xi_{p^\infty})$ is totally ramified but $\mathbb{Q}_p^{\mathrm{nr}}$ is unramified, we have $\mathbb{Q}_p(\xi_{p^\infty}) \cap \mathbb{Q}_p^{\mathrm{nr}} = \mathbb{Q}_p$ and therefore $\mathrm{Gal}(\mathbb{Q}_p(\xi_{p^\infty})\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\xi_{p^\infty})/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$.

**Theorem 6.10** (Local Kronecker-Weber Theorem)**.** $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{nr}}\mathbb{Q}_p(\xi_{p^\infty})$.

We can then construct $\mathrm{Art}_{\mathbb{Q}_p}$ as follows: As usual $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$ via $u\pi^n \mapsto (n, u)$. Then we set $\mathrm{Art}_{\mathbb{Q}_p}(p^n u) = ((\mathrm{Fr}_{\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p})^n, \theta^{-1}(u))$ (noting $\mathrm{Fr}_{\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p} \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\xi_{p^\infty})/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$).
How about the Artin map in general? Suppose $K$ is a local field with a chosen uniformiser $\pi$. For $n \geq 1$, we can construct $K_{\pi,n}$ which are totally ramified Galois extensions of $K$ such that $K_{\pi,n} \subset K_{\pi,n+1}$, such that for $n \geq m \geq 1$ we have a commutative diagram

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

with $\psi_i$ isomorphisms, and such that $K^{\mathrm{ab}} = K^{\mathrm{nr}} K_{\pi,\infty}$ where $K_{\pi,\infty} = \bigcup_n K_{\pi,n}$. Once these are constructed, we would have an isomorphism $\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \to \varprojlim_n \mathcal{O}_K/U_K^{(n)} \cong \mathcal{O}_K^\times$. We then define $\mathrm{Art}_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ by the formula $\pi^n u \mapsto ((\mathrm{Fr}_{K^{\mathrm{nr}}/K})^n, \psi^{-1}(u))$ where recall that we can make the identification $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K)$.

*Remark.* This looks like $\mathrm{Art}_K$ depends on $\pi$ but, trust me, a different choice of uniformiser would eventually give the same map.

The construction of these fields is (or can be) done by Lubin-Tate theory.

# 7 Lubin-Tate Theory

## 7.1 Formal Group Laws

Let $R$ be a ring and $R[[X_1, \ldots, X_n]]$ the formal power series ring in $n$ variables over $R$.

**Definition 7.1.** A (one-dimensional commutative) formal group law over $R$ is a power series $F(X, Y) \in R[[X, Y]]$ satisfying:
1. $F(X, Y) \equiv X + Y$ modulo terms of degree at least 2.
2. $F(F(X, Y), Z) = F(X, F(Y, Z))$.
3. $F(X, Y) = F(Y, X)$.

**Example 7.1.** $\hat{\mathbb{G}}_a(X, Y) = X + Y$ is a formal group law, and is usually called the formal additive group. $\hat{\mathbb{G}}_m(X, Y) = X + Y + XY$ is also a formal group law, and is called the formal multiplicative group.

**Lemma 7.1.** *Let $F$ be a formal group law over $R$. Then $F(X, 0) = X$ and $F(0, Y) = Y$. Furthermore, there is a unique power series $i(X) \in XR[[X]]$ such that $F(X, i(X)) = 0$.*

*Proof.* Example sheet. □

Suppose $K$ is a complete non-Archimedean valued field and $F$ is a formal group law over $\mathcal{O}_K$, then $F(x, y)$ converges for all $x, y \in \mathfrak{m}_K$ to an element in $\mathfrak{m}_K$. The operation $x \cdot_F y = F(x, y)$ turns $\mathfrak{m}_K$ into a group.

