Local Fields *

Artie Khovanov

Compiled on May 30, 2023

These are some notes for the Cambridge Mathematical Tripos Part III course *Local Fields* in Michaelmas 2022. This is NOT a verbatim copy of the lectured material: I've edited the content to help me understand it. As a result, any errors are mine alone.

I'm actively maintaining these notes. If you want to report typos or mistakes, please email aik31@cam.ac.uk or message me on Discord at `FM22#2007`.

Contents

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

1 Basic Theory

We want to find integer solutions to Diophantine equations

$$f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n].$$

This is hard, so we also study congruences: solutions modulo $p, p^2, \ldots$ Local fields package this information together.

1.1 Absolute value

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

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

(ii) $|xy| = |x||y|$

(iii) $|x + y| \leq |x| + |y|$ (**triangle inequality**)

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

Examples 1.2.

1. $K = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ with the usual absolute value $|a + ib| = \sqrt{a^2 + b^2}$. We write $|\cdot|_\infty$ for this absolute value.
2. Let K be any field. The **trivial absolute value** on K is
$$|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}.$$
Note that $x^n = 1 \implies |x| = 1$, so the only absolute value on a finite field is the trivial absolute value.
3. Take $K = \mathbb{Q}$ and let p be a prime. For $0 \neq x \in \mathbb{Q}$, write $x = p^n \frac{a}{b}$ where $n \in \mathbb{Z}$, and a and b are both coprime to p. Then set
$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{if } x = p^n \frac{a}{b} \end{cases}.$$

This is indeed an absolute value. Indeed, axiom (i) is trivial, and (ii) holds as a product of numbers coprime to p is coprime to p. For (iii), have $y = p^m \frac{c}{d}$ with (wlog) $m \geq n$; then

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

This is in fact stronger than the triangle inequality.

An absolute value $|\cdot|$ on K induces a metric $d(x,y) = |x-y|$ on K, which in turn induces a topology on K.

Note that, by the same proofs as in the real case, limits with respect to this topology commute with field operations; in particular, polynomials are continuous. This makes $(K, |\cdot|)$ into a topological field, and $K^\times$ into a topological group.

Definition 1.3. Let $|\cdot|$ and $|\cdot|'$ be two absolute values on a field K. These are **equivalent** if they induce the same topology on K. An equivalence class of absolute values on K is called a **place**.

From now on, all absolute values are nontrivial unless otherwise stated.

Proposition 1.4. *Let $|\cdot|$ and $|\cdot|'$ be two (nontrivial) absolute values on a field K. TFAE:*

1. *$|\cdot|$ and $|\cdot|'$ are equivalent.*
2. *$|x| < 1 \iff |x|' < 1$ for all $x \in K$.*
3. *$\exists c \in \mathbb{R}$ such that, for all $x \in K$, $|x|' = |x|^c$.*

The last condition implies that the absolute value of a place is determined up to a uniform exponential factor.

Proof.
(1) $\implies$ (2): $|x| < 1 \iff x^n \to_{|\cdot|} 0 \iff x^n \to_{|\cdot|'} 0 \iff |x|' < 1$. Here $\to_{|\cdot|}$ means that the limit is with respect to the topology of $|\cdot|$.

(2) $\implies$ (3): Fix $a \in K^\times$ such that $|a| > 1$ (exists since $|\cdot|$ is nontrivial). It suffices to show that, for all $x \in K^\times$, $\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}$. Suppose FAC (wlog) that, for some x, $\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}$. Then there are $m, n \in \mathbb{N}$ such that

$$\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}.$$

But then $n\log|x| < m\log|a|$ and $n\log|x|' > m\log|a|'$. Exponentiating, have $\left|\frac{x^n}{a^m}\right| < 1$, but $\left|\frac{x^n}{a^m}\right|' > 1$.#

(3) $\implies$ (1): Clear. □

Note that, by our definition, $|\cdot|_\infty^2$ on $\mathbb{C}$ is not an absolute value. Some authors replace the triangle inequality with $|x+y|^\beta \leq |x|^\beta + |y|^\beta$ (for β fixed) in order to allow such functions. By the last theorem, the resulting theory is the same.

Definition 1.5. An absolute value $|\cdot|$ on K is **non-Archimedean** if it satisfies the **ultrametric inequality** $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$. Otherwise, $|\cdot|$ is **Archimedean**. We sometimes call K itself (non-)Archimedean when $|\cdot|$ is understood.

This course mainly deals with non-Archimedean absolute values.

Example 1.6. $|\cdot|_\infty$ on $\mathbb{Q}$ is Archimedean, but $|\cdot|_p$ is non-Archimedean.

Lemma 1.7. *Let $|\cdot|$ be a non-Archimedean absolute value on K, and let $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$.*

Proof.

$$|x - y| \leq \max\{|x|, |-y|\} = |y| \text{ (as } |-y| = y)$$
$$|y| \leq \max\{|x|, |x-y|\} = |x-y| \text{ (otherwise } |y| \leq |x|_\#)$$

□

Geometrically, this shows that all triangles are isosceles in non-Archimedean fields.

Convergence is easier to check in a non-Archimedean field:

Proposition 1.8. *Let $(K, |\cdot|)$ be non-Archimedean, and let (x_n) be a sequence in K. If $|x_n - x_{n+1}| \to 0$, then (x_n) is Cauchy. In particular, if K is complete with respect to $|\cdot|$, then (x_n) converges.*

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

$$|x_n - x_m| = |(x_n - x_{n+1}) + (x_{n+1} - x_{n+2}) + \cdots + (x_{m-1} - x_m)| < \varepsilon$$

by the ultrametric inequality, so (x_n) is Cauchy. □

Example 1.9. Take $p = 5$. We will construct a sequence (x_n) such that

(i) $x_n^2 + 1 \equiv 0 \bmod 5^n$

(ii) $x_n = x_{n+1} \bmod 5^n$

Indeed, take $x_1 = 2$, and suppose we have constructed x_n. Let $x_n^2 + 1 = a5^n$, and set $x_{n+1} = x_n + b5^n$. Then

$$x_{n+1}^2 + 1 = a5^n + 2bx_n5^n + b^2 5^{2n}$$

so it suffices to choose b satisfying $a + 2bx_n \equiv 0 \bmod 5$. This is possible since $x_n \not\equiv 0$ by construction, so we have shown that such a sequence exists.

By condition (ii), (x_n) is Cauchy wrt $|\cdot|_5$. Suppose $x_n \to l \in \mathbb{Q}$; then $x_n^2 \to l^2$. But, by condition (i), $x_n^2 \to -1$, so $l^2 = -1$.$_\#$

Therefore $\mathbb{Q}$ is not complete with respect to $|\cdot|_5$.

Let $(K, |\cdot|)$ be a valued field. Recall that we can construct completions of metric spaces using equivalence classes of Cauchy sequences. We can therefore construct the **completion** $\hat{K}$ of K with respect to (the metric induced by) $|\cdot|$.

In fact, the metric space $\hat{K}$ is a field equipped with a natural absolute value (usually also written $|\cdot|$) extending $|\cdot|$ on K; it is given by

$$|(x_n)| = \lim_{n\to\infty} |x_n|.$$

Example 1.10. $\mathbb{R}$ (equipped with $|\cdot|_\infty$) is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$.

Definition 1.11. The valued field of **p-adic numbers** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Let $(K, |\cdot|)$ be a non-Archimedean valued field. For $x \in K$ and $r \in \mathbb{R}_+$, write $B(x,r)$ and $\overline{B}(x,r)$ for the open and closed balls of radius r about x in the metric induced by $|\cdot|$. These violate our geometric intuition:

Lemma 1.12.

(i) Open balls don't have centres: if $z \in B(x,r)$, then $B(z,r) = B(x,r)$.

(ii) Closed balls also don't have centres: if $z \in \overline{B}(x,r)$, then $\overline{B}(z,r) = \overline{B}(x,r)$.

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

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

Proof.
(i): Let $y \in B(x,r)$. Then $|x-y| < r$, so $|z-y| \leq \max\{|z-x|, |x-y|\} < r$. Hence $B(x,r) \subseteq B(z,r)$; by symmetry, $B(x,r) = B(z,r)$.

(ii): Same as (i).

(iii): Let $y \notin B(x,r)$. If $z \in B(x,r) \cap B(y,r)$, then, by (i), $B(x,r) = B(z,r) = B(y,r)$.$_\#$ Thus $B(x,r)$ and $B(y,r)$ are disjoint, so the complement of $B(x,r)$ is open.

(iv): Let $z \in \overline{B}(x,r)$; then $z \in B(z,r) = B(x,r)$ by (ii). □

1.2 Valuation rings

Definition 1.13. Let K be a field. A **valuation** on K is a function $v : K^\times \to \mathbb{R}$ satisfying

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

(ii) $v(x+y) \geq \min\{v(x), v(y)\}$

Valuations correspond to non-Archimedean places. Indeed, fix $0 < \alpha < 1$; a valuation v on K then induces a non-Archimedean absolute value on K given by $|x| = \alpha^{v(x)}$ (with $|0| = 0$). Conversely, a non-Archimedean absolute value $|\cdot|$ on K yields a valuation $v(x) = \log_\alpha |x|$.

Reusing the language of absolute values, we ignore the **trivial valuation** $v(x) = 0$, and say valuations v, w are **equivalent** if there is some $c \in \mathbb{R}_+$ such that $v(x) = c \cdot w(x)$ for all $x \in K^\times$.

Example 1.14.

1. Let $K = \mathbb{Q}$; $v_p(x) = -\log_p |x|_p$ is the **p-adic valuation**. If $x = p^n \frac{a}{b}$ with a, b, coprime to p (as before), $v_p(x) = n$.
2. Let $K = k(\!(t)\!) \coloneqq \operatorname{Frac} k[\![t]\!]$ be the field of formal Laurent series over a field k. Its **t-adic valuation** is given by

$$v\left(\sum_i a_i t^i\right) = \min\{i \mid a_i \neq 0\}$$

This is in fact the completion of the previous example (coefficients in $\mathbb{F}_p$, series in p).

Definition 1.15. Let $(K, |\cdot|)$ be a non-Archimedean valued field, with valuation v. The **valuation ring** $\mathcal{O}_K$ of K is

$$\mathcal{O}_K = \{x \in K \mid |x| \leq 1\} = \overline{B}(0,1) = \{0\} \cup \{x \in K^\times \mid v(x) \geq 0\}.$$

Proposition 1.16.

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

Proof.
(i): $|0| = 0$ and $|1| = 1$, so $0, 1 \in \mathcal{O}_K$. Closed balls are open by previous proposition. Closure is an easy check.

(ii): Easy checks.

(iii): $|x| = 1 \iff |x^{-1}| = |x|^{-1} = 1$, so $|x| = 1 \iff x, x^{-1} \in \mathcal{O}_K$. □

Definition 1.17. Let $\mathfrak{m} = \{x \in \mathcal{O}_K \mid |x| < 1\} \trianglelefteq \mathcal{O}_K$; then $k = \mathcal{O}_K/\mathfrak{m}$ is the **residue field** of K with respect to $|\cdot|$.

Observe that $\mathfrak{m}$ is a maximal ideal in $\mathcal{O}_K$. In fact, it is the only one:

Corollary 1.18. *$\mathcal{O}_K$ is a local ring with (unique) maximal ideal $\mathfrak{m}$.*

Proof. $\mathcal{O}_K \setminus \mathfrak{m} = \mathcal{O}_K^\times$. □

For any $x \in \mathfrak{m}$, we have $\mathcal{O}_K + x^{-1}\mathcal{O}_K = K$; in particular, $K = \operatorname{Frac} \mathcal{O}_K$.

Example 1.19. Let $K = \mathbb{Q}$ with $|\cdot|_p$. Then $\mathcal{O}_K = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$, $\mathfrak{m} = p\mathbb{Z}_{(p)}$, and $k = \mathbb{F}_p$.

Definition 1.20. Let v be a valuation on a field K. If $\operatorname{im} v \cong \mathbb{Z}$, then v is a **discrete valuation** on K, and K is **discretely valued**. An element $\pi \in \mathcal{O}_K$ is a **uniformiser** if $v(\pi) > 0$ and $v(\pi)$ generates $\operatorname{im} v$.

Example 1.21. $\mathbb{Q}$ with a p-adic valuation and $k(t)$ with the t-adic valuation are discretely valued fields.

If w is a discrete valuation on K, we can rescale it to obtain an equivalent valuation v with $\operatorname{im} v = \mathbb{Z}$. Then v is called a **normalised valuation**. Its uniformisers are precisely those elements $\pi \in K$ with $v(\pi) = 1$.

We can characterise discrete valuations in terms of their valuation rings.

Lemma 1.22. *Let v be a valuation on K. TFAE:*

(i) *v is discrete.*

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

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

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

Proof.
(i) $\implies$ (ii): As K is a field, $\mathcal{O}_K$ is an ID. Now, let $0 \neq I \trianglelefteq \mathcal{O}_K$, and find $x \in I$ of minimal value by discreteness of v. Then $(x) = \{a \in \mathcal{O}_K \mid v(a) \geq x\} \subseteq I$; on the other hand, if $y \in I$, then $v(x^{-1}y) \geq 0$, so $y = x(x^{-1}y) \in (x)$. Hence $I = (x)$.

(ii) $\implies$ (iii): Clear.

(iii) $\implies$ (iv): Write $\mathfrak{m} = (x_1, \ldots, x_n)$; wlog set $v(x_1) \leq \cdots \leq v(x_n)$. Then $x_2, \ldots, x_n \in (x_1)$, so $\mathfrak{m} = (x_1)$.

(iv) $\implies$ (i): Let $\mathfrak{m} = (\pi)$, and let $c = v(\pi)$. If $v(x) > 0$, then $x \in \mathfrak{m}$, so $v(x) \geq c$. Hence $(0, c)$ is disjoint from $\operatorname{im} v$. Since non-discrete subgroups of $\mathbb{R}$ are dense, and the discrete subgroups of $\mathbb{R}$ are all isomorphic to $\mathbb{Z}$, we are done. □

Condition (ii) is the most powerful; we therefore make the following definition.

Definition 1.23. A **discrete valuation ring** (DVR) is a local PID; equivalently, it is a PID with exactly one nonzero prime ideal.

In fact, all DVRs have associated discrete valuations.

Lemma 1.24.

(i) *Let v be a discrete valuation on a field K. Then $\mathcal{O}_K$ is a DVR.*

(ii) *Let R be a DVR. Then there exists a discrete valuation v on $\operatorname{Frac} R$ such that $\mathcal{O}_K = R$.*

Proof.

(i) $\mathcal{O}_K$ is a PID by the last lemma, and contains the unique maximal ideal $\mathfrak{m}$.

(ii) Let R have unique nonzero prime ideal $\mathfrak{m}$. Then $\mathfrak{m} = (\pi)$ for some prime $\pi \in R$. By unique factorisation, any $0 \neq x \in R$ can be written uniquely $x = u\pi^k$ for some unit $u \in R^\times$ and $k \in \mathbb{N}$, so any $0 \neq x \in \operatorname{Frac} R$ can be written uniquely as $x = u\pi^k$ for $u \in R^\times$ and $k \in \mathbb{Z}$. Define $v(x) = k$; can easily check this satisfies the requirements.

□

Example 1.25. $\mathbb{Z}_{(p)}$ and $k[\![t]\!]$ are DVRs.

1.3 Completions of non-Archimedean valued fields

Let $(K, |\cdot|)$ be a non-Archimedean valued field with $\mathcal{O}_K$ and $\mathfrak{m}$ as before. Its completion $\hat{K}$ is also non-Archimedean, and $\hat{K}$ is discretely valued iff K is. More precisely, let v be the normalised valuation on $\hat{K}$; then $v(K^\times) = v(\hat{K}^\times)$. In particular, a uniformiser on K (if it exists) remains a uniformiser on $\hat{K}$.

Example 1.26. The ring of **p-adic integers** $\mathbb{Z}_p$ is the valuation ring of $\mathbb{Q}_p$:

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

Since p is a uniformiser on $\mathbb{Q}$ wrt $|\cdot|_p$, the ring $\mathbb{Z}_p$ is a DVR with maximal ideal (p) and nonzero ideals (p^n) $(n \geq 0)$.

We understand the metric structure on $\hat{K}$, but we also want to understand its algebraic structure. To do this, we will consider an algebraic notion of completion.

Definition 1.27. Let $(A_n)_{n=1}^\infty$ be a sequence of sets/groups/rings equipped with homomorphisms $\varphi_n : A_{n+1} \to A_n$, called **transition maps**. The **inverse limit** $\varprojlim_n A_n$ of A_n is the set/group/ring given by

$$\varprojlim_n A_n = \left\{ (a_n) \in \prod_n A_n \;\middle|\; \varphi_n(a_n + 1) = a_n \right\} \leq \prod_n A_n,$$

with operations defined componentwise.

Let $\theta_m : \varprojlim_n A_n \to A_m$ denote the mth natural projection. The inverse limit satisfies the following universal property:

Proposition 1.28 (Universal property of the inverse limit)**.** *For any structure B together with homomorphisms $\psi_n : B \to A_n$ such that*

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

commutes, there is a unique homomorphism $\psi : B \to \varprojlim_n A_n$ such that $\theta_m \circ \psi = \psi_m$.

Proof. Define $\psi : B \to \prod_n A_n$ by $\psi(b) = \prod_n \psi_n(b)$. Since $\psi_n = \varphi_n \circ \psi_{n+1}$, $\psi(b) \in \varprojlim_n A_n$. This map is clearly structure-preserving, and unique since it is determined by its projections. □

Definition 1.29. Let $I \trianglelefteq R$. The **I-adic completion** of R is the ring $\hat{R} = \varprojlim_n \frac{R}{I^n}$ where the transition maps $R/I^{n+1} \to R/I^n$ are the natural projections.

By the universal property, there is a natural map $\iota : R \to \hat{R}$, constructed from the quotient maps. Then R is **I-adically complete** if ι is an isomorphism.

Let $\hat{\mathcal{O}}_K$ be the valuation ring of $\hat{K}$, and $\hat{\mathfrak{m}}$ its maximal ideal.

Proposition 1.30. *Let $\pi \in \hat{\mathfrak{m}}$ (that is, $|\pi| < 1$). Then*

(i) $\hat{\mathcal{O}}_K$ is (π)-adically complete; that is,

$$\hat{\mathcal{O}}_K \xrightarrow[\iota]{\simeq} \varprojlim_n \frac{\hat{\mathcal{O}}_K}{(\pi)^n}$$

(ii) Fix a set $A \subseteq \hat{\mathcal{O}}_K$ of coset representatives of $\hat{\mathcal{O}}_K/(\pi)$. Every $x \in \hat{\mathcal{O}}_K$ can be written uniquely as a Taylor series $x = \sum_{i=0}^{\infty} a_i \pi^i$, where $a_i \in A$; conversely, every such series $\sum_{i=0}^{\infty} a_i \pi^i$ converges in $\mathcal{O}_K$.

Proof.

(i) If $x \in \ker i$, then $v(x) \geq nv(\pi)$ for all $n \in \mathbb{N}$, so $x = 0$. Hence i is injective.

Fix $(x_n) \in \varprojlim_n \hat{\mathcal{O}}_K/(\pi)^n$. By definition, $x_n \equiv x_{n+1} \bmod \pi^n$, so

$$v(x_n - x_{n+1}) \geq nv(\pi).$$

By the ultrametric inequality, (x_n) is Cauchy; by completeness, x_n converges to some $x \in \hat{\mathcal{O}}_K$. Then $i(x) = (x_n)$, so i is surjective.

(ii) Exercise.

□

Note that this result does not extend to non-principal ideals. In particular, if $\hat{K}$ is not discretely valued, then it is not necessarily $\hat{\mathfrak{m}}$-adically complete.

Corollary 1.31. *Let $\hat{K}$, π and A as before. Then every $x \in \hat{K}$ can be written uniquely as a Laurent series $x = \sum_{i=-k}^{\infty} a_i \pi^i$, where $k \in \mathbb{N}$ and $a_i \in A$; conversely, every such series $\sum_{i=-k}^{\infty} a_i \pi^i$ converges in $\hat{K}$.*

Proof. Fix $0 \neq x \in \hat{K}$. For large enough $k \in \mathbb{N}$, have $v(\pi^k x) = kv(\pi) + v(x) > 0$. Done by the previous proposition. □

We want to view the algebraic structure of $\hat{K}$ in terms of that of K.

Proposition 1.32.

$$\frac{\hat{\mathcal{O}}_K}{\hat{\mathfrak{m}}} \cong \frac{\mathcal{O}_K}{\mathfrak{m}} = k.$$

Proof. Consider the natural map $\varphi : \mathcal{O}_K \to \hat{\mathcal{O}}_K/\hat{\mathfrak{m}}$. Then $x \in \ker \varphi$ iff $x \in \hat{\mathfrak{m}} \cap \mathcal{O}_K = \mathfrak{m}$, so φ descends to an injective map $\psi : \mathcal{O}_K/\mathfrak{m} \hookrightarrow \hat{\mathcal{O}}_K/\hat{\mathfrak{m}}$.

It remains to show this map is surjective. Indeed, take $x \in \hat{\mathcal{O}}_K$. Since $\mathcal{O}_K$ is dense and $\hat{\mathfrak{m}} + x$ is open (as it is a ball), there is some $y \in \mathcal{O}_K \cap \hat{\mathfrak{m}} + x$. Then $\psi(y + \mathfrak{m}) = x + \hat{\mathfrak{m}}$. □

When K is discretely valued, $\mathfrak{m}^n = \{x \in \mathcal{O}_K \mid v(x) \geq n\}$ is also a ball, so the proof above also gives isomorphisms

$$\frac{\mathcal{O}_K}{\mathfrak{m}^n} \xrightarrow[\psi_n]{\simeq} \frac{\hat{\mathcal{O}}_K}{\hat{\mathfrak{m}}^n}$$

via the natural map.