**Example 7.2.** On $\mathbb{Q}_p$, $x \cdot_{\hat{\mathbb{G}}_m} y = x + y + xy$ gives a group structure on $p\mathbb{Z}_p$, and we have an isomorphism $(p\mathbb{Z}_p, \cdot_{\hat{\mathbb{G}}_m}) \cong (1 + p\mathbb{Z}_p, \times), x \mapsto 1 + x$.

**Definition 7.2.** A homomorphism of formal group laws $F, G$ over $R$ is an element $f(X) \in XR[[X]]$ such that $f(F(X, Y)) = G(f(X), f(Y))$.

$f(X) = X$ is a homomorphism $F \to F$, which we'll take as the identity. We can also compose homomorphisms, so we define an isomorphism to be a homomorphism with a two-sided inverse. We write $\mathrm{End}_R(F)$ to be the set of homomorphisms $F \to F$.

**Proposition 7.2.** *Let $R$ be a $\mathbb{Q}$-algebra. There is an isomorphism of formal group laws $\exp : \hat{\mathbb{G}}_a \to \hat{\mathbb{G}}_m$ given by*

$$\exp(X) = \sum_{n=1}^{\infty} \frac{1}{n!} X^n$$

*(and yes, the sum does start from $n = 1$).*

*Proof.* Define

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

Ehhh let's say it's not hard to verify that $\exp(\log(X)) = \log(\exp(X)) = X$ and $\exp(\hat{\mathbb{G}}_a(X,Y)) = \hat{\mathbb{G}}_m(\exp(X), \exp(Y))$. □

**Lemma 7.3.** *$\mathrm{End}_R(F)$ is a (noncommutative) ring with addition given by $(f +_F g)(X) = F(f(X), g(X))$ and multiplication given by composition.*

*Proof.* Just checking. Let's do some of them, say that $+_F$ is well-defined. The rest are exercises. Suppose $f, g \in \mathrm{End}_R(F)$. Then

$$\begin{aligned}
(f +_F g) \circ F(X,Y) &= F(f(F(X,Y)), g(F(X,Y))) \\
&= F(F(f(X), f(Y)), F(g(X), g(Y))) \\
&= F(F(f(X), g(X)), F(f(Y), g(Y))) \\
&= F((f +_F g)(X), (f +_F g)(Y))
\end{aligned}$$

□

## 7.2 Lubin-Tate Formal Groups

Suppose $K$ is a non-Archimedean local field and $|k| = q$.

**Definition 7.3.** A formal $\mathcal{O}_K$-module is a formal group law $F$ over $\mathcal{O}_K$ together with a ring homomorphism $[-]_F : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$, such that for all $a \in \mathcal{O}_K$, $[a]_F(X) \equiv aX \pmod{X^2}$.
A homomorphism of formal $\mathcal{O}_K$-modules $F, G$ is a homomorphism of formal group laws $F \to G$ such that $f \circ [a]_F = [a]_G \circ f$ for all $a \in \mathcal{O}_K$.

**Definition 7.4.** Let $\pi \in \mathcal{O}_K$ be a uniformiser. A Lubin-Tate series for $\pi$ is a power series $f(X) \in \mathcal{O}_K[[X]]$ such that:
(a) $f(X) \equiv \pi X \pmod{X^2}$.
(b) $f(X) \equiv X^q \pmod{\pi}$.

**Example 7.3.** On $K = \mathbb{Q}_p$, $f(X) = (X+1)^p - 1$ is a Lubin-Tate series for $\pi$.

**Theorem 7.4.** *Let $f(X)$ be a Lubin-Tate series for $\pi$. Then:*
*(i) There is a unique formal group law $F_f$ over $\mathcal{O}_K$ such that $f \in \mathrm{End}_{\mathcal{O}_K}(F_f)$.*
*(ii) There is a ring homomorphism $[-]_f : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F_f)$ which makes $F_f$ a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$.*
*(iii) If $g(X)$ is another Lubin-Tate series for $\pi$, then $F_f \cong F_g$ as formal $\mathcal{O}_K$-modules.*

**Definition 7.5.** $F_f$ is the Lubin-Tate formal group for $\pi$.

**Example 7.4.** On $K = \mathbb{Q}_p$, the Lubin-Tate formal group for $f(X) = (X+1)^p - 1$ is simply $\hat{\mathbb{G}}_m$. Indeed, $f(\hat{\mathbb{G}}_m(X,Y)) = (1+X)^p(1+Y)^p - 1 = \hat{\mathbb{G}}_m(f(X), f(Y))$.

**Lemma 7.5.** *Let $f, g$ be Lubin-Tate series for $\pi$ and take a homogenous linear form $L(X_1, \ldots, X_n) = \sum_{i=1}^n a_i X_i, a_i \in \mathcal{O}_K$. Then there is a unique power series $F(X_1, \ldots, X_n) \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ such that:*
*(i) $F(X_1, \ldots, X_n) \equiv L(X_1, \ldots, X_n)$ modulo terms of degree at least 2.*
*(ii) $f(F(X_1, \ldots, X_n)) = F(g(X_1), \ldots, g(X_n))$.*

*Proof.* We'll show by induction that there exists unique polynomials $F_m \in \mathcal{O}_K[X_1, \ldots, X_m]$ of total degree at most $m$ such that:
(a) $f(F_m(X_1, \ldots, X_n)) \equiv F_m(g(X_1), \ldots, g(X_n))$ modulo terms of degree at least $m+1$.
(b) $F_m(X_1, \ldots, X_n) \equiv L(X_1, \ldots, X_n)$ modulo terms of degree at least 2.
(c) $F_m \equiv F_{m+1}$ modulo terms of degree at least $m+1$.
For $m = 1$, we can just take $F_1 = L$. (b) is immediate, (c) is vacuous and (a) follows from the fact that $f(X), g(X) \cong \pi X$ modulo $X^2$.
Suppose we've constructed $F_1, \ldots, F_m$, we set $F_{m+1} = F_m + h$ for some $h$ homogenous of degree $m+1$ which is to be determined. Again (b) and (c) are clear. For (a), since $f(X+Y) = f(X) + f'(X)Y \pmod{Y^2}$ and $f'(X) \equiv \pi \pmod{X}$, we have $f \circ (F_m + h) \equiv f \circ F_m + \pi h$ modulo terms of degree at least $m+2$. Similarly, since $g(X) \equiv \pi X \pmod{X^2}$, $(F_m + h) \circ g \equiv F_m \circ g + h(\pi X_1, \ldots, \pi X_n) \equiv F_m \circ g + \pi^{m+1} h(X_1, \ldots, X_n)$ modulo terms of degree at least $m+2$.
So what we need is $f \circ F_m - F_m \circ g \equiv (\pi - \pi^{m+1})h$ modulo terms of degree at least $m+2$. But $f(X), g(X) \equiv X^q \pmod{\pi}$, so

$$f \circ F_m - F_m \circ g \equiv F_m(X_1, \ldots, X_n)^q - F_m(X_1^q, \ldots, X_n^q) \equiv 0 \mod \pi$$

In other words, $f \circ F_m - F_m \circ g \in \pi \mathcal{O}_K[X_1, \ldots, X_n]$. So we have no choice but to take $h = \pi^{-1}(1 - \pi^m)^{-1} r \in \mathcal{O}_K[X_1, \ldots, X_n]$ where $r(X_1, \ldots, X_n)$ is the degree $m+1$ term in $f \circ F_m - F_m \circ g$, which works by our computation.
We then just take $F \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ to be the limit of $F_m$, which exists by (c). This satisfies the required property by construction, and has to be unique due to the uniqueness of $F_m$'s. □