These results allow us to describe the structure of $\hat{K}$ very explicitly.

Corollary 1.33. *Suppose K is discretely valued, and let $\pi \in \mathcal{O}_K$ be a uniformiser. Then*

(i)

$$\hat{\mathcal{O}}_K \cong \varprojlim_n \frac{\mathcal{O}_K}{(\pi)^n}.$$

(ii) Fix a set $A \subseteq \mathcal{O}_K$ of coset representatives of $\mathcal{O}_K/(\pi)$. Then every $x \in \hat{K}$ can be written uniquely as a Laurent series $x = \sum_{i=-k}^{\infty} a_i \pi^i$, where $k \in \mathbb{N}$ and $a_i \in A$; conversely, every such series $\sum_{i=-k}^{\infty} a_i \pi^i$ converges in $\hat{K}$. Further, $k = 0$ iff $x \in \hat{\mathcal{O}}_K$, and the series is finite iff $x \in K$.

Proof.

(i) The isomorphisms ψ_n given above commute with the transition maps. We are done by the universal property of the inverse limit and $\hat{\mathfrak{m}}$-adic completeness of $\hat{\mathcal{O}}_K$.

(ii) Follows from part (i) and the previous corollary.

□

Example 1.34. $\hat{\mathbb{Z}}_p \cong \varprojlim_n \mathbb{Z}_{(p)}/(p)^n\mathbb{Z}_{(p)}$.

In the case of $\mathbb{Q}_p$, we can go further.

Proposition 1.35. *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.*

Proof. By the above, it suffices to show $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$, as then $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Indeed, let $\frac{a}{b} \in \mathbb{Z}_{(p)}$ (so $b \not\equiv 0 \bmod p$). For $n \in \mathbb{N}$, we can choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \bmod p^n$. Then $y_n \to \frac{a}{b}$ as $n \to \infty$. □

Corollary 1.36.

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

(ii) Every element $x \in \mathbb{Q}_p$ can be written uniquely as a Laurent series in p with coefficients in $\{0, 1, \ldots, p-1\}$: $x = \sum_{i=-k}^{\infty} a_i p^i$.

Proof. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$, the natural inclusion gives isomorphisms $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$. For the Laurent series coefficients, we have $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, so $\{0, \ldots, p-1\}$ is a set of coset representatives of $\mathbb{Z}_p/p\mathbb{Z}_p$. □

Example 1.37. In $\mathbb{Q}_p$, $\frac{1}{1-p} = 1 + p + p^2 + \ldots$

2 Complete Valued Fields

In this section, let $(K, |\cdot|)$ be a complete discretely-valued field with uniformiser π, and let v be the associated normalised valuation.

Fix $x \in \mathcal{O}_K$ and let $n = v(x) \geq 0$. Then $x \equiv 0 \bmod \pi^n$, but $x \not\equiv 0 \bmod \pi^{n+1}$. In particular, $x \equiv 0 \bmod \pi^k \iff v(x) \geq k$.

2.1 Hensel's lemma

Theorem 2.1 (Hensel's lemma, version 1)**.** *Let $f \in \mathcal{O}_K[X]$, and suppose 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. Set $r = v(f'(a))$; then the hypothesis implies that $v(f(a)) > 2r$; in particular, $f(a) \equiv 0 \bmod \pi^{2r+1}$.

We will construct a sequence (x_n) in $\mathcal{O}_K$ such that

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

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

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

Suppose we have constructed $x_1, \ldots, x_n$ satisfying (i) and (ii). Define

$$x_{n+1} \coloneqq x_n - \frac{f(x_n)}{f'(x_n)} \coloneqq x_n + c.$$

Since $x_n \equiv x_1 \bmod \pi^{r+1}$, have $f'(x_n) \equiv f'(x_1) \not\equiv 0 \bmod \pi^{r+1}$ and $f'(x_n) \equiv f'(x_1) \equiv 0 \bmod \pi^r$. Hence $v(f'(x_n)) = r$, and so $v(x_{n+1} - x_n) = v(c) \geq n + r$ by (i). Hence (ii) holds.

Now, expanding $f(X + Y)$ in powers of Y, we get

$$f(X+Y) = f(X) + f'(X)Y + \frac{1}{2}f''(X)Y^2 + \cdots = \sum_{k=0}^{\infty} \frac{1}{k!} f^{(k)}(X) Y^k.$$

Therefore

$$f(x_{n+1}) = f(x_n + c) = \underbrace{f(x_n) + f'(x_n)c}_{0} + c^2 y \text{ where } y \in \mathcal{O}_K.$$

Hence

$$v(f(x_{n+1})) \geq \underbrace{2v(c)}_{\geq n+r} + \underbrace{v(y)}_{\geq 0} \geq n + r + 1.$$

Thus (i) holds.

By (ii), (x_n) is Cauchy; let $x_n \to x \in \mathcal{O}_K$ (as $\mathcal{O}_K$ is closed). By (i), $f(x) = \lim_{n\to\infty} f(x_n) = 0$. Moreover, (ii) implies that $a = x_1 \equiv x_n \bmod \pi^{1+r}$, so in fact $a \equiv x \bmod \pi^{r+1}$. By definition of r, we then have $|x - a| < |f'(a)|$, proving existence. By the argument establishing (i), we also have $v(f'(x)) = r = v(f'(a))$.

For uniqueness, suppose x' also satisfies $f(x') = 0$ and $|x' - a| < |f'(a)|$. Set $\delta = x' - x \neq 0$. By the ultrametric inequality, $|\delta| = |(x-a) - (x'-a)| < |f'(a)|$. But then also

$$0 = f(x+\delta) = \underbrace{f(x)}_{0} + \delta f'(x) + \delta^2 y \text{ where } y \in \mathcal{O}_K,$$

so $f'(x) = -\delta y$. Hence $|f'(a)| = |f'(x)| \leq |\delta|$.$_{\#}$ □

The proof method can be viewed as a non-Archimedean analogue of the Newton-Raphson iteration method for finding real roots of functions.

Corollary 2.2. *Let $f \in \mathcal{O}_K[X]$, and let $\bar{c} \in k = \mathcal{O}_K/\mathfrak{m}$ be a simple root of $\overline{f}(X) \coloneqq f(X) \bmod \mathfrak{m} \in k[X]$. Then $\exists! x \in \mathcal{O}_K$ such that $f(x) = 0$ and $x \equiv \bar{c} \bmod \mathfrak{m}$.*

Proof. Apply Hensel's Lemma to a lift $c \in \mathcal{O}_K$ of $\bar{c}$. Indeed, $f(c) \bmod \mathfrak{m} = \overline{f}(\bar{c}) = 0$ but $f'(c) \bmod \mathfrak{m} = \overline{f}'(\bar{c}) \neq 0$. Then $|f(c)| < 1 = |f'(c)|^2$. □

Example 2.3. $f(X) = X^2 - 2$ has a simple root mod 7. Therefore there is some (unique) $\sqrt{2} \in \mathbb{Z}_7$.

Corollary 2.4. $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^3 & p = 2 \end{cases}$

Proof.
$p > 2$: Let $b \in \mathbb{Z}_p^\times$. Applying the previous corollary to $f(X) = X^2 - b$, which has simple roots, find that $b \in (\mathbb{Z}_p^\times)^2 \iff \bar{b} \in (\mathbb{F}_p^\times)^2$. Therefore $\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 = \mathbb{Z}/2\mathbb{Z}$.

Now, we have an isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \cong \mathbb{Q}_p^\times$ by $(u, n) \to up^n$. This isomorphism yields the desired result.

$p = 2$: Let $b \in \mathbb{Z}_2^\times$, and again consider $f(X) = X^2 - b$. This time, $f'(X) \equiv 0 \bmod 2$, so f has no simple roots mod 2. We consider instead congruences modulo 8.

Indeed, 3, 5 and 7 are not squares mod 8, but 1 is. Conversely, suppose $b \equiv 1 \bmod 8$. Then $|f(1)|_2 \leq 2^{-3} < |f'(1)|_2^2 = 2^{-2}$, so we can apply Hensel's lemma to get a root $x \in \mathbb{Z}_2$ of f. Therefore $b \in (\mathbb{Z}_2^\times)^2 \iff b \equiv 1 \bmod 8$. Hence $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times$. Using $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$ again, we get the result. □

Theorem 2.5 (Hensel's lemma, version 2)**.** *Let $f \in \mathcal{O}_K[X]$. Let $\overline{f} \in k[X]$ be the reduction of f. Suppose that it factors in $k[X]$ as $\overline{f} = \bar{g}\bar{h}$, with $\bar{g}$ and $\bar{h}$ coprime. Then there is a factorisation $f = gh$ in $\mathcal{O}_k[X]$ such that g reduces to $\bar{g}$, h reduces to $\bar{h}$ and $\deg g = \deg \bar{g}$.*

Proof. Exercise. □

Corollary 2.6. *Suppose $f(x) = a_n X^n + \cdots + a_0 \in K[X]$ is irreducible, with $a_n \neq 0$. Then $|a_i| \leq \max(|a_0|, |a_n|)$.*

Proof. Rescaling by π^{-k} for $k = \min_i v(a_i)$, we have wlog $f \in \mathcal{O}_K[X]$ with $\max_i |a_i| = 1$. It remains to show that $\max(|a_0|, |a_n|) = 1$, that is, that one of a_0 and a_n does not lie in $\mathfrak{m}$. Indeed, suppose both do; then there is a minimal $0 < r < n$ with $|a_r| = 1$ (i.e., $a_r \notin \mathfrak{m}$). But then

$$f(X) \equiv X^r(\underbrace{a_r}_{\not\equiv 0} + \cdots + a_n X^{n-r}) \bmod \mathfrak{m};$$

this lifts by Hensel's lemma to a factorisation $f = gh$ in $\mathcal{O}_K[X]$ with $0 < \deg g < n$.$_\#$ □

2.2 Teichmüller lifts

Definition 2.7. A ring R of characteristic $p > 0$ is **perfect** if the Frobenius automorphism $x \to x^p$ is a bijection; that is, if every element has a p^{th} root. A **perfect field** is a perfect ring that is a field.

Examples 2.8.

1. The finite fields $\mathbb{F}_{p^n}$ are perfect.
2. $\mathbb{F}_p(t^{\frac{1}{p^\infty}}) = \mathbb{F}_p(t, t^{\frac{1}{p}}, t^{\frac{1}{p^2}}, \dots)$ is perfect. This is called the *perfection* of $\mathbb{F}_p(t)$.

Note that a field k of characteristic $p > 0$ is perfect iff all its finite extensions are separable.

Theorem 2.9 (Teichmüller Lifting)**.** *Suppose $k = \mathcal{O}_K/\mathfrak{m}$ is perfect of char p. Then there is a unique map $[\cdot] : k \to \mathcal{O}_K$ such that*

(i) $a \equiv [a] \bmod \mathfrak{m}\ \forall a \in k$

(ii) $[ab] \equiv [a][b] \bmod \mathfrak{m}\ \forall a, b \in k$

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

Definition 2.10. The element $[a] \in \mathcal{O}_K$ given by the theorem is called the **Teichmüller lift** of a.

Lemma 2.11. *Let $x, y \in \mathcal{O}_K$ such that $x \equiv y \bmod \mathfrak{m}^k$. Then $x^p \equiv y^p \bmod \mathfrak{m}^{k+1}$.*

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

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

Since $\operatorname{char} k = p$, we have $p \in \mathfrak{m}$. Thus each $\binom{p}{i} y^{p-i}(u\pi^k)^i \in \mathfrak{m}^{k+1}$ (for $i > 0$), giving the result. □

Proof of Teichmüller lifting. Fix $a \in k$. For each $i \geq 1$, choose a lift $y_i \in \mathcal{O}_K$ of $a^{\frac{1}{p^i}}$, and define $x_i = y_i^{p^i}$.

Claim: (x_i) is a Cauchy sequence whose limit $x \in \mathcal{O}_K$ is independent of the choice of y_i.

Indeed, $y_i \equiv y_{i+1}^p \bmod \mathfrak{m}$ by construction, so, by the previous lemma,

$$x_i = y_i^{p^i} \equiv y_{i+1}^{p^{i+1}} = x_{i+1} \bmod \mathfrak{m}^{i+1}.$$

Now suppose (x_i') arises from some other choice of y_i' lifting to $a^{\frac{1}{p^i}}$. By the same argument, $x_i' \to x' \in \mathcal{O}_K$. Now, consider the sequence (x_i'') whose even terms are x_i and whose odd terms are x_i'. This sequence is *also* given by a choice of lifts of $a^{\frac{1}{p_i}}$, so $x_i'' \to x''$. Since the even and odd terms of (x_i'') converge to x and x', respectively, in fact $x = x'' = x'$. Hence the limit is independent of the choice of y_i.

Set $[a] = x$. Then

$$x_i = y^{p^i} \equiv \left(a^{\frac{1}{p^i}}\right)^{p^i} = a \bmod \mathfrak{m}$$

so $x \equiv a \bmod \mathfrak{m}$. This shows (i).

Now let $b \in K$ have $[b]$ defined via lifts u_i of $b^{\frac{1}{p^i}}$, with $b = \lim_i z_i$, where $z_i = u_i^{p^i}$. Then $u_i y_i$ is a lift of $(ab)^{p^i}$, so

$$[ab] = \lim_{i\to\infty} x_i z_i = \lim_{i\to\infty} x_i \lim_{i\to\infty} z_i = [x_i][z_i].$$

This shows (ii).

It remains to show uniqueness. Indeed, let $\varphi : k \to \mathcal{O}_K$ satisfy (i) and (ii). For $a \in k$, $\varphi(a^{\frac{1}{p^i}})$ is a lift of $a^{\frac{1}{p^i}}$ by (i). Hence, by (ii),

$$[a] = \lim_{i\to\infty} \varphi\left(a^{\frac{1}{p^i}}\right)^{p^i} = \lim_{i\to\infty} \varphi(a) = \varphi(a).$$

Now suppose $\operatorname{char} K = p$. Then $y_i + u_i$ is a lift of $a^{\frac{1}{p^i}} + b^{\frac{1}{p^i}} = (a+b)^{\frac{1}{p^i}}$. Then

$$[a+b] = \lim_{i\to\infty} (y_i + u_i)^p = \lim_{i\to\infty} (y_i^p + u_i^p) = \lim(x_i + z_i) = [a] + [b].$$

Taking constant lifts, $[0] = 0$ and $[1] = 1$. Hence $[\cdot]$ is a homomorphism. □

Example 2.12. Let $K = \mathbb{Q}_p$; then $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$. Let $a \in \mathbb{F}_p^\times$; then $[a]^{p-1} = [a^{p-1}] = [1] = 1$, so $[a]$ is a $(p-1)^{\text{th}}$ root of unity.

We can generalise:

Lemma 2.13. *Suppose $k \subseteq \overline{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$) and fix $a \in k^\times$. Then $[a] \in \mathcal{O}_K^\times$ is a root of unity.*

Proof. By assumption, a lies in some $\mathbb{F}_p^n$, so $a^{p^n-1} = 1$. Hence

$$[a]^{p^n-1} = [a^{p^n-1}] = [1] = 1.$$

□

Theorem 2.14. *Suppose k is perfect and* $\operatorname{char} K = p > 0$. *Then $K \cong k(\!(t)\!)$.*

Proof. Since $\operatorname{char} k \mid \operatorname{char} K$, we have $\operatorname{char} k = p$ also. Hence $[\cdot]$ is a ring homomorphism, so the map $\varphi : k(\!(t)\!) \to K$ by $\varphi(\sum_i a_i t^i) = \sum_i [a_i]\pi^i$ is also a ring homomorphism. Since such series are exactly the elements of K, φ is a bijection, and hence an isomorphism. □

2.3 Extensions of complete valued fields

Theorem 2.15. *Let L/K be a finite extension of degree n.*

(i) $|\cdot|$ extends uniquely (up to equivalence) to an absolute value $|\cdot|_L$ on L given by $|x|_L = |N_{L/K}(x)|^{1/n}$.

(ii) $(L, |\cdot|_L)$ is complete.

Recall that $N_{L/K}$ is multiplicative, and that $N_{L/K}(x)$ is some $\pm a_0^k$, where a_0 is the constant term of m_x. In particular, $N_{L/K}(x) = 0 \implies x = 0$.

Definition 2.16. Let $(K, |\cdot|)$ be a non-Archimedean valued field, and V a K-vector space. A **norm** on V is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ satisfying

(i) $\|x\| = 0 \iff x = 0$.

(ii) $\|\lambda x\| = |\lambda|\|x\|$ for $x \in V$ and $\lambda \in K$.

(iii) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

Example 2.17. If V is finite-dimensional over k and $\{e_i\}$ is a basis, then the **sup norm** $\|\cdot\|_{\sup}$ on V is given by $\|x\|_{\sup} = \max_i |x_i|$, where $x = \sum_i x_i e_i$. This is indeed a norm.

The norm $\|\cdot\|_{\sup}$ depends on the choice of basis $\{e_i\}$, but, as we will see soon, all norms end up being essentially the same anyway.

Definition 2.18. Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent if there are constants $c, d > 0$ such that, for all $x \in V$, $c\|x\|_1 \leq \|x\|_2 \leq \|x\|_1$.

A norm on V induces a metric by $\|x - y\|$, and thus a topology; equivalent norms induce the same topology on V.

Proposition 2.19. *Let $(K, |\cdot|)$ be a complete non-Archimedean valued field, and let V be a vector space over K. Then V is complete wrt $\|\cdot\|_{sup}$.*

Proof. Let (v_i) be a Cauchy sequence in v. Write $v_i = \sum_j x_{ij} e_j$; for each j, the sequence $(x_{ij})_i$ in K is Cauchy, by definition. Let $x_{ij} \xrightarrow[i\to\infty]{} x_j \in K$ by completeness; then $v_i \to \sum_j x_j e_j$. □

Theorem 2.20. *Let $(K, |\cdot|)$ be a complete non-Archimedean valued field, and let V be a vector space over K. Then any two norms on V are equivalent. In particular, V is complete wrt any norm.*

Proof. Fix a basis $\{e_i\}$ of V for the sup norm, and take any norm $\|\cdot\|$ on V. It suffices to show $\|\cdot\|$ is equivalent to $\|\cdot\|_{\sup}$.

Set $D = \max_i \|e_i\|$; then, for $x = \sum_i x_i e_i$, we have

$$\|x\| \leq \max_i \|x_i e_i\| \leq D \max_i |x_i| = D\|x\|_{\sup}.$$

To find C, proceed by induction on $n = \dim V$. For $n = 1$, have

$$\|x\| = |x_1|\|e_1\| = \|x\|_{\sup}\|e_1\|,$$

so take $C = \|e_1\|$.

For $n > 1$, consider $V_i = \langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n\rangle$. By induction, each V_i is complete wrt $\|\cdot\|$, and hence each V_i is closed in V (wrt $\|\cdot\|$). Then $S = \bigcup_i (e_i + V_i)$ is a closed set not containing 0, so its complement contains some open ball $B(0, C)$ $(C > 0)$. Fixing $0 \neq x \in V$, suppose $|x_j| = \max_i \|x_i\|$, so that $\|x\|_{\sup} = |x_j|$. Then also $x/x_j \in (e_j + V_j) \subseteq S$, so $\|x/x_j\| \geq C$, and so $\|x\| \geq C\|x\|_{\sup}$. Completeness follows since V is complete wrt the sup norm. □

Proof of Theorem 2.15.

(i) Consider extensions $|\cdot|_L$ and $|\cdot|'_L$ of $|\cdot|$ to K. Viewing L as a K-vector space, these extensions are norms. By the previous proposition, therefore, they are equivalent as norms, and so equivalent as absolute values. Therefore $|\cdot|_L = |\cdot|'^{\,c}_L$; since the absolute values agree on K, we must have $c = 1$ and so $|\cdot|_L = |\cdot|'_L$.

Since $N_{L/K}(x) = x^n$ for $x \in K$, we do indeed have that $|\cdot|_L$ extends $|\cdot|$ on K.

It remains to show $|\cdot|_L$ is indeed a norm. Since $N_{L/K}(x) = 0 \implies x = 0$, and $N_{L/K}$ is multiplicative, conditions (i) and (ii) are easily satisfied by $|\cdot|_L$.

To show condition (iii), we need some preparation.

□

Definition 2.21. Let $R \leq S$ be rings. $s \in S$ is **integral over** R if s is a root of some monic polynomial in $R[X]$.

The **integral closure** of R in S is the set $R^{\mathrm{int}(S)} = \{s \in S \mid s \text{ integral over } R\}$.

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

Proposition 2.22. *$R^{intS} \leq S$, and moreover R^{intS} is integrally closed in S.*

Proof. Example sheet. □

Lemma 2.23. *Let $(K, |\cdot|)$ be a non-Archimedean valued field. Then $\mathcal{O}_K$ is integrally closed in K.*

Proof. Let $x \in K$ be integral over $\mathcal{O}_K$, and suppose (wlog) that $x \neq 0$. Take $a_0, \ldots, a_{n-1} \in \mathcal{O}_K$ such that

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0,$$

so that

$$x = -a_{n-1}x^{-1} - \cdots - a_0x^{-n}.$$

If $|x| > 1$, then, since $|a_i| \leq 1$,

$$|x| = |-a_{n-1}x^{-1} - \cdots - a_0 x^{-n}| < 1.\#$$

Hence $|x| \leq 1$, that is, $x \in \mathcal{O}_K$. □

Lemma 2.24. *$\mathcal{O}_L \coloneqq \{y \in L \mid |y|_L \leq 1\}$ is the integral closure of $\mathcal{O}_K$ in L.*

Proof. Let $0 \neq y \in L$, and let $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ be its minimal polynomial over K.

Claim: y is integral over K iff $f \in \mathcal{O}_K[X]$.