*Proof of Theorem 7.4.* (i) By the lemma, there exists a unique power series $F_f \in \mathcal{O}_K[[X, Y]]$ such that $F(X, Y) \equiv X + Y$ modulo terms of degree at least 2 and $f(F_f(X, Y)) = F_f(f(X), f(Y))$.
So it suffices to show that $F_f$ is a formal group law. This follows from the uniqueness part of the lemma. For example, to show associativity, we do the following: $F_f(X, F_f(Y, Z)) \equiv X + Y + Z \equiv F_f(F_f(X, Y), Z)$ modulo terms of degree at least 2. Moreover, $f \circ F_f(X, F_f(Y, Z)) = F_f(f(X), f(F_f(Y, Z))) = F_f(f(X), F_f(f(Y), f(Z)))$ and $f \circ F_f(F_f(X, Y), Z) = F_f(f \circ F_f(X, Y), f(Z)) = F_f(F_f(f(X), f(Y)), f(Z))$. So by the uniqueness part of the lemma we must have $F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$.
Commutativity follows from the same process, and is left as exercise.
(ii) We know again from the lemma that there is a unique power series $[a]_f \in \mathcal{O}_K[X]$ such that $[a]_f \equiv aX \pmod{X^2}$ and $f \circ [a]_f = [a]_f \circ f$. We also know $[a]_f \circ F_f = F_f \circ [a]_f$ by uniqueness, same for checking everything that needs to be checked.
(iii) Suppose $g$ is another Lubin-Tate series. Let $\theta(X) \in \mathcal{O}_K[[X]]$ be the unique power series such that $\theta(X) \equiv X \mod X^2$ and $\theta \circ f = g \circ \theta$. Then $\theta \circ F_f = F_g \circ \theta$ by uniqueness, so $\theta$ is a member of $\mathrm{Hom}_{\mathcal{O}_K}(F_f, F_g)$. Reversing the roles of $f, g$ gives an inverse. □

## 7.3 Lubin-Tate Extensions

Let $K$ be a non-Archimedean local field with $|k| = q$ and uniformiser $\pi$. Let $\bar{K}$ be an algebraic closure of $K$ and $\bar{\mathfrak{m}} \leq \mathcal{O}_{\bar{K}}$ the maximal ideal.

**Lemma 7.6.** *Let $F$ be a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$, then $\bar{\mathfrak{m}}$ becomes an (actual) $\mathcal{O}_K$-module with $x +_F y = F(x, y), a \cdot_F x = [a]_F(x)$.*

*Proof.* Sadly $\bar{K}$ is not complete, so we can't apply convergence arguments directly. But there is an easy fix: For any $x \in \bar{\mathfrak{m}}$, we have $x \in \mathfrak{m}_L$ for some $L/K$ finite. Since $[a]_F \in \mathcal{O}_K[[X]]$, $[a]_F(x)$ converges in $L$ to something in $\mathfrak{m}_L \subset \bar{\mathfrak{m}}$. Similarly addition is well-defined and they are by definition compatible enough to give $\bar{\mathfrak{m}}$ the structure of an $\mathcal{O}_{\bar{K}}$-module. □

**Definition 7.6.** Suppose $f$ is a Lubin-Tate series and $F_f$ is the Lubin-Tate formal group law associated to it. The $\pi^n$-torsion group is $\mu_{f,n} = \{x \in \bar{\mathfrak{m}} : \pi^n \cdot_{F_f} x = 0\} = \{x \in \bar{\mathfrak{m}} : f_n(x) = f \circ \cdots \circ f(x) = 0\}$.

It's clear that $\mu_{f,n}$ is an $\mathcal{O}_K$-module and that $\mu_{f,n} \subset \mu_{f,n+1}$.

**Example 7.5.** For $K = \mathbb{Q}_p$, we can take $f(X) = (X + 1)^p - 1$. Then $[p^n]_{F_f}(X) = f \circ \cdots \circ f(X) = (X+1)^{p^n} - 1$, so $\mu_{f,n} = \{\xi^i_{p^n} - 1 : i = 0, 1, \ldots, p^n - 1\}$. Hey these are uniformisers in a certain field extension!

Now let $f(X) = \pi X + X^q$ which is certainly a Lubin-Tate series for $\pi$. Then $f_n(X) = f \circ \cdots \circ f(X) = f_{n-1}(X)(\pi + f_{n-1}(X)^{q-1})$. Set $h_n(X) = f_n(X)/f_{n-1}(X) = \pi + f_{n-1}(X)^{q-1}$.

**Proposition 7.7.** *$h_n$ is always separable, Eisenstein and has degree $q^{n-1}(q-1)$.*

*Proof.* It's clear that $h_n(X)$ is monic of degree $q^{n-1}(q-1)$. Since $f(X) \equiv X^q \pmod{\pi}$, we have $f_{n-1}(X)^{q-1} \equiv X^{q^{n-1}(q-1)} \pmod{\pi}$. As $f_{n-1}(X)$ has constant term 0, $h_n(X) = \pi + f_{n-1}(X)^{q-1}$ must be Eisenstein.
Since $h_n(X)$ is irreducible, it is separable if $\operatorname{char} K = 0$. Otherwise $\operatorname{char} K = p$ and we need only to show that $h_n' \neq 0$.
$h_1(X) = \pi + X^{q-1}$ is certainly separable. Suppose $h_{n-1}, \ldots, h_1$ are separable, then $f_{n-1} = h_{n-1} \cdots h_1$ is also separable since $h_i$'s are irreducible polynomials of distinct degrees. Therefore $h_n(X) = \pi + f_{n-1}(X)^{q-1}$ has derivative $h_n'(X) = (q-1)f_{n-1}'(X)f_{n-1}(X)^{q-2} \neq 0$. □

**Proposition 7.8.** *(i) $\mu_{f,n}$ is a free module of rank 1 over $\mathcal{O}_K/\pi^n\mathcal{O}_K$.*
*(ii) If $g$ is another Lubin-Tate series for $\pi$, then we have an isomorphism $\mu_{f,n} \cong \mu_{g,n}$ of $\mathcal{O}_K$-modules and $K(\mu_{f,n}) = K(\mu_{g,n})$.*

*Proof.* (i) Let $\alpha \in \bar{K}$ be a root of $h_n(X)$. Since $h_n(X)$ and $f_{n-1}(X)$ are coprime, we have $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$. The map $\tilde{\phi} : \mathcal{O}_K \to \mu_{f,n}, a \mapsto a \cdot_{F_f} \alpha$ is a homomorphism of $\mathcal{O}_K$-modules with $\pi^n\mathcal{O}_K \leq \ker \tilde{\phi}$ (since $\alpha \in \mu_{f,n}$). As $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$, $\pi^{n-1} \cdot_{F_f} \alpha \neq 0$, so in fact $\pi^n\mathcal{O}_K = \ker \tilde{\phi}$. We therefore get an injection $\phi : \mathcal{O}_K/\pi^n\mathcal{O}_K \to \mu_{f,n}$. Since $f_n$ is separable, $|\mu_{f,n}| = \deg f_n = q^n = |\mathcal{O}_K/\pi^n\mathcal{O}_K|$, so $\phi$ can only be an isomorphism.
(ii) Let $\theta : F_f \to F_g$ be the isomorphism of formal $\mathcal{O}_K$-modules as in Theorem 7.4(iii). Then $\theta$ also gives rise to an isomorphism $\theta : (\bar{\mathfrak{m}}, +_{F_f}, \cdot_{F_g}) \to (\bar{\mathfrak{m}}, +_{F_g}, \cdot_{F_g})$ of $\mathcal{O}_K$-modules, which restrict to an isomorphism $\mu_{f,n} \cong \mu_{g,n}$.
Furthermore, since $\mu_{f,n}$ is algebraic, $K(\mu_{f,n})/K$ is finite hence complete. But $\theta(X) \in \mathcal{O}_K[[X]]$, so for any $x \in \mu_{f,n}$ we have $\theta(x) \in K(\mu_{f,n})$. So $K(\mu_{g,n}) \subset K(\mu_{f,n})$. Reversing the roles of $f, g$ gives the converse. □

**Definition 7.7.** Set $K_{\pi,n} = K(\mu_{f,n})$ for any Lubin-Tate series $f$.

*Remark.* $K_{\pi,n}$ does not depend on the choice of $f$ by the preceding proposition. We also have $K_{\pi,n} \subset K_{\pi,n+1}$.