If $f \in \mathcal{O}_K[X]$, then clearly y is integral over $\mathcal{O}_K$. Conversely, suppose that there is some (nonzero) monic polynomial $g \in \mathcal{O}_K[X]$ with $g(y) = 0$. Then $f \mid g$, and so every root of f is a root of g. Since roots of g are integral over K, all roots of f (in some algebraic closure) are integral over K. By Vieta's formulae, the coefficients a_i are integral over $\mathcal{O}_K$; since $\mathcal{O}_K$ is integrally closed in K, the a_i in fact lie in $\mathcal{O}_K$. This proves the claim.

Now, $|a_i| \leq \max\{|a_0|, 1\}$, and $N_{L/K}(y) = \pm a_0^m \in \mathcal{O}_K$, so we have

$$y \in \mathcal{O}_L \iff |N_{L/K}(y)| \leq 1 \iff |a_0| \leq 1 \iff |a_i| \leq 1 \ \forall i \iff f \in \mathcal{O}_K[X].$$

We are then done by the claim. □

Proof of Theorem 2.15, cont.

(i) It remains to show property (iii) of the absolute value. Indeed, let $x, y \in L$, and suppose (wlog) that $|x|_L \leq |y|_L$. Then $\left|\frac{x}{y}\right| \leq 1$, so $\frac{x}{y} \in \mathcal{O}_L$. By the last lemma, $\mathcal{O}_L$ is a ring, so $1 + \frac{x}{y} \in \mathcal{O}_L$. Hence

$$\left|1 + \frac{x}{y}\right| \leq 1 \implies |x + y| \leq |y| \leq \max\{x, y\}.$$

(ii) Again viewing L as a K-vector space, it is complete wrt *any* norm, and absolute values on L are norms.

□

Corollary 2.25. *Let L/K be finite. Then L is discretely valued wrt $|\cdot|_L$.*

Proof. Let $n = [L : K]$. Let v be a valuation on K, and let v_L be the unique valuation on L extending v. For $y \in L^\times$, we have $v_L(y) = \frac{1}{n} v(N_{L/K}(y))$ by definition, so $v_L(L^\times) \subseteq \frac{1}{n} v(K^\times)$. Since v is discrete, so is v_L. □

Corollary 2.26. *Let $\overline{K}/K$ be an algebraic closure. Then $|\cdot|$ extends to a unique absolute value $|\cdot|_{\overline{K}}$ on $\overline{K}$.*

Proof. Let $x \in \overline{K}$; then $x \in L$ for some *finite* subextension L/K. Then define $|x|_{\overline{K}} \coloneqq |x|_L$. This is well-defined: if $x \in L$ and $x \in L'$, then $|x|_L = |x|_{LL'} = |x|_{L'}$ by uniqueness of extension in LL'/K. Similarly, $|x|_{\overline{K}}$ is an absolute value. Uniqueness also follows by uniqueness on finite extensions. □

Note that, since K has extensions of arbitrarily large degree, $|\cdot|_{\overline{K}}$ cannot be discrete.

Example 2.27. Let $K = \mathbb{Q}_p$; then $\sqrt[n]{p} \in \overline{\mathbb{Q}}_p$ for each $n \in \mathbb{N}$. Then $v(\sqrt[n]{p}) = \frac{v_p(p)}{n} = \frac{1}{n}$.

Note that $\overline{\mathbb{Q}_p}$ is not complete wrt this valuation (see ES2). On ES2, we will also see that its completion $\mathbb{C}_p$ is also algebraically closed. This field is isomorphic to $\mathbb{C}$ as a field, but not as a topological space.

Proposition 2.28. *Let L/K be a finite extension. Suppose that*

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

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

Then there is some $a \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[a]$.

We will see later that, in fact, $(i) \implies (ii)$.

Proof. By PET, write $k_L = k(\overline{\alpha})$. Let $\alpha \in \mathcal{O}_L$ be a lift of $\overline{\alpha}$ and $g \in \mathcal{O}_K[X]$ a monic lift of the minimal polynomial of $\overline{\alpha}$. On L, let v_L be the normalised valuation on L, and fix a uniformiser π_L.

Since $\overline{g} \in k[X]$ is irreducible and separable, it has simple roots: that is, $g(\alpha) \equiv 0 \bmod \pi_L$, but $g'(\alpha) \not\equiv 0 \bmod \pi_L$.

Suppose $g(\alpha) \equiv 0 \bmod \pi_L^2$. Expanding about α,

$$g(\alpha + \pi_L) \equiv \underbrace{g(\alpha)}_{0} + \pi_L g' \bmod \pi_L^2,$$

so

$$v_L(g(\alpha + \pi_L)) = v_L(\pi_L g'(\alpha)) = v_L(\pi_L) = 1.$$

Hence either $v_L(g(\alpha)) = 1$ or $v_L(g(\alpha + \pi_L)) = 1$. Since both of these are lifts of $\overline{\alpha}$, assume wlog that $v_L(g(\alpha)) = 1$.

Set $\beta \coloneqq g(\alpha) \in \mathcal{O}_K[\alpha]$; this is a uniformiser for K.

Let $m = [K(\alpha) : K]$, and define a map

$$\begin{aligned} \mathcal{O}_K^n &\xrightarrow{\varphi} L \\ (x_0, \ldots, x_{n-1}) &\to \sum_i x_i \alpha^i \end{aligned}$$

$\mathcal{O}_K$ is compact and φ is continuous (since field operations are), so $\operatorname{im}\varphi = \mathcal{O}_K[\alpha]$ is compact, and hence closed, in L.

Since $k_L = k(\overline{\alpha})$, take a set $A \subseteq \mathcal{O}_K[\alpha]$ of coset representatives for the residue field $k_L = \mathcal{O}_L/(\beta)$. Let $y \in \mathcal{O}_L$, and write $y = \sum_{i=0}^{\infty} \lambda_i \beta^i$, for $\lambda_i \in A$. Since the partial sums lie in the closed set $\mathcal{O}_K[\alpha]$, so does their limit y. $\square$

3 Local fields

Let X be a topological space. We say X is **locally compact** if every point $x \in X$ has a neighbourhood U contained in a compact set Z (so $x \in U \subseteq Z \subseteq X$).

Definition 3.1. Let $(K, |\cdot|)$ be a valued field. Then K is a **local field** if it is complete and locally compact.

Example 3.2. $\mathbb{R}$ and $\mathbb{C}$ are local fields.

3.1 Basic properties

Proposition 3.3. *Let $(K, |\cdot|)$ be a non-Archimedean valued field. TFAE:*

1. *K is locally compact.*
2. *$\mathcal{O}_K$ is compact.*
3. *v is discrete and k is finite.*

Proof.
$(i) \implies (ii)$: Let U be a compact neighbourhood of 0; since U contains an open ball, any $x \in \mathcal{O}_K$ with small enough absolute value has $x\mathcal{O}_K \subseteq U$. Since $x\mathcal{O}_K$ is closed, it is compact. But $x\mathcal{O}_K \xrightarrow[x^{-1}\cdot]{\simeq} \mathcal{O}_K$, so $\mathcal{O}_K$ is also compact.

$(ii) \implies (iii)$: Let $x \in \mathfrak{m}$ and let $A_x \subseteq \mathcal{O}_K$ be a set of coset representatives for $k = \mathcal{O}_K/(x)$. Then

$$\mathcal{O}_K = \bigsqcup_{y \in A_x} y + (x)$$

is a disjoint open cover for $\mathcal{O}_K$, so A_x must be finite by compactness. Hence k is finite.

Now, suppose v is not discrete; find a sequence (x_n) in $\mathcal{O}_K$ such that $v(x_1) > v(x_2) > v(x_3) > \cdots > 0$. Then $(x) \subsetneq (x_2) \subsetneq \cdots \subsetneq \mathcal{O}_K$, so (by correspondence) we have found infinitely many ideals in the finite field k.$_\#$

$(iii) \implies (i)$: Let (x_n) be a sequence in $\mathcal{O}_K$, and fix a uniformiser $\pi \in \mathcal{O}_K$. Since each factor $(\pi)^i/(\pi)^{i+1} \cong k$ is finite, each quotient $\mathcal{O}_K/(\pi)^i$ is finite by induction. Hence each $(x_n \bmod \pi^i)$ can only take finitely many values.

Now, find a subsequence $(x_{1,n})$ of (x_n) such that $x_{1,n} \equiv a_1 \bmod \pi$ for some $a_1 \in \mathcal{O}_K/(\pi)$; inductively construct nested subsequences $(x_{i,n})$ with $x_{i,n} \equiv a_i \bmod \pi^i$ for some $a_i \in \mathcal{O}_K/(\pi)^i$. $a_i \equiv a_{i+1} \bmod \pi^i$. Then $x_{i,i} \equiv a_i \bmod \pi^i$ and $x_{i,i} \equiv x_{i+1,i+1} \bmod \pi^i$ (since the sequences are nested). By completeness (and the ultrametric inequality), have $x_{n,n} \to x \in \mathcal{O}_K$. Thus $\mathcal{O}_K$ is a sequentially compact metrisable space, and thus compact. □

Examples 3.4. $\mathbb{Q}_p$ and $\mathbb{F}_p(\!(t)\!)$ are local fields.

Definition 3.5. Let (A_n) be a sequence of finite sets, with transition maps. The **profinite topology** on $A = \varprojlim_n A_n$ is the weakest topology on A such that the projections $A \to A_n$ are continuous, where A_n is given the discrete topology.

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

Proposition 3.6. *Let K be a non-Archimedean local field with uniformiser π. Under the isomorphism $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/(\pi)^n$, the standard topology on $\mathcal{O}_K$ agrees with the profinite topology.*

Proof. **Claim:** $B = \{a + (\pi)^n \mid n \in \mathbb{N},\ a \in \mathcal{O}_K\}$ is a basis for both topologies.

The claim is obvious for the topology from $|\cdot|$; for the profinite topology, observe that the n^{th} projection $\mathcal{O}_K \to \mathcal{O}_K/(\pi)^n$ is continuous iff each $a + (\pi)^n$ is open. □

Lemma 3.7. *Let K be a non-Archimedean local field, and let L/K be a finite extension. Then L is also a local field.*

Proof. We showed in the last section that L is complete and discretely valued. It therefore suffices to show that $k_L = \mathcal{O}_L/\mathfrak{m}\mathcal{O}_L$ is finite.

Indeed, let $(\alpha_1, \ldots, \alpha_n)$ be a K-basis for L. Since $|\cdot|_L$ is equivalent to $\|\cdot\|_{\sup}$ as a K-norm on L, there is some $r > 0$ such that

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

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

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

so, since $\mathcal{O}_K$ is Noetherian, $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. Taking a quotient by $\mathfrak{m}$, k_L is a finitely-generated k-module; since k is finite, so must be k_L. □

3.2 Classification

Local fields can be classified; this classification needs the following definition.

Definition 3.8. A non-Archimedean valued field $(K, |\cdot|)$ has **equal characteristic** if $\operatorname{char} K = \operatorname{char} k$; otherwise, K has **mixed characteristic**.

Example 3.9. $\mathbb{Q}_p$ has mixed characteristic (0 and p), but $\mathbb{F}_p(\!(t)\!)$ has equal characteristic $p > 0$.

Note that, since k is finite, we have $\operatorname{char} k > 0$, and so equal characteristic fields have $\operatorname{char} K > 0$.

Theorem 3.10. *Let K be a non-Archimedean local field of equal characteristic $p > 0$. Then $K \cong \mathbb{F}_{p^n}(\!(t)\!)$.*

Proof. K is a complete, discretely valued field of positive characteristic; moreover k is finite and hence perfect. Then $K \cong \mathbb{F}_{p^n}(\!(t)\!)$ via the representation of elements of K as Laurent series with coefficients in k. Indeed, set the coset representatives to be the Teichmüller lifts; then the lifting map $k \to \mathcal{O}_K$ is a ring homomorphism. □

Lemma 3.11. *An absolute value $|\cdot|$ on a field K is non-Archimedean iff $\{|n| \mid n \in \mathbb{Z}\}$ is bounded.*

Proof. Suppose $|\cdot|$ is non-Archimedean. Since $|-n| = |n|$, it suffices to show $|n|$ is bounded on $\mathbb{N}$; then

$$|n| = |1 + \cdots + 1| \leq |1|.$$

Conversely, suppose $|n| \leq B$ for $n \in \mathbb{Z}$, and let $x, y \in K$ with $|x| \leq |y|$. Then

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

so $|x+y| \leq |y|(B(m+1))^{\frac{1}{m}} \to |y|$. Thus the ultrametric inequality holds. □

Theorem 3.12 (Ostrowski)**.** *Any nontrivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.*

Proof. Fix a nontrivial absolute value $|\cdot|$ on $\mathbb{Q}$.

Archimedean case: Find $b \in \mathbb{Z}$ with $|b| > 1$. Let $a > 1$ be an integer, and expand b^n (uniquely) in base a as

$$b^n = c_m a^m + \cdots + c_0 a^0 \text{ for } c_i \in \{0, \ldots, a-1\} \text{ and } c_m \neq 0.$$

Let $B = \max_i |c_i|$; then

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

Taking n^{th} roots, and using the fact that $a^m \leq b^n$, so $m \leq n \log_a b$, have

$$|b| \leq \underbrace{[(n(\log_a b) + 1)B]^{\frac{1}{n}}}_{\xrightarrow[n\to\infty]{} 1} \max\{|a|^{\log_a b}, 1\}.$$

Therefore $|b| \leq \max\{|a|^{\log_a b}, 1\}$; then $|a| \leq 1$ and $|b| \leq |a|^{\log_a b}$. Swapping a and b, also get $|a| \leq |b|^{\log_b a}$. From these we get $\frac{\log|a|}{\log a} = \frac{\log|b|}{\log b}$, and so, setting $\lambda = \frac{\log|b|}{\log b}$, we get $|a| = a^\lambda$ for all $a > 1$. Hence $|x| = |x|_\infty^\lambda$ for all $x \in \mathbb{Q}$.

Non-Archimedean case: For $n \in \mathbb{Z}$, $|n| \leq 1$; find $n \in \mathbb{Z}$ with $n < 1$. Let $n = p_1^{e_1} \ldots p_r^{e_r}$ be the prime factorisation of n. Then some $p \in \{p_1, \ldots, p_r\}$ has $|p| < 1$. Suppose that also $|q| < 1$ for some prime $q \neq p$. Find $r, s \in \mathbb{Z}$ such that $1 = rp + sq$; then

$$1 = |rp + sq| \leq \max\{|rp|, |sq|\} < 1._{\#}$$

Thus $|q| = 1$ for all primes $q \neq p$. Let $|p| = \alpha < 1$; then $|x| = \alpha^{v_p(x)}$, so $|\cdot|$ is equivalent to $|\cdot|_p$. □

Theorem 3.13. *Let $(K, |\cdot|)$ be a non-Archimedean local field of mixed characteristic. Then K is a finite extension of $\mathbb{Q}_p$ for some prime p.*

Proof. Since $\operatorname{char} k \mid \operatorname{char} K$, K must have characteristic 0. Hence K is an extension of $\mathbb{Q}$.

Since $|\cdot|$ is non-Archimedean, the absolute value restricted to $\mathbb{Q}$ is equivalent to some $|\cdot|_p$. Since K is complete, it is in fact an extension of $\mathbb{Q}_p$; it now suffices to show $\mathcal{O}_K$ is finite as a $\mathbb{Z}_p$-module.

Indeed, let $\pi \in \mathcal{O}_K$ be a uniformiser, and v a normalised valuation on K. Set $v(p) = e$. Then $l = \mathcal{O}_K/(p) = \mathcal{O}_K/(\pi)^e$ is finite since $k = \mathcal{O}_K/(\pi)$ is; since $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p \hookleftarrow \mathcal{O}_K/(p) = l$, the field l is a fd $\mathbb{F}_p$-vector space.

Let $x_1, \dots, x_n \in \mathcal{O}_K$ be coset representatives for a $\mathbb{F}_p$-basis for l. Then

$$A = \left\{ \sum_{j=1}^{n} a_j x_j \;\middle|\; a_j \in \{0, \dots, p-1\} \right\}$$

is a set of coset representatives for l.

Let $y \in \mathcal{O}_K$; expanding in powers of p with coefficients in A, we have

$$y = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{n} a_{ij} x_j \right) p^i = \sum_{j=0}^{n} \underbrace{\left(\sum_{i=0}^{\infty} a_{ij} p^i \right)}_{\in \mathbb{Z}_p} x_i,$$

so $\{x_1, \dots x_n\}$ generate $\mathcal{O}_K$ as a $\mathbb{Z}_p$-module.

Hence K is a finite extension of $\mathbb{Q}_p$. □

Theorem 3.14. *Let $(K, |\cdot|)$ be a complete Archimedean field. Then $K \cong \mathbb{R}$ or $\mathbb{C}$ with the standard absolute value.*

Proof. Example sheet. □

In summary, if K is a local field, then one of the following holds:

(i) $K \cong \mathbb{R}$ or $\mathbb{C}$ (Archimedean).

(ii) $K \cong \mathbb{F}_{p^n}(\!(t)\!)$ (non-Archimedean equal characteristic).

(iii) K is a finite extension of $\mathbb{Q}_p$ (non-Archimedean mixed characteristic).

3.3 Global fields

Definition 3.15. A **global field** is a field which is one of

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

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

Lemma 3.16. *Let $(K, |\cdot|)$ be a complete discretely valued field, and let L/K be a (finite) Galois extension with (unique) absolute value $|\cdot|_L$ extending $|\cdot|$. Fix $x \in L$ and $\sigma \in \operatorname{Gal}(L/K)$. Then $|\sigma(x)|_L = |x|_L$.*

Proof. $x \to |\sigma x|_L$ is an absolute value on L extending $|\cdot|$. Done by uniqueness. □

Lemma 3.17 (Krasner)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field, and let $f \in K[X]$ be a separable irreducible polynomial with roots $\alpha_1, \ldots, \alpha_n \in K^{sep}$, the separable closure of K. Suppose $\beta \in K^{sep}$ satisfies $|\beta - \alpha_1| < |\beta - \alpha_i|$ for $i = 2, \ldots, n$. Then $K(\alpha_1) \subseteq K(\beta)$.*

Proof. Let $L = K(\beta)$ and $L' = L(\alpha_1, \ldots, \alpha_n)$. Then L'/L is Galois as it is the splitting field of a separable polynomial. Let $\sigma \in \mathrm{Gal}(L'/L)$. We have

$$|\beta - \sigma\alpha_1| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1|,$$

so σ fixes α_1, and so

$$\alpha_1 \in L'^{\mathrm{Gal}(L'/L)} = L = K(\beta).$$

□

This lets us show that 'nearby' polynomials define the same extension:

Proposition 3.18. *Let $(K, |\cdot|)$ be a complete discretely valued field, and let $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathcal{O}_K[X]$ be a separable irreducible monic polynomial with roots $\alpha_1, \ldots, \alpha_n \in K^{sep}$. Then there is some $\varepsilon > 0$ such that, for any monic $g(X) = \sum_{i=0}^{n} b_i X^i \in \mathcal{O}_K[X]$ with $|a_i - b_i| < \varepsilon$, there is a root β of g such that $K(\alpha_1) = K(\beta)$.*

Proof. By continuity, choose ε small enough that

$$|g(\alpha_1)| < |f'(\alpha_1)|^2 \text{ and } |f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha_1)|$$

for all sufficiently close g.

Fix such a g; then, since triangles are isosceles,

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

Applying Hensel's lemma to the field $K(\alpha_1)$ at α_1, there is some $\beta \in K(\alpha_1)$ such that $g(\beta) = 0$ and $|\beta - \alpha_1| < |g'(\alpha_1)|$.

Since the α_i are integral, each $|\alpha_1 - \alpha_i| < 1$, and so

$$|g'(\alpha_1)| = |f'(\alpha_1)| = \prod_{i=2}^{n} |\alpha_1 - \alpha_i| \leq |\alpha_1 - \alpha_i| \text{ for } i = 2, \ldots, n.$$

By Krasner's lemma, also $\alpha_1 \in K(\beta)$, so $K(\beta) = K(\alpha_1)$. □

Theorem 3.19. *Let K be a local field. Then K is the completion of a global field.*

Proof.
Case 1: Archimedean.

$\mathbb{R}$ and $\mathbb{C}$ are completions of $\mathbb{Q}$ and $\mathbb{Q}(i)$ (wrt $|\cdot|_\infty$), respectively.

Case 2: equal characteristic non-Archimedean.

$\mathbb{F}_q(\!(t)\!)$ is the completion of $\mathbb{F}_q(t)$ wrt the t-adic absolute value.

Case 3: mixed characteristic non-Archimedean.

Note $\operatorname{char} K = 0$. By PET, write $K = \mathbb{Q}_p(a)$, where a is a root of a monic irreducible polynomial $f \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, choose $g \in \mathbb{Z}[X]$ as in the last proposition. Then $K = \mathbb{Q}_p(\beta)$, where β is a root of g. But then $\mathbb{Q}(\beta)$ is dense in K, so K is the p-adic completion of $\mathbb{Q}(\beta)$. □

4 Dedekind domains

Definition 4.1. A ring R is a **Dedekind domain** if

(i) R is a Noetherian integral domain.

(ii) R is integrally closed (in $\operatorname{Frac} R$).

(iii) Every nonzero prime ideal of R is maximal.

Example 4.2. The ring of integers of a number field is a Dedekind domain, as we will see later. Any PID is a Dedekind domain, and so any DVR is a Dedekind domain.

4.1 Basic properties

Theorem 4.3. *A ring is a DVR iff it is a local Dedekind domain.*

Lemma 4.4. *Let R be a Noetherian ring, and let $0 \neq I \trianglelefteq R$. Then there are nonzero primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r \trianglelefteq R$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq I$.*

Proof. Suppose not. Since R is Noetherian, there is a maximal counterexample I. Since I cannot be prime, choose $x, y \notin I$ such that $xy \in I$. Then

$$I \subsetneq I + (x) \coloneqq I_1 \text{ and } I \subsetneq I + (x) \coloneqq I_2.$$

By maximality of I, find primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s \trianglelefteq R$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq I_1$ and $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq I_2$. But then

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq I_1 I_2 = I + (xy) = I. \#$$

□

Lemma 4.5. *Let R be an integral domain which is integrally closed in its fraction field K, and let $0 \neq I \trianglelefteq R$ be finitely generated. If $x \in K$ satisfies $xI \subseteq I$, then in fact $x \in R$.*

Proof. Let $I = (c_1, \dots, c_n)$. It suffices to show x is integral over R.

Write $I \ni xc_i = \sum_j a_{ij} c_j$ for some $a_{ij} \in R$, and set $B = xI - A \in \mathcal{M}_n(K)$. Then $B\mathbf{c} = \mathbf{0}$ in K^n, so, multiplying by the adjugate, $\det B\mathbf{c} = \mathbf{0}$. Since R is an integral domain, $\det B = 0$. But $\det B$ is a monic polynomial in x with coefficients in R. □

Proof of theorem.
A DVR is clearly both a local ring and a Dedekind domain (as it is a PID).

Conversely, let R be a local Dedekind domain with unique maximal ideal $\mathfrak{m}$. Since we already know R is local, it suffices to show it is a PID.

Step 1: $\mathfrak{m}$ is principal.

Let $0 \neq x \in \mathfrak{m}$. Then $(x) \supseteq \mathfrak{m}^n$ for some $n \geq 1$; let n be minimal, and choose $y \in \mathfrak{m}^{n-1} \setminus (x)$. Set $\pi = x/y \in \operatorname{Frac} R$; then we have

$$y\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (x),$$

so $\pi^{-1}\mathfrak{m} \subseteq R$. If $\pi^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, then, by the last lemma, $\pi^{-1} \in R$, and so $y \in (x)$.$_\#$ Hence $\pi^{-1}\mathfrak{m} = R$, and so $\mathfrak{m} = (\pi)$ is principal. Note that this means $\pi \in R$.

Step 2: R is a PID. Let $0 \neq I \trianglelefteq R$ be prime, and consider the ascending chain

$$I \subseteq \pi^{-1}I \subseteq \pi^{-2}I \subseteq \cdots \subseteq \operatorname{Frac} R.$$

Since $\pi^{-1} \notin R$, each inclusion is strict (otherwise $\pi^{-1}I = I_\#$). Since R is Noetherian, there is some n such that $\pi^{-(n+1)}I \not\subseteq R$.

If $\pi^{-n}I \subseteq \mathfrak{m} = (\pi)$, then $\pi^{-(n+1)}I \subseteq R.$$_\#$ Hence $\pi^{-n}I = R$, and so $I = (\pi^n)$ is principal. □

We can view DVRs as *localisations* of Dedekind domains. Localisations are covered in more generality and detail in Commutative Algebra.

Definition 4.6. Let R be an integral domain, and let $S \subseteq R$ be a multiplicative subset ($1 \in S$ and $x, y \in S \implies xy \in S$) not containing zero. Then the **localisation** $S^{-1}R$ of R wrt S is the ring

$$S^{-1}R = \left\{ \frac{r}{s} \;\middle|\; r \in R, s \in S \right\} \leq \operatorname{Frac} R.$$

If $\mathfrak{p} \trianglelefteq R$ is prime, write $R_\mathfrak{p}$ for the localisation of R wrt $R \setminus \mathfrak{p}$.

Examples 4.7. $\mathfrak{p} = 0 \implies R_\mathfrak{p} = \operatorname{Frac} R$. If $R = \mathbb{Z}$, then $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid (b, p) = 1\}$.

Localisations (of integral domains) are integral domains; if R is Noetherian, then all localisations of R are Noetherian. There is also a bijection

$$\begin{aligned} \{\text{prime ideals of } A \text{ disjoint from } S\} &\longleftrightarrow \{\text{prime ideals of } S^{-1}A\} \\ \mathfrak{p} &\longrightarrow \mathfrak{p}S^{-1}R = S^{-1}\mathfrak{p} \\ \mathfrak{q} \cap A &\longleftarrow \mathfrak{q}. \end{aligned}$$

Corollary 4.8. *Let R be a Dedekind domain, and let $0 \neq \mathfrak{p} \trianglelefteq R$ be prime. Then $R_\mathfrak{p}$ is a DVR.*

Proof. $R_\mathfrak{p}$ is a Noetherian integral domain.

Since prime ideals of R are maximal, the only prime ideal of R disjoint from $R \setminus \mathfrak{p}$ is $\mathfrak{p}$ itself. By the bijection, the only prime (and hence the only maximal) ideal of $R_\mathfrak{p}$ is $\mathfrak{p}R_\mathfrak{p}$. In particular, $R_\mathfrak{p}$ is local.

By the theorem, it now suffices to show that $R_\mathfrak{p}$ is integrally closed in $\operatorname{Frac} R = \operatorname{Frac} R_\mathfrak{p}$. Fix an integral element $x \in \operatorname{Frac} R_\mathfrak{p}$ satisfying the monic polynomial $f \in R_\mathfrak{p}[X]$. Clearing the common denominator $s \notin \mathfrak{p}$ of f, we get the relation

$$sx^n + b_{n-1}x^{n-1} + \dots b_1 x_1 + b_0 = 0 \text{ for some } b_i \in R.$$

Multiplying by s^{n-1}, we get

$$(sx)^n + sb_{n-1}(sx)^{n-1} + \cdots + s^n b_0 = 0,$$

so sx is integral over R, and so $sx \in R$. Hence $x \in R_\mathfrak{p}$. □

We showed earlier that DVRs yield valuations on their fraction fields, so this corollary allows us to define valuations directly from primes.

Definition 4.9. Let R be a Dedekind domain, and let $0 \neq \mathfrak{p} \trianglelefteq R$ be prime. Write $v_\mathfrak{p}$ for the normalised valuation on $K := \operatorname{Frac} R = \operatorname{Frac} R_\mathfrak{p}$ that has valuation ring $R_\mathfrak{p}$.

Example 4.10. Let $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$. Then $v_\mathfrak{p}$ is just the p-adic valuation v_p, with valuation ring $\mathbb{Z}_{(p)}$.

Let $K_\mathfrak{p}$ be the completion with respect to $v_\mathfrak{p}$, and let $\mathcal{O}_{K_\mathfrak{p}}$ be its valuation ring.

Theorem 4.11. *Let R be a Dedekind domain and $0 \neq I \trianglelefteq R$. Then I can be written uniquely as a product of prime ideals in R:*

$$I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \text{ with the } \mathfrak{p}_i \text{ distinct.}$$

The proof requires properties of localisations which will not be proved here; see the Commutative Algebra course.

Proof sketch. We quote the facts

(i) For a ring R and $I, J \trianglelefteq R$, have $I = J$ iff $IR_\mathfrak{p} = JR_\mathfrak{p}$ for all primes $\mathfrak{p} \trianglelefteq R$.

(ii) Suppose R is a Dedekind domain, and $\mathfrak{p}_1, \mathfrak{p}_2 \trianglelefteq R$ are nonzero primes. Then

$$\mathfrak{p}_1 R_{(\mathfrak{p}_2)} = \begin{Bmatrix} R_{(\mathfrak{p}_2)} & \mathfrak{p}_1 \neq \mathfrak{p}_2 \\ \mathfrak{p}_2 R_{(\mathfrak{p}_2)} & \mathfrak{p}_1 = \mathfrak{p}_2 \end{Bmatrix}.$$

We have shown that I contains a product of primes; write

$$\mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_r^{\beta_r} \subseteq I$$

for distinct primes $\mathfrak{p}_i \trianglelefteq R$.

If $\mathfrak{p} \notin \{\mathfrak{p}_i\}$ is some other nonzero prime ideal, then, by fact (ii), we have

$$IR_\mathfrak{p} \supseteq \mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_r^{\beta_r} R_\mathfrak{p} = R_\mathfrak{p}.$$

Also, since localisations are DVRs, we have

$$IR_{(\mathfrak{p}_i)} = (\underbrace{\mathfrak{p}_i R_{(\mathfrak{p}_i)}}_{\mathfrak{m}})^{\alpha_i} = \mathfrak{p}_i^{\alpha_i} R_{\mathfrak{p}_i}$$

for some $0 \leq \alpha_i \leq \beta_i$. By fact (i), we then have the equality $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$.

Since this factorisation is determined by the value of $IR_\mathfrak{p}$ at each prime $\mathfrak{p} \trianglelefteq R$, it must be unique, by unique factorisation in DVRs. □

Proposition 4.12.

(i) $\mathcal{O}_{K_\mathfrak{p}} \cong \varprojlim_n R/\mathfrak{p}^n$

(ii) Any $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ *is a uniformiser of* $\mathcal{O}_{K_\mathfrak{p}}$.

(iii) Let $A \subseteq R$ *be a set of coset representatives of* $R/\mathfrak{p}$. *Every element* $x \in K_\mathfrak{p}$ *can be written uniquely as a Laurent series in* π *with coefficients in* A*:*

$$x = \sum_{i=-k}^{\infty} a_i \pi^i.$$

Proof. We saw earlier that $\mathbb{Z}$ is dense in its valuation ring $\mathbb{Z}_{(p)}$ wrt v_p. The same proof shows R is dense in its valuation ring $R_\mathfrak{p}$ (wrt $v_\mathfrak{p}$). Indeed, for $y \notin \mathfrak{p}$, $(y) + \mathfrak{p}^n = R$, so y has an inverse mod $\mathfrak{p}^n$.

Now, $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$ and $\mathfrak{p}R_\mathfrak{p} \cap R = \mathfrak{p}$. Further, any $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ has $v_\mathfrak{p}(\pi) = 1$. We are done by the argument in the $\mathbb{Z}_p$ case, with π in place of p. □

4.2 Extensions of Dedekind domains

Let L/K be a finite extension of fields. For $x \in L$, recall that the *trace* $\mathrm{Tr}_{L/K}(x)$ of x is the trace of multiplication by x, as a K-linear map.

If L/K is separable of degree n and $\sigma_1, \dots \sigma_n : L \to \overline{K}$ denote the n (algebraic) embeddings of L into an algebraic closure of K, then

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

Lemma 4.13. *Let* L/K *be a finite separable extension of fields. Then the symmetric bilinear form* $(x, y) \to \mathrm{Tr}_{L/K}(xy)$ *on* L *is nondegenerate.*

This bilinear form is called the **trace form**. In fact, we will show on the example sheet that the converse is true: if the trace form is nondegenerate, then L/K is separable.

Proof. Let $n = [L : K]$. By PET, let $L = K(\alpha)$ for some $\alpha \in L$. Let A be the matrix of the trace form with respect to the basis $\{1, \alpha, \dots, \alpha^{n-1}\}$. Now, $A = BB^\top$, where $B_{ij} = \sigma_j(\alpha^{i-1})$. Then B is a Vandermonde matrix in the embeddings $\sigma_j\alpha$, which are distinct by separability, so

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

Hence $\det A = (\det B)^2 \neq 0$. □

For the rest of this section, let $\mathcal{O}_K$ be a Dedekind domain with fraction field K, and let L/K be a finite separable extension. Let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L.

Theorem 4.14. *$\mathcal{O}_L$ is a Dedekind domain.*

Proof. Since $\mathcal{O}_L$ is a subring of the field L, it is an integral domain.

$\mathcal{O}_L$ is Noetherian: Let $(e_1, \dots, e_n)$ be a K-basis for L. Clearing denominators in K, we can assume that $e_i \in \mathcal{O}_L$ for all i. Then let $(f_1, \dots, f_n)$ be the dual basis wrt the trace form, so that $\operatorname{Tr} e_i f_j = \delta_{ij}$. Fix $x \in \mathcal{O}_L$, and write $x = \sum_i \lambda_i f_i$ for some $\lambda_i \in K$. By construction, $\operatorname{Tr}_{L/K}(xe_i) = \lambda_i$, so

$$x = \sum_{i=1}^{n} \operatorname{Tr}_{L/K}(xe_i) f_i$$

Now, each $xe_i \in \mathcal{O}_L$; then $\operatorname{Tr}_{L/K}(xe_i)$ is a sum of elements in $\overline{K}$, each of which is integral over $\mathcal{O}_K$, so $\operatorname{Tr}_{L/K}(xe_i) \in \mathcal{O}_K$. Therefore

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

Since $\mathcal{O}_K$ is Noetherian, $\mathcal{O}_L$ is also Noetherian.

$\mathcal{O}_L$ is integrally closed (in its faction field): We have $\operatorname{Frac} \mathcal{O}_L = L$, and integral closures are integrally closed (exercise).

Every nonzero prime ideal $\mathfrak{P} \trianglelefteq \mathcal{O}_L$ is maximal: Let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$; this is a prime ideal of $\mathcal{O}_K$. Let $0 \neq x \in \mathfrak{P} \trianglelefteq \mathcal{O}_L$; then x satisfies a relation

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0 \text{ for some } a_i \in \mathcal{O}_K;$$

in particular, $a_0 \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, so $\mathfrak{p} \neq 0$.

It remains to show $\mathfrak{P}$ is maximal. Indeed, we have an inclusion $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$. We showed earlier that $\mathcal{O}_L$ is a finitely-generated $\mathcal{O}_K$ module; this means $\mathcal{O}_L/\mathfrak{P}$ is a finite-dimensional vector space over $\mathcal{O}_K/\mathfrak{P}$. But $\mathcal{O}_L/\mathfrak{P}$ is also an integral domain, so it is in fact a field (apply rank-nullity to $y \to zy$). Hence $\mathfrak{P}$ is maximal. □

In fact, this theorem holds without the separability assumption, but the proof is harder.

Corollary 4.15. *The ring of integers of a number field is a Dedekind domain.*

Suppose that, in fact, $\mathcal{O}_K$ is the ring of integers of a number field, and let $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ be a nonzero prime. Set $N_\mathfrak{p} = \#|\mathcal{O}_K/\mathfrak{p}|$; by convention, we normalise $|\cdot|_\mathfrak{p}$ by

$$|\cdot|_\mathfrak{p} \coloneqq N_\mathfrak{p}^{-v_p(\cdot)}.$$

Lemma 4.16. *Let $0 \neq x \in \mathcal{O}_K$. Then*

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

Proof. By definition, $x(\mathcal{O}_K)_\mathfrak{p} = (\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p})^{v_p(x)}$. The lemma then follows from the fact that $I = J$ iff $I(\mathcal{O}_K)_\mathfrak{p} = J(\mathcal{O}_K)_\mathfrak{p}$ for all primes $\mathfrak{p}$. □

Fix a nonzero prime $\mathfrak{p} \trianglelefteq \mathcal{O}_K$. Note that $\mathcal{O}_K$ is *not* necessarily the valuation ring of K with respect to $\mathfrak{p}$ — that's the localisation $(\mathcal{O}_K)_\mathfrak{p}$. However, this notation is reasonable as $\mathcal{O}_K$ is dense in the valuation ring.

Now, $\mathfrak{p}\mathcal{O}_L \subsetneq \mathcal{O}_L$ (this is a general commutative algebra fact). Therefore we can factor $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_k^{e_k}$, with $e_i > 0$ for all i; then say $\mathfrak{P} \mid \mathfrak{p}$ if $\mathfrak{P} = \mathfrak{P}_i$ for some i. We will show on the example sheet that $\mathfrak{P} \mid \mathfrak{p}$ iff $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$.

Theorem 4.17. *Take $\mathfrak{p}$ as above. The absolute values on L extending $|\cdot|_\mathfrak{p}$ are, up to equivalence, precisely $|\cdot|_{\mathfrak{P}_1}, \dots, |\cdot|_{\mathfrak{P}_r}$.*

Proof. Fix $0 \neq x \in \mathcal{O}_K$. By the last lemma, $v_{\mathfrak{P}_i}(x) = e_i v_\mathfrak{p}(x)$. Hence each $|\cdot|_{\mathfrak{P}_i}$ *does* extend $|\cdot|_\mathfrak{p}$, up to equivalence (scaling by e_i).

Conversely, suppose $|\cdot|$ is an absolute value on L extending $|\cdot|_\mathfrak{p}$. Since $|\cdot|$ is bounded on $\mathbb{Z}$, it is non-Archimedean. Let $R \leq L$ be the valuation ring for $|\cdot|$. Then $\mathcal{O}_K \subseteq R$; then R is integrally closed in L, so in fact $\mathcal{O}_L \subseteq R$. Define

$$\mathfrak{P} = \{x \in \mathcal{O}_L \mid |x| < 1\} = \mathcal{O}_L \cap \mathfrak{m}_R;$$

then $\mathfrak{P} \trianglelefteq \mathcal{O}_L$ is prime. Note that $\mathfrak{P}$ is nonzero since $0 \neq \mathfrak{p} \subseteq \mathfrak{P}$.

Now, $(\mathcal{O}_L)_\mathfrak{P} \subseteq R$: indeed, if $s \in \mathcal{O}_L \setminus \mathfrak{P}$, then $|s| = 1$. Since $(\mathcal{O}_L)_\mathfrak{P}$ is a DVR, it is a maximal subring of its fraction field, so in fact $(\mathcal{O}_L)_\mathfrak{P} = R$. Hence $|\cdot| \sim |\cdot|_\mathfrak{P}$.

Then, since $|\cdot|$ extends $|\cdot|_\mathfrak{p}$, we have that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, and therefore

$$\mathfrak{P} \supseteq (\mathfrak{P} \cap \mathcal{O}_K)\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L,$$

that is, $\mathfrak{P} \mid \mathfrak{p}$. □

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

Corollary 4.18. *Let K be a number field with ring of integers $\mathcal{O}_K$. An absolute value $|\cdot|$ on K is equivalent to one of the following:*

(i) $|\cdot|_\mathfrak{p}$ for some nonzero prime $\mathfrak{p} \trianglelefteq \mathcal{O}_K$.

(ii) $|\cdot|_\sigma$ for some embedding $\sigma : K \hookrightarrow \mathbb{C}$.

Proof. Suppose $|\cdot|$ is non-Archimedean. Then its restriction to $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p, so, by the last theorem, $|\cdot| \sim |\cdot|_\mathfrak{p}$ for some prime $\mathfrak{p} \mid (p)$ in $\mathcal{O}_K$.

The Archimedean case is an exercise. □

4.2.1 Completions of extensions

Let $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ and $\mathfrak{P} \trianglelefteq \mathcal{O}_L$ be nonzero primes with $\mathfrak{P} \mid \mathfrak{p}$. Write $K_\mathfrak{p}$ and $L_\mathfrak{P}$ for the respective completions of K and L wrt $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{P}$. We want to understand the structure of such completions.

We have towers of extensions $L_\mathfrak{P}/L/K$ and $L_\mathfrak{P}/K_\mathfrak{p}/K$. We therefore have a natural product map

$$\begin{aligned} \pi_\mathfrak{P} : L \otimes_K K_\mathfrak{p} &\longrightarrow L_\mathfrak{P} \\ l \otimes \hat{k} &\longrightarrow l\hat{k} \end{aligned}$$

Lemma 4.19.

(i) $\pi_\mathfrak{P} : L \otimes_K K_\mathfrak{p} \to L_\mathfrak{P}$ *is surjective.*

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

Proof. Let $\operatorname{im} \pi_\mathfrak{P} \coloneqq M = LK_\mathfrak{p} \subseteq L_\mathfrak{P}$. Write $L = K(\alpha)$; then $M = K_\mathfrak{p}(\alpha)$, so $M/K_\mathfrak{p}$ is finite of degree at most $[L : K]$.

Then M is complete; indeed, it is a finite extension of a complete valued field. But $L \subseteq M \subseteq L_\mathfrak{P}$, so in fact $M = L_\mathfrak{P}$. □

Note that the structure of $LK_\mathfrak{p}$ depends on the way L and $K_\mathfrak{p}$ embed into $L_\mathfrak{P}$, so $[L_\mathfrak{P} : K_\mathfrak{p}]$ can vary with $\mathfrak{P}$. We will see precisely how in the next section.

Lemma 4.20 (Chinese Remainder Theorem)**.** *Let R be a ring, and let $I_1, \ldots, I_n \trianglelefteq R$ be pairwise comaximal ideas (that is, $I_i + I_j = R$ for $i \neq j$). Then $\bigcap_j I_j = \prod_j I_j \coloneqq I$, and*

$$R/I \cong \prod_j R/I_j$$

Proof. Example sheet. □

Theorem 4.21. *The natural map $L \otimes_K K_\mathfrak{p} \to \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$, given componentwise by products $\pi_\mathfrak{P}$, is an isomorphism.*

Proof. Write $L = K(\alpha)$, and let $f \in K[X]$ be the minimal polynomial of α. Over $K_\mathfrak{p}$, let f factor into irreducibles $f_1 \ldots f_r$, which are distinct by separability. Then $L \cong K[X]/(f)$, so

$$L \otimes_K K_\mathfrak{p} \cong K_\mathfrak{p}[X]/(f) \cong \prod_{i=1}^{r} K_\mathfrak{p}[X]/(f_i)$$

by CRT. Set $L_i \coloneqq K_\mathfrak{p}[X]/(f_i)$; these are finite extensions of $K_\mathfrak{p}$.

Now, L_i contains $K_\mathfrak{p}$, but it also contains (a copy of) L: map

$$L \cong K[X]/(f) \hookrightarrow K_\mathfrak{p}[X]/(f_i) = L_i.$$

Moreover, L is dense in L_i since we can approximate elements of $K_\mathfrak{p}[X]/(f_i)$ coefficient-wise by elements of $K[X]/(f)$, since K is dense in $K_\mathfrak{p}$.