We'll show that they also have the properties predicted in §6.4.

**Proposition 7.9.** *$K_{\pi,n}/K$ is a totally ramified Galois extension of degree $q^{n-1}(q-1)$.*

*Proof.* Choose the Lubin-Tate series $f(X) = \pi X + X^q$.
$K_{\pi,n}/K$ is Galois since $K_{\pi,n} = K(\mu_{f,n})$ is the splitting field fo $f_n(X)$ over $K$. Let $\alpha$ be a root of $h_n(X) = f_n(X)/f_{n-1}(X)$. It suffices to show that $K(\alpha) = K_{\pi,n}$, since $\alpha$ is a root of an Eisenstein polynomial of degree $q^{n-1}(q-1)$. It's certainly true that $K(\alpha) \subset K_{\pi,n}$. Conversely, the preceding proposition shows that every element $x \in \mu_{f,n}$ can be written in the for $a \cdot_{F_f} \alpha$ for some $a \in \mathcal{O}_K$ (as $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$). So $x \in [a]_{F_f}(\alpha) \in K(\alpha)$. □

**Theorem 7.10.** *There are isomorphisms $\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ determined by $\psi_n(\sigma) \cdot_{F_f} x = \sigma(x)$ for all $x \in \mu_{f,n}, \sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. Moreover, $\psi_n$ does not depend on $f$.*

*Proof.* Let $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. Then $\sigma$ preserves $\mu_{f,n}$ and acts continuously on $K(\mu_{f,n}) = K_{\pi,n}$.
To construct $\psi_n$, let's take the Lubin-Tate series to be $f(X) = \pi X + X^q$ 'coz why not. Since $F_f(X,Y) \in \mathcal{O}_K[[X,Y]]$ and $[a]_{F_f} \in \mathcal{O}_K[[X]]$ for all $a \in \mathcal{O}_K$, we know that $\sigma(x +_{F_f} y) = \sigma(x) +_{F_f} \sigma(y)$ for all $x, y \in \mu_{f,n}$ and $\sigma(a \cdot_{F_f} x) = a \cdot_{F_f} \sigma(x)$. Thus $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n})$, so it induces a group homomorphism $\mathrm{Gal}(K_{\pi,n}/K) \to \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n})$ which is injective since $K_{\pi,n} = K(\mu_{f,n})$.
Since $\mu_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$ as $\mathcal{O}_K$-modules, we have

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

We obtain an injection $\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \to (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ defined by sending $\sigma$ to the unique element of $\psi_n(\sigma) \in (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ such that $\psi_n(\sigma) \cdot_{F_f} x = \sigma(x)$ for all $x \in \mu_{f,n}$. $\psi_n$ is surjective since $[K_{\pi,n} : K] = q^{n-1}(q-1) = |(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times|$.
For uniqueness, suppose $g$ is another Lubin-Tate series and we obtain $\psi'_n : \mathrm{Gal}(K_{\pi,n}/K) \to (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$. Let $\theta : F_f \to F_g$ be an isomorphism of formal $\mathcal{O}_K$-modules given in Theorem 7.4. It then induces an isomorphism $\mu_{f,n} \to \mu_{g,n}$ of $\mathcal{O}_K$-modules. Hence for any $x \in \mu_{f,n}$, we have $\theta(\psi_n(\sigma) \cdot_{F_f} x) = \psi_n(\sigma) \cdot_{F_g} \theta(x)$. On the other hand, since $\theta \in \mathcal{O}_K[[X]]$, we have $\theta(\sigma(x)) = \sigma(\theta(x))$ for all $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. So $\theta(\psi_n(\sigma) \cdot_{F_f} x) = \theta(\sigma(x)) = \sigma(\theta(x)) = \psi'_n(\sigma) \cdot_{F_g} \theta(x)$. This means that we must have $\psi_n(\sigma) = \psi'_n(\sigma)$. □

Let's construct Artin reciprocity with these maps, following §6.4. Start by setting $K_{\pi,\infty} = \bigcup_{n \geq 1} K_{\pi,n}$ and $\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \to \varprojlim_n (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times$ the isomorphism induced by $\psi_n$'s.