The theorem then follows from the following three claims:

(i) $L_i \cong_{LK_\mathfrak{P}} L_\mathfrak{p}$ for some prime divisor $\mathfrak{P} \mid \mathfrak{p}$ in $\mathcal{O}_L$.

(ii) Each divisor $\mathfrak{P}$ appears at most once.

(iii) Each divisor $\mathfrak{P}$ appears at least once.

(i): Since $L_i/K_\mathfrak{p}$ is finite, there is a unique absolute value $|\cdot|$ on L_i extending $|\cdot|_\mathfrak{p}$ on $K_\mathfrak{p}$. By the last theorem, $|\cdot|\big|_L \sim |\cdot|_\mathfrak{P}$ for some prime $\mathfrak{P} \mid \mathfrak{p}$. Since L is dense in L_i, which is complete, the absolute values are in fact equivalent on all L_i, so $L_i \cong L_\mathfrak{P}$.

(ii): Suppose $L_i \cong L_j$ are isomorphic by a map preserving L and $K_\mathfrak{p}$. But we can view the isomorphism as a map $\varphi : K_\mathfrak{p}[X]/(f_i) \to K_\mathfrak{p}[X]/(f_j)$ preserving $K_\mathfrak{p}[X]$, so in fact $f_i = f_j$.

(iii): We just showed in a previous lemma that the natural map $\pi_\mathfrak{P} : L \otimes_K K_\mathfrak{P} \to L_\mathfrak{P}$ is surjective for any $\mathfrak{P} \mid \mathfrak{p}$. Since $L_\mathfrak{P}$ is a field, $\pi_\mathfrak{P}$ factors through some L_i; by surjectivity, $L_i \cong L_\mathfrak{P}$. □

The proof relates the factorisation of a prime $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ in $\mathcal{O}_L$ to the factorisation of the minimal polynomial of a primitive element of L/K in $K_\mathfrak{p}$.

Example 4.22. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$; and let $f = X^2 + 1$. Now, $f(X) \equiv (X + 2)(X + 3) \bmod 5$. By Hensel's lemma, $\sqrt{-1} \in \mathbb{Q}_5$, so f splits in $\mathbb{Q}_5$, and so (5) splits in $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$.

Corollary 4.23. *Let $x \in L$. Then*

$$N_{L/K}(x) = \prod_{\substack{\mathfrak{P} \trianglelefteq \mathcal{O}_L \\ \mathfrak{P} \mid \mathfrak{p}}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(x).$$

Proof. Fix a prime $\mathfrak{p}$ of K, and let the primes over it be $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$; let $\mathcal{B}_i$ be a $K_\mathfrak{p}$-basis for $L_{\mathfrak{P}_i}$. By the last theorem, $\mathcal{B} = \bigcup_i \mathcal{B}_i$ is a $K_\mathfrak{p}$-basis for $L \otimes_K K_\mathfrak{p}$. Let $\operatorname{mult} x$ be the K-linear map given by multiplication by x.

Let $[\operatorname{mult} x]_\mathcal{B}$ (resp. $[\operatorname{mult} x]_{\mathcal{B}_i}$) be the matrix for $\operatorname{mult} x$ on $L \otimes_K K_\mathfrak{p}$ (resp. $L_{\mathfrak{P}_i}$) wrt the basis $\mathcal{B}$ (resp. $\mathcal{B}_i$).

By construction, we can write

$$[\operatorname{mult} x]_\mathcal{B} = \begin{pmatrix} [\operatorname{mult} x]_{\mathcal{B}_1} & & \\ & \ddots & \\ & & [\operatorname{mult} x]_{\mathcal{B}_r} \end{pmatrix}.$$

Since extending the scalars from K to $K_\mathfrak{p}$ doesn't change $\det \operatorname{mult} x$, we get the result:

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

□

4.3 Decomposition groups

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$, and write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$, for distinct primes $\mathfrak{P}_i \trianglelefteq \mathcal{O}_L$ and $e_i > 0$. Note that $\mathfrak{p} \subseteq \mathcal{O}_K \cap \mathfrak{P}_i \subsetneq \mathcal{O}_K$, so, by maximality of $\mathfrak{p}$, we have $\mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_K$. We showed the converse earlier, so the primes $\mathfrak{P}_i$ dividing $\mathfrak{p}\mathcal{O}_L$ are exactly those lying over $\mathfrak{p}$.

Definition 4.24. Call e_i the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$; say $\mathfrak{p}$ **ramifies** in L if some $e_i > 1$.

Example 4.25. Let $\mathcal{O}_K = \mathbb{C}[t]$, and $\mathcal{O}_L = \mathbb{C}[T]$, with $\mathcal{O}_K \to \mathcal{O}_L$ by $t \to T^n$. Then $t\mathcal{O}_L = (T)^n$, so the ramification index of (T) over (t) is n.

Geometrically, this corresponds to the degree n covering of Riemann surfaces $\mathbb{C} \to \mathbb{C}$ by $z \to z^n$; this is ramified (as an analytic map) at 0 with index n.

Definition 4.26. $f_i \coloneqq [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is the **residue class degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Alternatively, write $e_{\mathfrak{P}_i/\mathfrak{p}}$ for e_i and $f_{\mathfrak{P}_i/\mathfrak{p}}$ for f_i.

Theorem 4.27.

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

Proof. We use the following facts about localisation (left as an exercise):

(1) $(\mathcal{O}_L)_\mathfrak{p}$ is the integral closure of $(\mathcal{O}_K)_\mathfrak{p}$ in L.

(2) $\mathfrak{p}(\mathcal{O}_L)_\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}(\mathcal{O}_L)_\mathfrak{p}$.

(3) $(\mathcal{O}_L)_\mathfrak{p}/\mathfrak{P}_i(\mathcal{O}_L)_\mathfrak{p} \cong \mathcal{O}_L/\mathfrak{P}_i$, and $(\mathcal{O}_K)_\mathfrak{p}/\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$.

In particular, (2) and (3) imply that the e_i and f_i stay the same after localisation at $\mathfrak{p}$. We may therefore reduce to the case where $\mathcal{O}_K$ is a DVR, and hence a PID.

By CRT, we have

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

We count dimensions of both sides as $k = \mathcal{O}_K/\mathfrak{p}$-vector spaces.

RHS: For each i, we have an ascending chain of k-vector spaces

$$0 \le \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \le \dots \le \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \le \mathcal{O}_L/\mathfrak{P}_i^{e_i}.$$

Therefore $\dim_k \mathcal{O}_L/\mathfrak{P}_i^{e_i}$ is the sum of the dimensions of the quotients in the chain, that is,

$$\dim_k \mathcal{O}_L/\mathfrak{P}_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_k \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}.$$

But each quotient $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is an $\mathcal{O}_L/\mathfrak{P}_i$-module, generated by any $x \in \mathfrak{P}_i^j \setminus \mathfrak{P}_i^{j+1}$ (to see this, localise at $\mathfrak{P}$). Hence $\dim_k \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1} = f_i$, and so

$$\dim_k \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{P}_i^{e_i} = \sum_{i=1}^{r} e_i f_i.$$

LHS: Observe that $\mathcal{O}_L$ is torsion-free. By the structure theorem, $\mathcal{O}_L$ is a free module over $\mathcal{O}_K$ of rank $n = [L : K]$. Hence $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (k)^n$ as k-modules, and so

$$\dim_k \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n.$$

This gives the result. □

This theorem has a geometric analogue: the valency theorem for maps of compact Riemann surfaces:

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

In fact, since, by a deep theorem, compact Riemann surfaces arise as algebraic curves, these theorems generalise to the same thing!

Definition 4.28. Let L/K be an extension of complete discretely valued fields with normalised valuations v_L and v_K and uniformisers π_L and π_K. The **ramification index** e of the extension is $e \coloneqq e_{L/K} = v_L(\pi_K)$, so that $\pi_K\mathcal{O}_L = \pi_L^e\mathcal{O}_L$. The **residue class degree** is $f \coloneqq f_{L/K} = [k_L : k]$.

Let $\mathfrak{P} \mid \mathfrak{p}$. The two definitions of e and f are related: indeed, uniformisers and residue fields do not change when taking completions, so $e_{\mathfrak{P}/\mathfrak{p}} = e_{L_\mathfrak{P}/K_\mathfrak{p}}$ and $f_{\mathfrak{P}/\mathfrak{p}} = f_{L_\mathfrak{P}/K_\mathfrak{p}}$.

Corollary 4.29. *Let L/K be a finite separable extension of complete discretely valued fields. Then $[L : K] = e_{L/K}f_{L/K}$.*

Proof. The valuation ring $\mathcal{O}_K$ is a DVR (and so a Dedekind domain); it has integral closure $\mathcal{O}_L$ in L, and this is also a DVR. We can therefore apply the previous theorem with the unique primes $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ and $\mathfrak{P} \trianglelefteq \mathcal{O}_L$; we are done by the above discussion. □

In fact, this holds even when L/K is not separable (see the note after Theorem 4.14).

Suppose further that L/K is Galois. Then, for $\sigma \in \mathrm{Gal}(L/K)$, have $\sigma(\mathfrak{P}_i) \cap \mathcal{O}_K = \mathfrak{p}$, and so $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some j. Hence $\mathrm{Gal}(L/K)$ acts on $\{\mathfrak{P}_1 \dots \mathfrak{P}_r\}$.

Proposition 4.30. *The action of* $\mathrm{Gal}(L/K)$ *on the $\mathfrak{P}_i$ is transitive.*

Proof. Suppose not; then there are some $i \neq j$ such that $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_j$ for all $\sigma \in \mathrm{Gal}(L/K)$. By CRT, choose $x \in \mathcal{O}_L$ such that $x \in \mathfrak{P}_i$ but $x \notin \sigma(\mathfrak{P}_j)$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Then

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathcal{O}_K \cap \mathfrak{P}_i = \mathfrak{p} \supseteq \mathfrak{P}_j;$$

since $\mathfrak{P}_j$ is prime, there is some $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(x) \in \mathfrak{P}_j$. But then $x \in \tau^{-1}\mathfrak{P}_j$.# □

Corollary 4.31. *We have $e \coloneqq e_1 = \dots = e_r$ and $f \coloneqq f_1 = \dots = f_r$. Hence we have $n = efr$.*

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

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

By transitivity of the action of $\mathrm{Gal}(L/K)$ and unique factorisation, the e_i are all equal.

Similarly, σ descends to give an isomorphism $\mathcal{O}_L/\mathfrak{P}_i \cong \mathcal{O}_L/\sigma(\mathfrak{P}_i)$, so the f_i are equal (again by transitivity).

Then the last theorem gives $n = efr$. □

Definition 4.32. The **decomposition group** at a prime $\mathfrak{P} \trianglelefteq \mathcal{O}_L$ is its stabiliser $G_{\mathfrak{P}} = \mathrm{Stab}_{\mathrm{Gal}(L/K)} \mathfrak{P}$.

Let $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ be prime, with $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}$. By transitivity of the Galois action, $G_{\mathfrak{P}}$ and $G_{\mathfrak{P}'}$ are conjugate.

Proposition 4.33.

(i) *$L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois.*

(ii) *There is a natural restriction map* $\mathrm{res} : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$ *which is injective, with image* $G_{\mathfrak{P}}$.

Proof.

(i) Let L be the splitting field of $f \in K[X]$. But then $L_{\mathfrak{P}}$ is the splitting field of $f \in K_{\mathfrak{p}}[X]$, since it is also generated by its roots.

(ii) Let $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$; then $\sigma L = L$. Hence $\mathrm{res}(\sigma) = \sigma|_L$ is well-defined. Since L is dense in $\mathcal{L}_{\mathfrak{P}}$ and σ is continuous (in fact, isometric) wrt the absolute value, res is injective. Now, for all $x \in L_{\mathfrak{P}}$, $|\sigma(x)|_{\mathfrak{P}} = |x|_{\mathfrak{P}}$, so $\sigma(\mathfrak{P}) = \mathfrak{P}$, and so $\sigma|_L \in G_{\mathfrak{P}}$.

It remains to show res surjects onto $G_{\mathfrak{P}}$; it suffices to show that

$$[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef = |G_{\mathfrak{P}}|.$$

Indeed, $|G_{\mathfrak{P}}| = ef$ by orbit-stabiliser: $\mathrm{Gal}(L/K) = [L : K] = efr$, and the orbits have size r by transitivity of the Galois action. Then $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef$ by the last corollary, since e and f doesn't change when we take completions.

□

4.4 Different and discriminant

Let L/K be a degree-n extension of algebraic number fields.

Definition 4.34. Let $x_1, \dots, x_n \in L$. Define their **discriminant**

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

where the σ_i are the n embeddings $L \hookrightarrow \bar{K}$.

If $y_i = \sum_j a_{ij}x_j$ for some $a_{ij} \in K$, then

$$\Delta(\mathbf{y}) = (\det(a_{ij}))^2\Delta(\mathbf{x}).$$

Also, if $x_1, \dots, x_n \in \mathcal{O}_L$, then $\Delta(\mathbf{x}) \in \mathcal{O}_K$.

Lemma 4.35. *Let k be a perfect field, and let R be a finite k-algebra. The trace form $(,) : R \times R \to k$ is nondegenerate iff $R \cong k_1 \times \cdots \times k_n$ for some fields k_i, where each extension k_i/k is finite (and hence separable).*

Proof. Example sheet. □

Theorem 4.36. *Let $0 \neq \mathfrak{p} \trianglelefteq \mathcal{O}_K$ be prime.*

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

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

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$, where the $\mathfrak{P}_i$ are distinct primes with each $e_i > 0$. By CRT,

$$R \coloneqq \frac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L} \cong \prod_i \frac{\mathcal{O}_L}{\mathfrak{P}_i^{e_i}}.$$

Note that the residue field k of K is finite, and so perfect.

(i) If $\mathfrak{p}$ is ramified, some $e_i > 1$, and so R has nilpotents. Therefore R cannot be isomorphic to a product of fields.

Fix $x_1, \dots, x_n \in \mathcal{O}_L$. Applying the previous lemma to the k-algebra R, the trace form is degenerate, so $\Delta(\bar{\mathbf{x}}) = 0$, where $\bar{x}_i$ is the image of x_i under the quotient. Lifting to $\mathcal{O}_L$, he have that $\Delta(\mathbf{x}) \in \mathfrak{p}$.

(ii) If $\mathfrak{p}$ is unramified, then R is isomorphic to a product of finite extensions of k, so the trace form is nondegenerate, and so $\Delta(\bar{\mathbf{x}}) \neq 0$ for any k-basis $(\bar{x}_1, \dots, \bar{x}_n)$ of R. Lifting these $\bar{x}_i$, we get elements $x_1, \dots, x_n \in \mathcal{O}_L$ such that $\Delta(\mathbf{x}) \notin \mathfrak{p}$.

□

Definition 4.37. The **discriminant** of the extension L/K is the ideal $d_{L/K} \trianglelefteq \mathcal{O}_K$ generated by the $\Delta(\mathbf{x})$:

$$d_{L/K} = (\{\Delta(\mathbf{x}) \mid x_1, \dots, x_n \in \mathcal{O}_L\}).$$

Corollary 4.38. *A nonzero prime $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ ramifies in L iff $\mathfrak{p} \mid d_{L/K}$. In particular, only finitely many primes ramify.*

In the case where $K = \mathbb{Q}$, we recover the integer *discriminant* $d_{L/\mathbb{Q}} = (\operatorname{disc} L)$.

Definition 4.39. The **inverse different** of L/K is

$$\mathcal{D}_{L/K}^{-1} = \{y \in L \mid \operatorname{Tr}_{L/K}(xy) \in \mathcal{O}_K \text{ for all } x \in \mathcal{O}_L\}.$$

Lemma 4.40. *$\mathcal{D}_{L/K}^{-1}$ is a fractional ideal.*

Proof. Let $x_1, \dots, x_n \in \mathcal{O}_L$ be a K-basis for L. Set

$$d \coloneqq \Delta(x_1, \dots, x_n) = \det\bigl(\mathrm{Tr}_{L/K}(x_i x_j)\bigr) \in \mathcal{O}_K.$$

For $y \in \mathcal{D}_{L/K}^{-1}$, we have $y = \sum_j \lambda_j x_j$ for some $\lambda_j \in K$.

Then

$$\mathrm{Tr}_{L/K}(yx_i) = \sum_i \lambda_i \,\mathrm{Tr}_{L/K}(x_i x_j) \coloneqq \sum_i \lambda_i A_{ij}.$$

Multiplying by $\operatorname{Adj} A \in \mathcal{M}_n(\mathcal{O}_K)$, we have

$$d \cdot \vec{\lambda} = \operatorname{Adj} A \cdot \mathrm{Tr}_{L/K}(y\mathbf{x}) \in \mathcal{O}_K,$$

so $\lambda_i \in \frac{1}{d}\mathcal{O}_K$, and so $y \in \frac{1}{d}\mathcal{O}_L$. Hence $\mathcal{D}_{L/K}^{-1} \subseteq \frac{1}{d}\mathcal{O}_L$, and so it is a fractional ideal. □

Definition 4.41. The **different** of L/K is $\mathcal{D}_{L/K}$, the inverse of $\mathcal{D}_{L/K}^{-1}$.

Let $\mathcal{J}_K$ and $\mathcal{J}_L$ be the groups of fractional ideals of $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. By unique factorisation, these are freely generated over their respective sets of nonzero prime ideals. Let $N_{L/K} : \mathcal{J}_L \to \mathcal{J}_K$ map $\mathfrak{P} \to \mathfrak{p}^f$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ and $f = f_{\mathfrak{P}/\mathfrak{p}}$ is the residue class degree.

We also have an inclusion $K^\times \to \mathcal{J}_K$ by $a \to (a)$. Then the element-wise and ideal-wise norms commute with respect to this inclusion; that is, the diagram below commutes:

$$\begin{array}{ccc} L^\times & \hookrightarrow & \mathcal{J}_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K^\times & \hookrightarrow & \mathcal{J}_K \end{array}$$

Indeed, for $x \in L^\times$, we have $v_{\mathfrak{p}}(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x)) = f_{\mathfrak{P}/\mathfrak{p}} v_{\mathfrak{P}}(x)$; we are done by unique prime factorisation.

Theorem 4.42. $N_{L/K}(\mathcal{D}_{L/K}) = d_{L/K}$.

Sketch proof. First, assume $\mathcal{O}_K$ and $\mathcal{O}_L$ are PIDs. Let $x_1, \dots, x_n$ be an $\mathcal{O}_K$-basis for $\mathcal{O}_L$, and let $y_1, \dots, y_n$ be a dual basis wrt the trace form. Then $y_1, \dots, y_n$ is a basis for $\mathcal{D}_{L/K}^{-1}$.

Let $\sigma_1, \dots, \sigma_n : L \hookrightarrow \bar{K}$ be the distinct embeddings of L. Then

$$\sum_i \sigma_i(x_j)\sigma_i(y_k) = \mathrm{Tr}(x_j y_k) = \delta_{ij},$$

but $\Delta(\mathbf{x}) = (\det(\sigma_i(x_j)))^2$, so $\Delta(\mathbf{x})\Delta(\mathbf{y}) = 1$.

Since $\mathcal{O}_L$ is a PID, we have $\mathcal{D}_{L/K}^{-1} = (\beta)$ for some $\beta \in \mathcal{O}_L$. Then

$$d_{L/K}^{-1} = (\Delta(\mathbf{x}))^{-1} = (\Delta(\mathbf{y})) = (\Delta(\beta x_1, \dots, \beta x_n)) = N_{L/K}(\beta)^2(\Delta(\mathbf{x})),$$

where the second equality follows from the fact that change of basis matrices are invertible. Hence $d_{L/K}^{-1} = N_{L/K}(\beta)^2 d_{L/K}$, and so

$$N_{L/K}(\beta) = N_{L/K}(\mathcal{D}_{L/K}^{-1}) = d_{L/K}^{-1}.$$

In general, localise at each prime $\mathfrak{p}$ of $\mathcal{O}_K$, and use the fact that

$$\mathcal{D}_{L/K}(\mathcal{O}_K)_{\mathfrak{p}} = \mathcal{D}_{(\mathcal{O}_L)_{\mathfrak{P}}/(\mathcal{O}_K)_{\mathfrak{p}}}$$

and

$$d_{L/K}(\mathcal{O}_K)_{\mathfrak{p}} = d_{(\mathcal{O}_L)_{\mathfrak{P}}/(\mathcal{O}_K)_{\mathfrak{p}}}.$$

The details are omitted. □

Theorem 4.43. *If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, where α has monic minimal polynomial $g \in \mathcal{O}_K[X]$, then*

$$\mathcal{D}_{L/K} = (g'(\alpha)).$$

Proof. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of g. Write

$$g(X) = (X - \alpha)(X^{n-1} + \beta_{n-2}X^{n-2} + \cdots + \beta_0)$$

for some $\beta_{n-2}, \ldots, \beta_0 \in \mathcal{O}_L$. Set $\beta_{n-1} = 1$.

Claim:

$$\sum_{i=1}^{n} \frac{g(X)}{X - \alpha_i} \cdot \frac{\alpha_i^r}{g'(\alpha_i)} = X^r \text{ for } 0 \leq r \leq n-1.$$

Indeed, the difference is a polynomial of degree strictly less than n vanishing at each $\alpha_1, \ldots, \alpha_n$.

Comparing coefficients, we have

$$\mathrm{Tr}_{L/K}\, \alpha^r \frac{\beta_s}{g'(\alpha)} = \delta_{rs}.$$

Now, $1, \alpha, \ldots, \alpha^{n-1}$ is a $\mathcal{O}_K$-basis for $\mathcal{O}_L$, so $\mathcal{D}_{L/K}^{-1}$ has an $\mathcal{O}_K$-basis

$$\frac{\beta_0}{g'(\alpha)}, \ldots, \frac{\beta_{n-1}}{g'(\alpha)}.$$

Since $b_{n-1} = 1$, $\mathcal{D}_{L/K}^{-1} = (1/g'(\alpha))$, and so $\mathcal{D}_{L/K} = (g'(\alpha))$. □

Let $\mathfrak{P}$ be a prime in $\mathcal{O}_L$, and let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. We define the **local different** $\mathcal{D}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ in the same way as we define $\mathcal{D}_{L/K}$, using the rings $\mathcal{O}_{K_{\mathfrak{p}}}$ and $\mathcal{O}_{L_{\mathfrak{p}}}$.

Theorem 4.44.

$$\mathcal{D}_{L/K} = \prod_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \mathfrak{P} \mid \mathfrak{p}}} \mathcal{D}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}.$$

Note that, since only ramified primes have nontrivial local differents, the product on the right is finite.

Proof.
Fact: Let $x \in L$, and fix a prime $\mathfrak{p}$ of K. Then

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

by the same argument as for the norm earlier.

Claim:

$$\mathcal{D}_{L/K} \subseteq \prod_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \mathfrak{P}|\mathfrak{p}}} \mathcal{D}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}.$$

Suppose $x \in \mathcal{D}^{-1}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ for every $\mathfrak{P} \mid \mathfrak{p}$. For any $y \in \mathcal{O}_L \subseteq \mathcal{O}_{L_{\mathfrak{P}}}$, we have $\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy) \in \mathcal{O}_{K_{\mathfrak{p}}}$. By $(\star)$, $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K$, and so $x \in \mathcal{D}^{-1}_{L/K}$. Therefore

$$\prod_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \mathfrak{P}|\mathfrak{p}}} \mathcal{D}^{-1}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = \bigcap_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \mathfrak{P}|\mathfrak{p}}} \mathcal{D}^{-1}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} \subseteq \mathcal{D}^{-1}_{L/K}.$$

Claim:

$$\mathcal{D}_{L/K} \supseteq \prod_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \mathfrak{P}|\mathfrak{p}}} \mathcal{D}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}.$$

Fix $\mathfrak{P} \mid \mathfrak{p}$, and define $r(\mathfrak{P}) = v_{\mathfrak{P}}(\mathcal{D}_{L/K})$ and $s(\mathfrak{P}) = v_{\mathfrak{P}}(\mathcal{D}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}})$. By unique factorisation, it suffices to show that $r(\mathfrak{P}) \leq s(\mathfrak{P})$.

Find $x \in \mathfrak{P}^{-r(\mathfrak{P})} \setminus \mathfrak{P}^{-r(\mathfrak{P})+1}$. Then $v_{\mathfrak{P}}(x) = -r(\mathfrak{P})$, and $v_{\mathfrak{P}'}(x) \geq 0$ for $\mathfrak{P}' \neq \mathfrak{P}$; that is, $x \in \mathcal{D}^{-1}_{L/K}$ and $x \in \mathcal{D}^{-1}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}$. Fix $y \in \mathcal{O}_{L_{\mathfrak{P}}}$; by $(\star)$, we have

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

so $x \in \mathcal{D}^{-1}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$; that is, $-r(\mathfrak{P}) = v_{\mathfrak{P}}(x) \geq -s(\mathfrak{P})$. □

Corollary 4.45.

$$d_{L/K} = \prod_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \mathfrak{P}|\mathfrak{p}}} d_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}.$$

Proof. Apply $N_{L/K}$. □

5 Extensions of local fields

From now on, let L/K be a finite separable extension of non-Archimedean local fields (we'll always assume local fields are non-Archimedean from now on); use notation as before. We have shown that, in this case,

$$[L : K] = e_{L/K} f_{L/K}.$$

Lemma 5.1 (Tower law)**.** *Let $M/L/K$ be a tower of finite, separable extensions of non-Archimedean local fields. We have*

(i) $f_{M/K} = f_{M/L} f_{L/K}$.

(ii) $e_{M/K} = e_{M/L} e_{L/K}$.

Proof.

(i)
$$f_{M/K} = [k_M : k] = [k_M : k_L][k_L : k] = f_{M/L} f_{L/K}$$

(ii) Follows from (i) and $[L : K] = e_{L/K} f_{L/K}$.

□

5.1 Unramified and totally ramified extensions

Definition 5.2. L/K is **unramified** if $e_{L/K} = 1$ (equivalently, $f_{L/K} = [L : K]$), ramified if $e_{L/K} > 1$, and **totally ramified** if $e_{L/K} = [L : K]$ (equivalently, $f_{L/K} = 1$).

Theorem 5.3. *There is an intermediate extension $L/K_0/K$ such that*

(i) K_0/K *is unramified.*

(ii) L/K_0 *is totally ramified.*

Proof. Let $k = \mathbb{F}_q$; then $k_L = \mathbb{F}_{q^f}$, where $f := f_{L/K}$. Let $m = q^f - 1$, and let $[\cdot] : \mathbb{F}_{q^f} \to L$ be the Teichmüller lift for L. Let $\mathbb{F}_{q^f}^\times = \langle \alpha \rangle$, and let $\zeta_m = [\alpha]$; set $K_0 = K(\zeta_m)$.

Now, ζ_m is a primitive m^{th} root of unity, so the extension K_0/K is cyclotomic and therefore Galois. Let $\mathcal{O}_{K_0}$ have maximal ideal $\mathfrak{m}_0$, and let the residue field be k_0. Then $k_0 = \mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^f}$; since in any case $k_0 \subseteq k_L$, in fact $k_0 = k_L$.

Let $\mathrm{res} : \mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_0/k)$ be the natural restriction map. Let $\sigma \in \mathrm{Gal}(K_0/K)$; then σ is determined by $\sigma(\zeta_m)$. We have $\sigma(\zeta_m) = \zeta_m$ iff $\sigma(\zeta_m) \equiv \zeta_m \bmod \mathfrak{m}_0$, since there is a bijection (by Hensel's lemma) between m^{th} roots of unity of K_0 and k_0. This means res is injective.

Hence
$$[K_0 : K] = |\,\mathrm{Gal}(K_0/K)| \leq |\,\mathrm{Gal}(k_0/k)| = f_{K_0/K},$$
so in fact $[K_0 : K] = f_{K_0/K}$, that is, res is an isomorphism and K_0/K is unramified. But $k_0 = k_L$, so $f_{L/K} = f_{K_0/K} = [K_0 : K]$, and $f_{L/K_0} = 1$; then L/K_0 is totally ramified. □

Theorem 5.4. *Let K be a local field, and write $k = \mathbb{F}_q$. For each $n \geq 1$, there is a unique unramified extension L/K of degree n. Moreover, L/K is Galois and the natural map* $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ *is an isomorphism.*

In particular, $\mathrm{Gal}(L/K) = \langle \mathrm{Frob}_{L/K} \rangle$ *is cyclic and generated by a lift of the Frobenius automorphism; that is, for every $x \in \mathcal{O}_L$,*

$$\mathrm{Frob}_{L/K}(x) \equiv x^q \bmod \mathfrak{m}_L.$$

Proof. Take $L = K(\zeta_m)$, where $m = q^n - 1$ and ζ_m is a primitive m^{th} root of unity. As in the last theorem, the natural restriction on Galois groups induces an isomorphism

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle x \to x^q \rangle.$$

Hence, in particular, the generator of $\mathrm{Gal}(L/K)$ descends to the *Frobenius*

$$\mathrm{Frob}_q : x \to x^q.$$

It remains to prove uniqueness. Indeed, if L/K is an unramified extension of degree n, then we can find a Teichmüller lift $\zeta \in L$ of a generator of $k_L^\times$. By Hensel's lemma, ζ is a primitive m^{th} root of unity, where $m = q^{f_{L/K}} - 1$. Since L/K is unramified,

$$[K(\zeta) : K] = f_{L/K} = n,$$

so $L = K(\zeta)$. □

Definition 5.5. Suppose L/K is Galois. The **inertia subgroup** is

$$I_{L/K} = \ker \mathrm{res} \leq \mathrm{Gal}(L/K).$$

Since $|\mathrm{Gal}(k_L/k)| = f_{L/K}$ and $e_{L/K} f_{L/K} = [L : K]$, we have $|I_{L/K}| = e_{L/K}$. By construction, $I_{L/K} = \mathrm{Gal}(L/K_0)$.

Definition 5.6. 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 $i \geq 1$ and $v_K(a_0) = 1$.

Note that, by Eisenstein's criterion (generalised to prime ideals), Eisenstein polynomials are irreducible.

Theorem 5.7.

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

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

Proof.

(i) We have $[L : K] = e_{L/K} \coloneqq e$. Let the minimal polynomial of π_L be

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in \mathcal{O}_K[X];$$

note $m \leq e$. For $i < m$, we have

$$v_L(a_i \pi_L^i) = v_L(a_i) + i = e \cdot v_K(a_i) + i \equiv i \bmod e;$$

in particular, each term has a distinct valuation. Now,

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

so

$$e \geq m = v_L(\pi_L^m) = \min_{0 \leq i < m} (i + e \cdot v_K(a_i)).$$

Therefore $v_K(a_i) \geq 1$ for all i, and so $v_K(a_0) = 1$, and $m = e$. Thus f is Eisenstein.

We have $L = K(\pi_L)$. For $y \in L$, write

$$y = \sum_{i=0}^{e-1} b_i \pi_L^i \text{ for some } b_i \in K.$$

Then

$$v_L(y) = \min_{0 \leq i < e} (i + e \cdot v_K(b_i)),$$

so $y \in \mathcal{O}_L$ (that is, $v_L(y) \geq 0$) iff $v_K(b_i) \geq 0$ for all i, 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 Eisenstein, and let $L = K(\alpha)$ where α is a root of f. Also set $e \coloneqq e_{L/K}$.

Then $v_L(a_i) \geq e$ and $v_L(a_0) = e$. If $v_L(\alpha) \leq 0$, we have

$$v_L(\alpha^n) = n v_L(\alpha) < (n-1)e + n v_L(\alpha) \leq v_L\left(-\sum_{i=0}^{n-1} a_i \alpha^i\right). \#$$

Hence $v_L(\alpha) > 0$.

For $i \neq 0$, $v_L(a_i \alpha^i) > e = v_L(a_0)$, so

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

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

□

5.2 Structure of units

Suppose K is a finite extension of $\mathbb{Q}_p$ (that is, suppose K has mixed characteristic). Let $e \coloneqq e_{K/\mathbb{Q}_p}$.

Theorem 5.8. *If $r > \frac{e}{p-1}$, then*

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

converges on $\pi^r \mathcal{O}_K$, and induces an isomorphism

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

Proof. From the example sheet, we have

$$v_K(n!) = e \cdot v_p(n!) = \frac{e(n - s_p(n))}{p-1} \leq \frac{e(n-1)}{p-1}.$$

where $s_p(n)$ is the sum of the p-adic digits of n (and so at least 1). For $x \in \pi^r \mathcal{O}_K$ and $n \geq 1$,

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

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

Similarly, consider $\log(1+x) : 1 + \pi^r \mathcal{O}_K \to \pi^r \mathcal{O}_K$ given by the power series

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

We can check convergence as before quite easily.

As power series over $\mathbb{Q}$, we have the identities $\exp(X+Y) = \exp(X)\exp(Y)$, $\exp(\log(1+X)) = 1+X$, and $\log(\exp(X)) = X$. Hence we have an isomorphism $\exp : (\pi^r \mathcal{O}_K, +) \xrightarrow{\simeq} (1 + \pi^r \mathcal{O}_K, \times)$. □

We cannot do this in equal characteristic as we cannot divide by $n!$ for $n > \operatorname{char} K$.

Now let K be any local field; let $U_K = \mathcal{O}_K^\times$ be its unit group.

Definition 5.9. Let $U_K^{(0)} = U_K$; for $k \geq 1$, let $U_K^{(s)} = (1 + \pi^s \mathcal{O}_K, \times)$ be the s^{th} **unit group**.

We have a descending chain

$$U_K^{(0)} \supseteq U_K^{(1)} \supseteq U_K^{(2)} \dots$$

Proposition 5.10.

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

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

Proof.

(i) The natural quotient $U_K^{(0)} = \mathcal{O}_K^\times \to k^\times$ given by reduction mod π is surjective, and has kernel $1 + \pi\mathcal{O}_K = U_K^{(1)}$.

(ii) Map

$$\begin{aligned} f : U_K^{(s)} &\longrightarrow k \\ 1 + \pi^s x &\longrightarrow x \bmod \pi \end{aligned}$$

We have

$$(1+\pi^s x)(1+\pi^s y) = 1 + \pi^s \underbrace{(x+y+\pi^s xy)}_{\equiv x+y \bmod \pi},$$

so f is a surjective group homomorphism, with $\ker f = U_K^{s+1}$.

□

Corollary 5.11. *Let $[K:\mathbb{Q}_p] < \infty$. Then there is a finite index subgroup of $\mathcal{O}_K^\times$ which is isomorphic to $(\mathcal{O}_K, +)$.*

Proof. Let $r > \frac{e}{p-1}$; we have seen that $U_K^{(r)} \cong (\mathcal{O}_K, +)$. But, by the last proposition, the successive quotients in the descending chain $\left(U_K^{(n)}\right)$ are finite, and so $U_K^{(r)}$ has finite index in $\mathcal{O}_K^\times = U_K^{(0)}$. □

Again, this doesn't hold in equal characteristic.

Example 5.12. In $\mathbb{Z}_p$ with $p > 2$, we have $e = 1$, so we can take $r = 1$. Then

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

explicitly, we map $x \to (x \bmod p, x/[x \bmod p])$.

When $p = 2$, we have to take $r = 2$. Then

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

explicitly, map $x \to (x \bmod 4, x/\varepsilon(x))$, where

$$\varepsilon(x) = \begin{Bmatrix} +1 & x \equiv 1 \bmod 4 \\ -1 & x \equiv 3 \bmod 4 \end{Bmatrix}.$$

This gives another proof that

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

5.3 Higher ramification groups

Let L/K be Galois.

Definition 5.13. For $s \in (-1, \infty)$, the s^{th} **ramification group** of L/K is

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

Examples 5.14.

1. $G_{-1}(L/K) = \mathrm{Gal}(L/K)$
2. $G_0(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \bmod \pi \ \forall x \in \mathcal{O}_L\} = I_{L/K}$

Note that, for $s \geq 0$,

$$G_s(L/K) = \ker\left(\mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{O}_L/\pi_L^{s+1}\mathcal{O}_L) \trianglelefteq \mathrm{Gal}(L/K)\right),$$

so, factoring the restrictions through each other, we have a descending chain of normal subgroups

$$\mathrm{Gal}(L/K) = G_{-1} \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots$$

Note that G_s only changes at integers; it is defined at non-integer reals so that it can be used to define *upper numbering*, which we will meet in the last (non-examinable) section.

Theorem 5.15.

(i) For $s \geq 0$,

$$G_s(L/K) = \{\sigma \in G_0 \mid v_L(\sigma(\pi_L) - \pi_L) \geq s+1\}.$$

(ii)

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

(iii) Let $s \geq 0$. Then there is an injective group homomorphism

$$\begin{aligned} \frac{G_s}{G_{s+1}} &\hookrightarrow \frac{U_L^{(s)}}{U_L^{(s+1)}} \\ \sigma &\longrightarrow \frac{\sigma(\pi_L)}{\pi_L} \end{aligned}$$

which is independent of the choice of π_L.

Proof. Note that these statements are equivalent to the same statement over L/K_0, since $G_0 = I_{L/K} = \mathrm{Gal}(L/K_0)$. We may therefore assume wlog that L/K is totally ramified.

(i) Since L/K is totally ramified, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Suppose $v_L(\sigma(\pi_L) - \pi_L) \geq s+1$.

Fix $x \in \mathcal{O}_L$; then $x = f(\pi_L)$ for some $f \in \mathcal{O}_K[X]$. Then

$$\sigma(x) - x = \sigma(f(\pi_L)) - f(\pi_L) = f(\sigma(\pi_L)) - f(\pi_L) = (\sigma(\pi_L) - \pi_L)g(\pi_L),$$

for some $g \in \mathcal{O}_K[X]$. Therefore

$$v(\sigma(x) - x) = v_L(\sigma(\pi_L) - \pi_L) + \underbrace{v_L(g(\pi_L))}_{\geq 0} \geq s+1,$$

so $\sigma \in G_s$.

(ii) Suppose $1 \neq \sigma \in \mathrm{Gal}(L/K)$. Since $L = K(\pi_L)$, we have $\sigma(\pi_L) \neq \pi_L$, and so $v_L(\sigma(\pi_L) - \pi_L) \coloneqq N < \infty$, Therefore $\sigma \notin G_s$ for $s > N$.

(iii) For $\sigma \in G_s$, by definition

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

Hence

$$\frac{\sigma(\pi_L)}{\pi_L} \in 1 + \pi_L^s \mathcal{O}_L = U_L^{(s)}.$$

We need to show that the map

$$\begin{aligned} \varphi : G_s &\longrightarrow \frac{U_L^{(s)}}{U_L^{(s+1)}} \\ \sigma &\longrightarrow \frac{\sigma(\pi_L)}{\pi_L} \end{aligned}$$

is a group homomorphism with kernel G_{s+1}.

For $\sigma, \tau \in G_s$, let $\tau(\pi_L) = u\pi_L$ for some $u \in \mathcal{O}_L^\times$. Then

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

But $\sigma(u) \in u + \pi_L^{s+1}\mathcal{O}_L$, so $\sigma(u)/u \in 1 + \pi_L^{s+1}\mathcal{O}_L = U_L^{s+1}$. Hence φ is a group homomorphism. Further, by (i)

$$\ker \varphi = \{\sigma \in G_s \mid \sigma(\pi_L) \equiv \pi_L \bmod \pi_L^{s+1} = G_{s+1}\}.$$

It remains to check independence. If $\pi_L' = u\pi_L$ is another uniformiser, with $a \in \mathcal{O}_K^\times$, then

$$\frac{\sigma(\pi_L')}{\pi_L'} = \frac{\sigma(u)}{u} \cdot \frac{\sigma(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \bmod U_L^{s+1}.$$

□

Corollary 5.16. $\mathrm{Gal}(L/K)$ *is solvable.*

Proof. Let $s \in \mathbb{Z}_{\geq -1}$. Then we have shown (in particular) that

$$\frac{G_s}{G_{s+1}} \cong \text{a subgroup of } \begin{cases} \mathrm{Gal}(k_L/k) & s = -1 \\ (k_L^\times, \times) & s = 0 \\ (k_L, +) & s \geq 1 \end{cases}$$

Therefore G_s/G_{s+1} is abelian, and hence solvable. □

Let $\operatorname{char} k = p$. Then $|G_0/G_1|$ is coprime to p, and $|G_1| = p^n$ for some $n \geq 0$. Since also $G_1 \trianglelefteq G_0$, G_1 is the unique Sylow-p subgroup of $G_0 = I_{L/K}$.

Definition 5.17. The group G_1 is the **wild inertia group**, and G_0/G_1 is the **tame quotient**.

Definition 5.18. Now suppose L/K is finite separable (not necessarily Galois). Then L/K is **tamely ramified** if $\operatorname{char} K \nmid e_{L/K}$; otherwise it is **wildly ramified**.

In the case that L/K is Galois, it is tamely ramified iff its wild inertia group G_1 is trivial.

Theorem 5.19. *Let $[K : \mathbb{Q}_p] < \infty$ and L/K finite; let $\mathcal{D}_{L/K} = (\pi_L)^{\delta(L/K)}$. Then $\delta(L/K) \geq e_{L/K} - 1$, with equality iff L/K is tamely ramified.*

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

Proof. We show on the example sheet that $\mathcal{D}_{L/K} = \mathcal{D}_{L/K_0}\mathcal{D}_{K_0/K}$. Therefore it suffices to check the unramified and totally ramified cases.

Suppose L/K is unramified. Then $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$ such that $k_L = k(\bar{\alpha})$. Let $g \in \mathcal{O}_K[X]$ be the minimal polynomial of α. Now, $[L : K] = [k_L : k]$, so $\bar{g} \in k[X]$ is the minimal polynomial of $\bar{\alpha}$. Since $\bar{g}$ is irreducible, it is separable, and so $g'(\alpha) \not\equiv 0 \bmod \pi_L$. Hence $\mathcal{D}_{L/K} = (g'(\alpha)) = \mathcal{O}_L$.

Suppose L/K is totally ramified. Then $[L : K] = e$, and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, where π_L has an Eisenstein minimal polynomial

$$g(X) = X^e + \sum_{i=0}^{e-1} a_i X^i \in \mathcal{O}_K[X].$$

Then

$$g'(\pi_L) = \underbrace{e\pi_L^{e-1}}_{v_L \geq e-1} + \sum_{i=1}^{e-1} \underbrace{i a_i \pi_L^{i-1}}_{v_L \geq e}.$$

Hence $v_L(g'(\pi_L)) \geq e - 1$, with equality iff $p \nmid e$. □

Corollary 5.20. *Let L/K be an extension of local fields. Let $\mathfrak{P} \trianglelefteq \mathcal{O}_L$ and $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Then $e(\mathfrak{P}/\mathfrak{p}) > 1$ iff $\mathfrak{P} \mid \mathcal{D}_{L/K}$.*

Proof. We have

$$\mathcal{D}_{L/K} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}.$$

Using $e(\mathfrak{P}/\mathfrak{p}) = e_{L_\mathfrak{P}/K_\mathfrak{p}}$, we are done by the last theorem. □

Example 5.21. Let $K = \mathbb{Q}_p$, and let $\xi_{p^n} \in \mathbb{Q}_p$ be a primitive p^nth root of unity. Let $L = \mathbb{Q}_p(\xi_{p^n})$; then the p^nth cyclotomic polynomial is

$$\varphi_{p^n}(X) = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + 1 \in \mathbb{Z}_p[X].$$

We show on the example sheet that

- $\varphi_{p^n}(X)$ is irreducible (and so is the minimal polynomial of ξ_{p^n}).
- $L/\mathbb{Q}_p$ has degree $p^{n-1}(p-1)$, and is Galois and totally ramified.
- $\pi := \xi_{p^n} - 1$ is a uniformiser of $\mathcal{O}_L$. Therefore $\mathcal{O}_L = \mathbb{Z}_p[\xi_{p^n} - 1] = \mathbb{Z}_p[\xi_{p^n}]$.