**Theorem 7.11** (Generalised Kronecker-Weber)**.** $K^{\mathrm{ab}} = K_{\pi,\infty}K^{\mathrm{nr}}$.

We then define $\mathrm{Art}_K$ by sending $\pi^n u \in K^\times$ to

$$(\mathrm{Fr}^n_{K^{\mathrm{nr}}/K}, \psi^{-1}(u)) \in \mathrm{Gal}(K^{\mathrm{nr}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

and its image equals $W(K^{\mathrm{ab}}/K)$.

*Remark.* This is independent of the choice of $\pi$.

# 8 Upper Numbering of Ramification Groups

Let $L/K$ be a finite Galois extension of non-Archimedean local fields. Consider the following function

$$\phi = \phi_{L/K} : \mathbb{R}_{\geq -1} \to \mathbb{R}, s \mapsto \int_0^s \frac{\mathrm{d}t}{[G_0 : G_t]}$$

with the convention $[G_0 : G_t]^{-1} = [G_t : G_0]$ for $t \in [-1, 0)$. For $m \in \mathbb{Z}_{\geq -1}$ and $m \leq s < m + 1$, we have

$$\phi(s) = \begin{cases} s[G_{-1} : G_0] & \text{for } m = -1 \\ (\#G_0)^{-1}(\#G_1 + \cdots + \#G_m + (s - m)\#G_{m+1}) & \text{for } m \geq 0 \end{cases}$$

In particular, $\phi$ is continuous, piecewise linear and strictly increasing. So we can define $\psi = \psi_{L/K}$ to be the inverse of $\phi_{L/K}$.

**Definition 8.1** (Upper Numbering)**.** The higher ramification groups in the upper numbering is defined by $G^s(L/K) = G_{\psi(s)}(L/K) \subset \mathrm{Gal}(L/K)$ for $s \in \mathbb{R}_{\geq -1}$.

The point is that while $G_s$ behaves well with subgroups, $G^s$ is excellent with quotients: If $F/K$ is a subextension, then $G_s(L/F) = G_s(L/K) \cap \mathrm{Gal}(L/F)$. On the other hand, if $F/K$ is also Galois, then $G^t(L/K)\,\mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/F) = G^t(F/K)$ (Herbrand's theorem). This is helpful, for example, when one tries to define higher ramification groups for infinite Galois extensions.

**Example 8.1.** Take $K = \mathbb{Q}_p, L = \mathbb{Q}_p(\xi_{p^n})$. Let $k \in \mathbb{Z}, 1 \leq k \leq n - 1$. For $p^{k-1} - 1 < s \leq p^k - 1$, we have $G_s \cong \{m \in (\mathbb{Z}/p^n\mathbb{Z})^\times : m \equiv 1 \pmod{p^k}\} \cong U^{(k)}/U^{(n)}$. $G_s$ jumps at $p^k - 1$ and $\phi_{L/K}$ is linear on $[p^{k-1} - 1, p^k - 1]$. Thus to compute $\phi_{L/K}$ it suffices to compute $\phi_{L/K}(p^k - 1)$.
We have $\phi_{L/K}(p^k - 1) = (p-1)(p-1)^{-1} + (p^2 - 1 - (p-1))(p(p-1))^{-1} + \cdots = k$ for $1 \leq k \leq n - 1$. So

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

In particular, $G^k \cong U^{(k)}/U^{(n)}$.