- $\mathrm{Gal}(L/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ is abelian, with the isomorphism mapping $(\xi_{p^n} \to \xi_{p^n}^m) \to m$.

Then

$$v_L(\sigma_m(\pi) - \pi) = v_L(\xi_{p^n}^m - \xi_{p^n}) = v_L(\xi_{p^n}^{m-1} - 1).$$

Let k be the maximal power such that $p^k \mid m-1$; then $\xi_{p^n}^{m-1}$ is a primitive p^{n-k}th root of unity, and so $\xi_{p^n}^{m-1} - 1$ is a uniformiser in $L' = \mathbb{Q}_p(\xi_{p^n}^{m-1})$. Hence

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

Hence $\sigma_m \in G_i$ iff $p^k \geq i+1$. Thus

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

These G_i look like the quotients of the unit groups. In fact, they are, since we can replace $\mathbb{Z}$ with $\mathbb{Z}_p$ in the quotients above without changing the groups. Local class field theory explains this phenomenon.

6 Local class field theory

6.1 Infinite Galois extensions

Let L/K be an algebraic extension of fields, *not necessarily finite*.

Definition 6.1. For $\alpha \in L$, let $f_\alpha \in K[X]$ be its minimal polynomial over K. Then L/K is **separable** if each $f_\alpha \in K[X]$ is separable, **normal** if each f_α splits in L, and **Galois** if it is separable and normal. If L/K is Galois, write $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$.

We want to generalise the Galois correspondence to infinite extensions.

Definition 6.2. Let $(I, \leq)$ be a poset. Say I is a **directed set** if, for all $i, j \in I$, there is some $k \in I$ such that $i \leq k$ and $j \leq k$.

Examples 6.3.

1. Any total order (e.g. $(\mathbb{N}, \leq)$) is a directed set.
2. $(\mathbb{N}_+, |)$ is a directed set.

Definition 6.4. Let $(I, \leq)$ be a directed set, and take an I-indexed collection of groups (or sets, or rings,...) $(G_i \mid i \in I)$, together with homomorphisms $\varphi_{ij} : G_j \to G_i$ for $i \leq j$, such that, for $i \leq j \leq k$,

$$\varphi_{ik} = \varphi_{ij}\varphi_{jk} \text{ and } \varphi_{ii} = 1.$$

Then $((G_i), (\varphi_{ij}))$ form an **inverse system**.

The **inverse limit** of the inverse system is then

$$\varprojlim_{i \in I} G_i = \left\{ (g_i) \in \prod_{i \in I} G_i \;\middle|\; \varphi_{ij}(g_j) = g_i \right\}.$$

Taking $I = \mathbb{N}$ with the natural order, we recover our earlier definition of an inverse limit.

We have projection maps $\psi_j : \varprojlim_{i \in I} G_i \to G_j$.

Definition 6.5. Suppose each G_i is finite. Then the **profinite topology** on $\varprojlim_{i \in I} G_i$ is the weakest topology making all the ψ_j continuous, wrt the discrete topology on the G_j.

Proposition 6.6. *Let L/K be Galois. Then*

(i) The set

$$I = \{F \mid L/F/K,\ F/K \text{ finite Galois}\}$$

forms an inverse system under inclusion.

(ii) For $F \subseteq F' \in I$, there is a restriction map

$$\mathrm{res}_{F,F'} : \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K),$$

and the natural map $\mathrm{Gal}(L/K) \to \varprojlim_I \mathrm{Gal}(F/K)$ is an isomorphism.

Example 6.7. Let $K = \mathbb{F}_q$ and $L = \bar{\mathbb{F}}_q$ its algebraic closure. We have a bijection

$$\begin{aligned} \{F/K \text{ finite Galois}\} &\longleftrightarrow \mathbb{N}_{\geq 1} \\ \mathbb{F}_{q^n} &\longleftrightarrow n \end{aligned}$$

With $\mathbb{F}q^m \subseteq \mathbb{F}_{q^n}$ iff $m \mid n$.

We also know that the Galois groups and restriction maps are

$$\begin{array}{ccccc} \mathrm{Frob}_q & & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & \xrightarrow{\text{res}} & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) & & \mathrm{Frob}_q \\ \updownarrow & & \downarrow\simeq & & \simeq\downarrow & & \updownarrow \\ 1 & & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\text{mod}} & \mathbb{Z}/m\mathbb{Z} & & 1 \end{array}$$

Hence we get an isomorphism

$$\begin{aligned} \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) &\xleftrightarrow{\simeq} \varprojlim_{(\mathbb{N}_{\geq 1}, |)} \mathbb{Z}/n\mathbb{Z} \coloneqq \hat{\mathbb{Z}} \\ \mathrm{Frob}_q &\longleftrightarrow 1 \end{aligned}$$

$\hat{\mathbb{Z}}$ is called the **projective completion** of $\mathbb{Z}$. Note that the subgroup $\langle \mathrm{Frob}_q \rangle \leq \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ corresponds to the inclusion

$$\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

Theorem 6.8 (Fundamental theorem of Galois theory)**.** *Let L/K be Galois, and endow $\mathrm{Gal}(L/K)$ with the profinite topology from $\varprojlim \mathrm{Gal}(F/K)$. Then there is an order-reversing bijection*

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

Moreover, F/K is finite iff $\mathrm{Gal}(L/F)$ is open, and F/K is Galois iff $\mathrm{Gal}(F/K) \trianglelefteq \mathrm{Gal}(L/K)$. In the latter case, $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.

Proof. Example sheet. □

6.2 The Weil group

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

Definition 6.9. L/K is **unramified** if every finite subextension F/K is unramified, and **totally ramified** if every finite subextension F/K is totally ramified.

Proposition 6.10. *Suppose L/K is unramified. Then L/K is Galois and*

$$\mathrm{Gal}(L/K) \xrightarrow[res]{\simeq} \mathrm{Gal}(k_L/k).$$

Proof. Since every finite subextension F/K is unramified, it is Galois, and hence normal and separable. Therefore L/K is normal and separable, and hence Galois.

Moreover, we have the following commutative diagram

$$\begin{array}{ccccc}
\mathrm{Gal}(L/K) & & \xrightarrow{\qquad\qquad\mathrm{res}\qquad\qquad} & & \mathrm{Gal}(k_L/k) \\
\downarrow\simeq & & & & \downarrow\simeq \\
\varprojlim_{\substack{L/F/K \\ F/K \text{ finite}}} \mathrm{Gal}(F/K) & \xrightarrow{\simeq} & \varprojlim_{\substack{L/F/K \\ F/K \text{ finite}}} \mathrm{Gal}(k_F/k) & \xleftrightarrow{\simeq} & \varprojlim_{\substack{k_L/k'/k \\ k'/k \text{ finite}}} \mathrm{Gal}(k'/k)
\end{array}$$

The isomorphisms along the bottom follow from the theory of finite unramified extensions. □

Suppose L_1/K and L_2/K are finite unramified extensions. We show on the example sheet that L_1L_2/K is still unramified. By Zorn's lemma, there is a maximal unramified subextension $L/K_0/K$.

Suppose L/K is Galois; then there is a surjection

$$\mathrm{res} : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K_0/K) \cong \mathrm{Gal}(k_L/k).$$

Note that L/K_0 is totally ramified, and so $k_L = k_{K_0}$. As before, let $I_{L/K} = \ker(\mathrm{res})$ be the **inertia subgroup**.

Let $\mathrm{Frob}_{k_L/k} \in \mathrm{Gal}(k_L/k)$ be the Frobenius $x \to x^{|k|}$.

Definition 6.11. The **Weil group** $W(L/K) \leq \mathrm{Gal}(L/K)$ is

$$W(L/K) = \mathrm{res}^{-1}\langle \mathrm{Frob}_{k_L/k} \rangle \leq \mathrm{Gal}(L/K).$$

If k_L/k is finite, then $\langle \mathrm{Frob}_{k_L/k} \rangle = \mathrm{Gal}(k_L/k)$, so $W(L/K) = \mathrm{Gal}(L/K)$. Otherwise, $\langle \mathrm{Frob}_{k_L/k} \rangle < \mathrm{Gal}(k_L/k)$, so $W(L/K) < \mathrm{Gal}(L/K)$ is a strict subgroup (e.g. $\mathbb{Z} < \hat{\mathbb{Z}}$ in the last example).

We have also have the following commutative diagram, in which the rows are exact.

$$\begin{array}{ccccc} I_{L/K} & \hookrightarrow & W(L/K) & \twoheadrightarrow & \langle \mathrm{Frob}_{k_L/k} \rangle \\ \| & & \downarrow & & \downarrow \\ I_{L/K} & \hookrightarrow & \mathrm{Gal}(L/K) & \twoheadrightarrow & \mathrm{Gal}(k_L/k) \end{array}$$

Definition 6.12. We endow $W(L/K)$ with the weakest topology such that

(1) $W(L/K)$ is a topological group (that is, multiplication and inversion are continuous).

(2) $I_{L/K} \leq W(L/K)$ is an open subgroup when equipped with the profinite topology (that is, the subspace topology from $\mathrm{Gal}(L/K)$).

Equivalently, the open sets of $W(L/K)$ are the translates of open subsets of $I(L/K)$ by elements of $W(L/K)$.

Note that this topology is in general *stronger* than the profinite/subspace topology induced by $\mathrm{Gal}(L/K)$. For example, $I_{L/K} \subseteq W(L/K)$ is not open in the subspace topology.

Proposition 6.13. *Let L/K be Galois.*

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

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

(iii) If F/K is a finite Galois subextension, then $W(L/K)/W(L/F) \cong \mathrm{Gal}(F/K)$.

Proof. (i) $W(L/K)$ is dense in $\mathrm{Gal}(L/K)$ iff, for all finite Galois subextensions F/K, $W(L/K)$ meets every coset of $\mathrm{Gal}(L/F)$; that is, iff $W(L/K)$ surjects onto $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K)$.

Indeed, consider the following diagram, whose rows are exact.

$$\begin{array}{ccccc} I_{L/K} & \hookrightarrow & W(L/K) & \twoheadrightarrow & \langle \mathrm{Frob}_{k_L/k} \rangle \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} \\ I_{F/K} & \hookrightarrow & \mathrm{Gal}(F/K) & \twoheadrightarrow & \mathrm{Gal}(k_F/k) \end{array}$$

We want to show b is surjective.

Indeed, let K_0/K be the maximal unramified subextension. Then $K_0 \cap F$ is the maximal unramified subextension of F/K. Hence

$$\mathrm{res} : \mathrm{Gal}(L/K_0) \twoheadrightarrow \mathrm{Gal}(K_0F/K_0) \cong \mathrm{Gal}(F/K_0 \cap F),$$

so a is surjective. Since $\mathrm{Gal}(k_F/k)$ is finite, it is generated by $\mathrm{Frob}_{k_F/k}$, so c is surjective. By a diagram chase, b is also surjective.

(ii) Consider the commutative diagram below.

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

Let $\sigma \in \mathrm{Gal}(L/F)$. Then $\sigma \in W(L/F)$ iff $\sigma|_{k_L} \in \langle \mathrm{Fr}_{k_L/k_F} \rangle$; since $\langle \mathrm{Fr}_{k_L/k_F} \rangle = \mathrm{Gal}(k_L/k_F) \cap \langle \mathrm{Fr}_{k_L/k} \rangle$, this is equivalent to $\sigma|_{k_L} \in \langle \mathrm{Fr}_{k_L/k} \rangle$. Hence $\sigma \in W(L/F)$ iff $\sigma \in W(L/K)$.

(iii) By the last two parts,

$$\frac{W(L/K)}{W(L/F)} =_{(ii)} \frac{W(L/K)}{W(L/K) \cap \mathrm{Gal}(L/F)} = \frac{W(L/K)\,\mathrm{Gal}(L/F)}{\mathrm{Gal}(L/F)} =_{(i)} \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)} = \mathrm{Gal}(F/K).$$

□

6.3 Statements of local class field theory

Let K be a local field.

Definition 6.14. An extension L/K is **abelian** if it is Galois and $\mathrm{Gal}(L/K)$ is abelian.

If L_1/K and L_2/K are abelian, then L_1L_2/K is abelian, so there is a maximal abelian extension K^{ab} in K^{sep}/K. If $L_1 \cap L_2 = K$, there is a canonical isomorphism $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Example 6.15. Let K^{un} be the maximal unramified extension in K^{sep}/K. Then

$$K^{\mathrm{un}} = \bigcup (\text{unramified extensions of } K) = \bigcup_{m=1}^{\infty} K(\xi_{q^m-1});$$

if $|k| = q$, then $k_{K^{\mathrm{un}}} = \bar{\mathbb{F}}_q$. Then

$$\mathrm{Gal}(K^{\mathrm{un}}) \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$$

is abelian, so K^{un} is abelian, and hence $K^{\mathrm{un}} \subseteq K^{\mathrm{ab}}$.

We have the usual exact sequence

$$I_{K^{\mathrm{ab}}/K} \hookrightarrow W(K^{\mathrm{ab}}/K) \twoheadrightarrow \langle \mathrm{Fr}_{K^{\mathrm{ab}}/K} \rangle$$

Theorem 6.16 (Local Artin reciprocity)**.**

*(1) Recall that we equipped $W(K^{ab}/K)$ with a special topology. There is a unique isomorphism of topological groups, called the **Artin map**,*

$$\mathrm{Art}_K : K^\times \xrightarrow{\simeq} W(K^{ab}/K)$$

satisfying the following properties:

(i) Let π be a uniformiser of K. Then

$$\mathrm{Art}_K(\pi)|_{K^{un}} = \mathrm{Fr}_{K^{un}/K}\,.$$

(ii) Let $K^{ab}/L/K$ be a finite subextension. Then

$$\mathrm{Art}_K(N_{L/K}(L^\times))|_L = 1.$$

(2) Let L/K be finite. Then Art_K induces an isomorphism

$$\frac{K^\times}{N_{L/K}(L^\times)} \cong \frac{W(K^{ab}/K)}{W(K^{ab}/L)} \cong \mathrm{Gal}(L/K).$$

This is a special case of the *local Langlands correspondence*. The (local) Artin map here is used to characterise the Artin map of *global* class field theory.

Let L/K be finite; then $N_{L/K}(L^\times)$ is an open finite-index subgroup of $K^\times$. In fact, the converse holds.

Theorem 6.17 (Existence theorem)**.** *Let $H \leq K^\times$ be an open finite-index subgroup. Then there is an extension L/K such that $N_{L/K}(L^\times) = H$.*

In particular, Art_K induces an inclusion-reversing bijection of posets

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

Theorem 6.18 (Norm functoriality)**.** *Let L/K be a finite separable extension. The square below commutes.*

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

Proposition 6.19. *Let L/K be a finite abelian extension of degree n. Then*

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

Proof. For $x \in L^\times$, we have

$$v_K(N_{L/K}(x)) = e_{L/K} v_L(N_{L/K}(x)) = f_{L/K} v_L(x).$$

Hence v_K gives a surjection

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

with kernel

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

By local Artin reciprocity,

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

so $[\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)] = e_{L/K}$. □

Corollary 6.20. *An extension L/K is finite iff $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$.*

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

Our goal for the rest of the course is to construct the Artin map. We will first look at the case of $K = \mathbb{Q}_p$.

Recall that

$$\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_{m=1}^{\infty} \mathbb{Q}_p(\xi_{p^m-1}) = \bigcup_{p\nmid m} \mathbb{Q}_p(\xi_m),$$

and that $\mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p$ is a totally ramified extension of degree $p^{n-1}(p-1)$, with an isomorphism

$$\theta_n : \mathrm{Gal}(\mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p) \xrightarrow{\simeq} (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

For $n \geq m \geq 1$, ww have the following commutative diagram.

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

Set $\mathbb{Q}_p(\xi_\infty) = \bigcup_{n=1}^{\infty} \mathbb{Q}_p(\xi_n)$. The extension $\mathbb{Q}_p(\xi_\infty)/\mathbb{Q}_p$ is Galois, and we have a natural isomorphism

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

In particular, $\mathbb{Q}_p(\xi_\infty)$ is abelian.

Since $\mathbb{Q}_p(\xi_\infty)$ is totally ramified, $\mathbb{Q}_p(\xi_\infty) \cap \mathbb{Q}_p^{\mathrm{un}} = \mathbb{Q}$, so we have a natural isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p(\xi_\infty)\mathbb{Q}_p^{\mathrm{un}}/\mathbb{Q}_p) \xrightarrow{\simeq} \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

Theorem 6.21 (Local Kroenecker-Weber)**.**

$$\mathbb{Q}_p^{ab} = \mathbb{Q}_p^{un}\mathbb{Q}_p(\xi_{p^\infty}).$$

Proof. Omitted. □

We construct $\mathrm{Art}_{\mathbb{Q}_p}$ as follows: we have an isomorphism $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$ by $p^n u \leftrightarrow (n, u)$. Then set

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

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

6.5 Construction of Art_K

Since composita of totally ramified extensions are not in general totally ramified, we have no maximal (abelian) totally ramified extension. In the case of $\mathbb{Q}_p$, we had a 'nice' totally ramified extension $\mathbb{Q}_p(\zeta_{p^\infty})$ which we could compose with $\mathbb{Q}_p^{\mathrm{un}}$ to get $\mathbb{Q}_p^{\mathrm{ab}}$. In general, we must construct something similar.

Let K be a local field and π a uniformiser of K. For $n \geq 1$, we will construct $K_{\pi,n}$, a totally ramified Galois extension satisfying

(i) $K \subseteq K_{\pi,1} \subseteq K_{\pi,2} \subseteq \dots$

(ii) For $n \geq m \geq 1$, we have a commutative diagram

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

(iii) Setting

$$K_{\pi,\infty} = \bigcup_{n=1}^{\infty} K_{\pi,n},$$

we have $K^{\mathrm{ab}} = K^{\mathrm{un}} K_{\pi,\infty}$.

The maps ψ_n in (ii) glue together to give an isomorphism

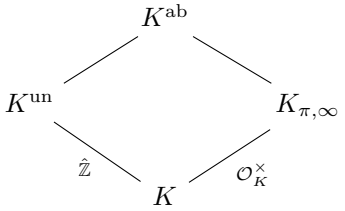
$$\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \xrightarrow{\simeq} \varprojlim_n \frac{\mathcal{O}_K}{U_K^{(n)}} \cong \mathcal{O}_K^\times.$$

Then define Art_K by

$$\begin{aligned} K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times &\to \mathrm{Gal}(K^{\mathrm{un}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \pi^n u \leftrightarrow (n,u) &\to (\mathrm{Fr}_{\mathrm{K^{un}/K}}{}^n, \psi^{-1}(u^{-1})) \end{aligned}$$

Again, the image lies in $W(K^{\mathrm{ab}}/K)$.

We have a lattice



Note that, although $K_{\pi,\infty}$ and the isomorphism $K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$ depend on π, Art_K in fact turns out to be independent of this choice.

It remains to construct the extensions $K_{\pi,n}$.

7 Lubin-Tate theory

7.1 Formal group laws

Definition 7.1. Let R be a ring. A (1-dimensional, commutative) **group law** over R is a power series $F(X,Y) \in R[\![X,Y]\!]$ satisfying

1. $F(X,Y) \equiv X + Y \bmod \deg 2$.
2. Associativity: $F(X,F(Y,Z)) = F(F(X,Y),Z)$.
3. Commutativity: $F(X,Y) = F(Y,X)$.

Examples 7.2.

(i) The **formal additive group** $\hat{\mathbb{G}}_a(X,Y) = X + Y$.

(ii) The **formal multiplicative group** $\hat{\mathbb{G}}_m(X,Y) = X + Y + XY$.

We don't need an 'inverse' axiom, since it follows from the others:

Lemma 7.3. *Let F be a formal group law over a ring R.*

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

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

Proof. Exercise. □

Let K be a complete non-Archimedean valued field, and let F be a formal group law over $\mathcal{O}_K$. For any $x, y \in \mathfrak{m}_K$, the series $F(x,y)$ converges in $\mathfrak{m}_K$. Define

$$x \cdot_F y = F(x,y);$$

then $(\mathfrak{m}_K, \cdot)$ is an abelian group.

Example 7.4. Consider $\hat{\mathbb{G}}_m$ on $\mathbb{Z}_p$. For $x, y \in p\mathbb{Z}_p$, we have $x \cdot_{\hat{\mathbb{G}}_m} y \coloneqq x + y + xy \in p\mathbb{Z}_p$; then

$$\begin{aligned}(p\mathbb{Z}_p, \hat{\mathbb{G}}_m) &\xrightarrow{\simeq} (1 + p\mathbb{Z}_p, \cdot)\\ x &\longrightarrow 1 + x.\end{aligned}$$

Definition 7.5. Let F, G be formal group laws over R. A **homomorphism** $f : F \to G$ is an element $f \in XR[\![X]\!]$ such that

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

Write $\mathrm{End}_R(F)$ for the set of homomorphisms $F \to F$.

A homomorphism $f : F \to G$ is an **isomorphism** if $\exists g : G \to F$ such that $f(g(X)) = X$ and $g(f(X)) = X$.

Proposition 7.6. *Let R be a $\mathbb{Q}$-algebra. There is an isomorphism of formal group laws*

$$\exp : \hat{\mathbb{G}}_a \xrightarrow{\simeq} \hat{\mathbb{G}}_m,$$

where

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

Proof. Define

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

Then the following equalities of formal power series hold:

$$\begin{aligned}\log(\exp(X)) &= \exp(\log(X)) = X\\ \exp\Big(\hat{\mathbb{G}}_a(X,Y)\Big) &= \hat{\mathbb{G}}_m(\exp(X), \exp(Y)).\end{aligned}$$

□

Lemma 7.7. $\mathrm{End}_R(F)$ *is a (not necessarily commutative) ring, with*

$$(f +_R g)(X) = F(f(X), g(X))$$

and

$$f \cdot_R g = f \circ g.$$

Proof. We will check the ring operations are well defined. The rest comprises similar computations.

Let $f, g \in \mathrm{End}_R(F)$. Then

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

so $f +_R g \in \mathrm{End}_R(F)$; also,

$$(f \cdot_R g)F = f \circ g \circ F = f \circ F \circ g = F \circ f \circ g = F(f \cdot_R g),$$

so $f \cdot_R g \in \mathrm{End}_R(F)$. □

7.2 Lubin-Tate formal groups

Let K be a local field, with $|k| = q$.

Definition 7.8. A **formal $\mathcal{O}_K$-module** over $\mathcal{O}_K$ is a formal group law $F \in \mathcal{O}_K[\![X, Y]\!]$, together with a ring homomorphism

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

such that, for all $a \in \mathcal{O}_K$,

$$[a]_F(X) \equiv aX \bmod X^2.$$

A homomorphism (isomorphism) $f : F \to G$ of formal $\mathcal{O}_K$-modules is a homomorphism (isomorphism) of formal group laws over $\mathcal{O}_K$ such that, for all $a \in \mathcal{O}_K$,

$$f([a]_F) = [f(a)]_G.$$

Definition 7.9. Let $\pi \in \mathcal{O}_K$ be a uniformiser. A **Lubin-Tate** series for π is a power series $f \in \mathcal{O}_K[\![X]\!]$ such that

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

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

Example 7.10. Let $K = \mathbb{Q}_p$. Then $f(X) = (X+1)^p - 1$ is a Lubin-Tate series for p.

Example 7.11. Lubin-Tate series always exist: take $f(X) = \pi X + X^q$.

Theorem 7.12. *Let $f(X)$ be a Lubin-Tate series for π.*

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

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

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

We call Ff the **Lubin-Tate formal group law** for π. It depends (up to isomorphism) only on π, and not on f.

Example 7.13. Let $K = \mathbb{Q}$ and $f(X) = (X+1)^p - 1$. Then $Ff = \hat{\mathbb{G}}_m$. Indeed, it suffices to show $f \circ \hat{\mathbb{G}}_m = \hat{\mathbb{G}}_m \circ f$. Then we can compute

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

Lemma 7.14 (Key Lemma)**.** *Suppose f and g are Lubin-Tate series for π, and take a linear form*

$$L(X_1, \dots, X_n) = \sum_{i=1}^{n} a_i X_i \text{ with } a_i \in \mathcal{O}_K.$$

Then there is a unique power series $F(X_1, \dots, X_n) \in \mathcal{O}_K[\![X_1, \dots, X_n]\!]$ such that

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

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

Proof. We will show by induction that there is a unique polynomial $F_m \in \mathcal{O}_K[X_1, \dots, X_m]$ of total degree at most m such that

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

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

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

Taking $F = \varprojlim_m F_m$, we are done. Note that condition (c) ensures F is well-defined; uniqueness follows from uniqueness of the F_m.

For $m = 1$, we must take $F_1 = L$ for (b) to hold. Since f is a Lubin-Tate series,

$$f(F_1(X_1, \dots, X_n)) \equiv \pi L(X_1, \dots, X_n) \equiv F_1(g(X_1), \dots, g(X_n)) \bmod \deg 2,$$

so (a) also holds.

Having constructed $F_1, \dots, F_m$, set $F_{m+1} = F_m + h$ for some degree-$(m+1)$ homogeneous $h \in \mathcal{O}_K[X_1, \dots, X_n]$. Conditions (b) and (c) are trivially satisfied; it remains to compute (a).

We have $f(X+Y) = f(X) + f'(X)Y + Y^2(\dots)$ and $f'(X) \equiv \pi \bmod X$, so

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

Since $g \equiv \pi X \bmod X^2$, we similarly have

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

Hence (a) holds iff

$$f \circ F_m - F_m \circ g \equiv (\pi - \pi^{m+1})h \bmod \deg m + 2. \qquad (\star)$$

But $f(X) \equiv g(X) \equiv X^q \bmod \pi$; since $\mathcal{O}_K/(\pi) \cong \mathbb{F}_q$,

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

Therefore $f \circ F_m - F_m \circ g \in \pi\mathcal{O}_K[\![X_1, \ldots, X_n]\!]$. Let r be the degree-$(m+1)$ homogeneous component of $f \circ F_m - F_m \circ g$; then set

$$h \coloneqq \frac{r}{\pi(1-\pi^m)} \in \mathcal{O}_K[X_1, \ldots, X_n].$$

Then h is unique by condition $(\star)$. □

Proof of theorem. (i) By the lemma, there is a unique $Ff(X,Y) \in \mathcal{O}_K[\![X,Y]\!]$ such that $Ff(X,Y) \equiv X + Y \bmod \deg 2$ and $f \circ F = F \circ (f,f)$; note that the second condition implies that Ff is an Ff-endomorphism if it is a formal group law. It remains to show Ff satisfies associativity and commutativity; these follow from uniqueness. We will check associativity; commutativity is left as an exercise.

Indeed,

$$Ff(X, Ff(Y,Z)) \equiv X + Y + Z \equiv Ff(Ff(X,Y), Z) \bmod \deg 2,$$

and

$$f \circ Ff(X, Ff(Y,Z)) = Ff(f(X), f \circ Ff(Y,Z)) = Ff(f(X), Ff(f(Y), f(Z))).$$

Similarly,

$$f \circ Ff(Ff(X,Y), Z) = Ff(Ff(f(X), f(Y)), f(Z)),$$

and so, by uniqueness, $Ff(X, Ff(Y,Z)) = Ff(Ff(X,Y), Z)$.

(ii) Fix $a \in \mathcal{O}_K$. There is a unique $[a]_{Ff} \in \mathcal{O}_K[\![X]\!]$ such that $[a]_{Ff} \equiv aX \bmod X^2$ and $f \circ [a]_{Ff} = [a]_{Ff} \circ f$. Then $[a]_{Ff} \circ Ff = Ff \circ [a]_{Ff}$ by uniqueness, so $[a] \in \mathrm{End}_{O_K}(Ff)$.

Again by a uniqueness argument, $[\cdot]_{Ff} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(Ff)$ is a ring homomorphism. Hence Ff is a formal $\mathcal{O}_K$-module (over $\mathcal{O}_K$). Note that, by uniqueness, $[\pi]_{Ff} = f$ (as $f \equiv \pi X \bmod X^2$).

(iii) If $g(X)$ is some other Lubin-Tate series for π, let $\theta(X) \in \mathcal{O}_K[\![X]\!]$ be the unique power series such that $\theta(X) \equiv X \bmod X^2$ and $\theta \circ f = g \circ \theta$. By uniqueness, $\theta \circ (Ff) = Fg(\theta(X), \theta(Y))$, so $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(Ff, Fg)$. Swapping f and g, we obtain $\varphi \in \mathrm{Hom}_{\mathcal{O}_K}(Ff, Fg)$; by uniqueness, $\theta \circ \varphi(X) = \varphi \circ \theta(X) = X$, so θ is an isomorphism of formal group laws.

Further, by uniqueness we have that, for $a \in \mathcal{O}_K$, $\theta \circ [a]_{Ff}(X) = [a]_{Fg} \circ \theta(X)$. Hence θ is an isomorphism of formal $\mathcal{O}_K$-modules.

□

7.3 Lubin-Tate extensions

Let K be a non-Archimedean local field with residue field k of order q, and let π be a uniformiser. Fix an algebraic closure $\bar{K}$ of K, and let $\bar{\mathfrak{m}} \trianglelefteq \mathcal{O}_{\bar{K}}$ be the unique maximal ideal.

Lemma 7.15. *Let F be a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. Then $\bar{\mathfrak{m}}$ becomes a (true) $\mathcal{O}_K$-module under the operations $x +_F y = F(x, y)$ and $a \cdot_F x = [a]_F(x)$.*

Proof. Since $\bar{K}$ is not complete, we do need to check that the operations are well-defined. Indeed, if $x \in \bar{\mathfrak{m}}$, then $x \in \mathfrak{m}_L$ for some finite L/K, which *is* complete. Since $[x]_F \in \mathcal{O}_K[\![X]\!]$ converges in L and $\mathfrak{m}_L$ is closed, in fact $[a]_F(x) \in \mathfrak{m}_L \subseteq \bar{\mathfrak{m}}$. Convergence of addition follows similarly (use the compostium).

The module structure follows from the definition of a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. □

Definition 7.16. Let $f(X)$ be a Lubin-Tate series for π, and let Ff be the Lubin-Tate formal group law for π. The **π^n-torsion group** is the set

$$\mu_{f,n} = \{x \in \bar{\mathfrak{m}} \mid \pi^n \cdot_{Ff} x = 0\} = \{x \in \bar{\mathfrak{m}} \mid f^n(x) = 0\},$$

where f^n is the n-fold composite $f \circ \cdots \circ f$.

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

Example 7.17. Let $K = \mathbb{Q}_p$, and $f = (X+1)^p - 1$. Then

$$[p^n]_{Ff} = f^n = (X+1)^{p^n} - 1,$$

so $\mu_{f,n} = \{\xi_{p^n}^i - 1 \mid 0 \le i < p^n\}$.

Now let $f(X) = \pi X + X^q$; then

$$f^n(X) = f \circ f^{n-1}(X) = f^{n-1}(X)(\pi + f^{n-1}(X)^{q-1}).$$

Then set $f^0(X) = 1$, and

$$h_n(X) \coloneqq \frac{f^n(X)}{f^{n-1}(X)} = \pi + f^{n-1}(X)^{q-1}.$$

Proposition 7.18.
$h_n(X)$ is a separable Eisenstein polynomial of degree $q^{n-1}(q-1)$.

Proof. Each h_n is clearly monic of degree $q^{n-1}(q-1)$. Since $f(X) \equiv X^q \bmod \pi$, $f^{n-1}(X)^{q-1} \equiv X^{q^{n-1}} \bmod \pi$. Since $f^{n-1}(X)$ has constant term 0, $h_n(X) = \pi + f^{n-1}(X)^{q-1}$ has constant term π. Hence h_n is Eisenstein; since it is irreducible, it must be separable unless $\operatorname{char} K = p > 0$; in this case, it suffices to show $h_n' \neq 0$.

Proceed by induction. Indeed, $h_1(X) = \pi + X^{q-1}$ is separable. Now, suppose $h_1(X), \ldots, h_{n-1}(X)$ are separable; then $f^{n-1}(X) = h_{n-1}(X) \ldots h_1(X)$ is separable since each polynomial is separable and irreducible of a different degree. Then

$$h_n'(X) = (q-1)(f^{n-1})'(X) f^{n-1}(X)^{q-2} \neq 0,$$

so $h_n(X)$ is separable. □

Proposition 7.19.

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

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

Proof.

(i) Let $\alpha \in K$ be a root of h_n. Since h_n and f^{n-1} are coprime, $\alpha \notin \mu_{f,n-1}$. Then the map

$$\begin{aligned} \tilde{\varphi} : \mathcal{O}_K &\to \mu_{f,n} \\ a &\to a \cdot_{Ff} \alpha \end{aligned}$$

is an $\mathcal{O}_K$-module homomorphism with kernel $\pi^n\mathcal{O}_K$ (since $\alpha \in \mu_{f,n} \setminus \pi_{f,n-1}$). Therefore $\tilde{\varphi}$ induces an injection $\varphi : \mathcal{O}_K/\pi^n\mathcal{O}_K \hookrightarrow \mu_{f,n}$. Since f^n is separable,

$$|\mu_{f,n}| = \deg f^n(X) = q^n = |\mathcal{O}_K/\pi^n\mathcal{O}_K|.$$

Hence φ is surjective, and hence a linear isomorphism.

(ii) There exists a formal $\mathcal{O}_K$-module isomorphism $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(Ff, Fg)$. This induces an isomorphism between $(\bar{\mathfrak{m}}, +_{Ff}, \cdot_{Ff})$ and $(\bar{\mathfrak{m}}, +_{Gf}, \cdot_{Gf})$ (to show the map converges, consider elements in their finite extensions as before), and hence an isomorphism $\mu_{f,n} \cong \mu_{g,n}$.

Since $\mu_{f,n}$ is finite, $K(\mu_{f,n})/K$ is finite, and hence complete. Now, $\theta \in \mathcal{O}_K[\![X]\!]$; for $x \in \mu_{f,n}$, we have $\theta(x) \in K(\mu_{g,n})$, and so $K(\mu_{g,n}) \subseteq K(\mu_{f,n})$. Repeating the argument with θ^{-1}, we get the reverse containment, so in fact $K(\mu_{g,n}) = K(\mu_{f,n})$.

□

We can now define our desired field.

Definition 7.20. $K_{\pi,n} \coloneqq K(\mu_{f,n})$ is the n^{th} **Lubin-Tate extension**.

Note that these don't depend on the choice of Lubin-Tate series. Observe that $K_{\pi,n} \subseteq K_{\pi,n+1}$, as we wanted. We need to prove that these extensions satisfy our desired properties.

Proposition 7.21. *The* $K_{\pi,n}$ *are totally ramified Galois extensions of degree* $q^{n-1}(q-1)$*.*

Proof. We may choose wlog $f(X) = \pi X + X^q$. Then $K_{\pi,n} = K(\mu_{f,n})$ is the splitting field of f^n, so it is Galois.

Now, let α be a root of $h_n(X)$, which is an Eisenstein polynomial of degree $q^{n-1}(q-1)$. Then α generates a totally ramified extension, so it suffices to show $K(\alpha) = K_{\pi,n}$. By definition of h_n, $f^n(\alpha) = 0$, so $K(\alpha) \subseteq K_{\pi,n}$.

Conversely, by the last proposition, $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$ generates $\mu_{f,n}$; that is, any $x \in \mu_{f,n}$ has form

$$x = a \cdot_{Ff} \alpha = [a]_{Ff}(\alpha), \text{ for some } a \in \mathcal{O}_K.$$

Since $K(\alpha)$ is complete and $[a]_{Ff}(X) \in \mathcal{O}_K[\![X]\!]$, we have $x = [a]_{Ff}(\alpha) \in K(\alpha)$, and so $K(\alpha) \supseteq K(\mu_{f,n})$. □

Theorem 7.22. *There are isomorphisms*

$$\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\simeq} \left(\frac{\mathcal{O}_K}{\pi^n \mathcal{O}_K}\right)^\times$$

such that, for all $x \in \mu_{f,n}$ and $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$,

$$\psi_n(\sigma) \cdot_{Ff} x = \sigma(x). \tag{$\star$}$$

Moreover, the ψ_n do not depend on f.

Proof. First, set $f(X) = \pi X + X^q$. Fix $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. Then σ acts on $\mu_{f,n}$ since $\sigma f = f$, and σ acts continuously on $K_{\pi,n} = K(\mu_{f,n})$. Now, $Ff(X,Y) \in \mathcal{O}_K[\![X,Y]\!]$, and, for $a \in \mathcal{O}_K$, we have $[a]_{Ff} \in \mathcal{O}_K[\![X]\!]$. Therefore, for $x, y \in \mu_{f,n}$ and $a \in \mathcal{O}_K$, we have

$$\begin{aligned} \sigma(x +_{Ff} y) &= \sigma(x) +_{Ff} \sigma(y); \\ \sigma(a \cdot_{Ff} x) &= a \cdot_{Ff} \sigma(x). \end{aligned}$$

Hence σ restricts to an $\mathcal{O}_K$-module automorphism of $\mu_{f,n}$; since $K_{\pi,n} = K(\mu_{f,n})$, the restriction map gives an injection

$$\mathrm{res} : \mathrm{Gal}(K_{\pi,n}) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n}).$$

But $\mu_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$ as $\mathcal{O}_K$-modules, so

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

Indeed, the automorphisms of a rank-1 R-module are exactly the maps given by multiplication by some element of $R^\times$.

Let ψ_n be the composition of res with this isomorphism; explicitly, $\psi_n(\sigma)$ is the unique element of $(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ such that

$$\psi_n(\sigma) \cdot_{Ff} x = \sigma(x) \text{ for } x \in \mu_{f,n}.$$

But

$$[K_{\pi,n} : K] = q^{n-1}(q-1) = \left|\left(\frac{\mathcal{O}_K}{\pi^n\mathcal{O}_K}\right)^\times\right|,$$

so ψ_n is also surjective. Therefore ψ_n is the required isomorphism.

Now let g be some other Lubin-Tate series for π; in the same way, obtain an isomorphism $\psi'_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\simeq} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$. Now, we have an isomorphism of formal $\mathcal{O}_K$-modules $\theta : Ff \xrightarrow{\simeq} Fg$; this induces an isomorphism $\theta : \mu_{f,n} \xrightarrow{\simeq} \mu_{g,n}$. For $x \in \mu_{f,n}$, we therefore have

$$\theta(\psi_n(\sigma) \cdot_{Ff} x) = \psi_n(\sigma) \cdot_{Fg} \theta(x).$$

Since $\theta \in \mathcal{O}_K[\![X]\!]$ and σ is continuous, we have, for $x \in \mu_{f,n}$,

$$\theta(\sigma(x)) = \sigma(\theta(x))$$

and so

$$\psi_n(\sigma) \cdot_{Fg} \theta(x) = \theta(\psi_n(\sigma) \cdot_{Ff} x) = \theta(\sigma(x)) = \sigma(\theta(x)) = \psi'_n(\sigma) \cdot_{Fg} \theta(x).$$

Therefore $\psi_n = \psi'_n$. □

Finally, set

$$K_{\pi,\infty} = \bigcup_{n=1}^{\infty} K_{\pi,n};$$

gluing the ψ_n, we get an isomorphism

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

As in the case of $\mathbb{Q}_p$, we can relate $K_{\pi,\infty}$ to K^{ab}:

Theorem 7.23 (Generalised local Kroenecker-Weber)**.**

$$K^{ab} = K_{\pi,\infty}K^{un}.$$

Proof. Omitted. □

We can now define the Artin map Art_K.

$$\begin{aligned} K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times &\to \mathrm{Gal}(K^{\mathrm{un}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \pi^n u \leftarrow (n,u) &\to (\mathrm{Frob}^n_{K^{\mathrm{un}}/K}, \psi^{-1}(u^{-1})) \end{aligned}$$

This map is independent of the choice of uniformiser π, and its image is exactly $W(K^{\mathrm{ab}}/K)$.

The remaining material is non-examinable.

8 Upper numbering of ramification groups

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

$$\begin{aligned} \varphi_{L/K} \coloneqq \varphi : \mathbb{R}_{\geq -1} &\to \mathbb{R} \\ s &\to \int_0^s \frac{1}{[G_0 : G_t]} \mathrm{d}t. \end{aligned}$$

By convention, for $t \in [-1, 0]$, we define

$$\frac{1}{[G_0 : G_t]} = [G_t : G_0] = [G : G_0].$$

Note that, since G_t only changes at integers, the function being integrated is a decreasing, strictly positive function that only changes at integers. Therefore φ is continuous (in fact piecewise linear) and strictly increasing.

More explicitly, let $m \in \mathbb{Z}_{\geq -1}$. Then, for $m \leq s < m+1$, we get

$$\varphi(s) = \begin{Bmatrix} s[G : G_0] & m = -1 \\ \frac{1}{|G_0|}(|G_1| + \cdots + |G_m| + (s-m)|G_{m+1}|) & m \geq 0 \end{Bmatrix}.$$

Definition 8.1. The higher ramification groups in **upper numbering** are

$$G^s(L/K) \coloneqq G_{\varphi_{L/K}(s)}(L/K) \leq \mathrm{Gal}(L/K),$$

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

Recall that $G_s(L/K)$ behaves well with respect to subgroups. Indeed, for an intermediate extension $L/F/K$, we have

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

Analogously, $G^t(L/K)$ behaves well with respect to quotients:

$$\frac{G^t(L/K)\,\mathrm{Gal}(L/F)}{\mathrm{Gal}(L/F)} = G^t(F/K).$$

This result is called Herbrand's theorem; it allows us to define upper numbering for infinite extensions.

Example 8.2. Let $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\zeta_{p^n})$. Let $1 \leq k \leq n-1$ be an integer; then, for $p^{k-1} - 1 < s \leq p^k - 1$, we computed earlier that

$$G_s(L/K) = \{m \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid m \equiv 1 \bmod p^k\} \cong \frac{U^k_{\mathbb{Q}_p}}{U^n_{\mathbb{Q}_p}}.$$

Then G_s changes only at $p^k - 1$, so $\varphi_{L/K}$ is linear on $[p^{k-1} - 1, p^k - 1]$. Thus, to compute $\varphi_{L/K}$, it suffices to compute $\varphi_{L/K}(p^k - 1)$. Since $[G_0 : G_{p^k - 1}] = p^{k-1}(p-1)$, we compute

$$\varphi_{L/K}(p^k - 1) = \frac{p-1}{p-1} + \frac{p^2 - 1 - (p-1)}{p(p-1)} + \cdots + \frac{p^k - 1 - (p^{k-1} - 1)}{p^{k-1}(p-1)} = k.$$

Therefore

$$G^s(L/K) \cong \begin{Bmatrix} \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^\times & s \leq 0 \\ \frac{1+p^k\mathbb{Z}}{p^n\mathbb{Z}} & k-1 \leq s \leq k;\ 1 \leq k \leq n-1 \\ 1 & s > n-1 \end{Bmatrix}.$$

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