Local Fields Notes

October 13, 2025

These notes are based on a course of the same title given by Professor Rong Zhou at Cambridge during Michaelmas Term 2024. They have been written up by Alexander Shashkov. There are likely plenty of errors, which are my own.

Contents

Part I

Basic Theory

Let $f(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r]$. We want to understand for which points $(a_1, \dots, a_r) \in \mathbb{Z}^r$ we have that $f(a_1, \dots, a_r) = 0$. This is a very hard question. But instead, we might ask the simpler question for solutions to

$$\begin{aligned} f(x_1, \dots, x_r) &\equiv 0 \mod p \\ f(x_1, \dots, x_r) &\equiv 0 \mod p^2 \\ &\dots \\ f(x_1, \dots, x_r) &\equiv 0 \mod p^n \end{aligned} \tag{0.1}$$

Local fields package all the $\mod p^n$ information together.

1 Absolute values

Definition 1.1. Let K be a field. An absolute value on K is a function

$$|\cdot| : K \to \mathbb{R}_{\geq 0} \tag{1.1}$$

such that

(i) $|x| = 0$ if and only if $x = 0$.

(ii) $|x||y| = |xy|$ for all $x, y \in K$.

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

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

Example 1.2. 1. $|a+bi| = \sqrt{a^2 + b^2}$ in $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. This is the $|\cdot|_\infty$, the valuation at infinity.

2. The trivial absolute value for any field K is

$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases} \tag{1.2}$$

We will mostly ignore the trivial absolute value in this course.

3. Let $K = \mathbb{Q}$, then the p-adic absolute value is

$$|x|_p = \begin{cases} p^{-v_p(x)} & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{1.3}$$

where $x = p^{v_p(x)} \frac{a}{b}$ with $p \nmid ab$.

Lemma 1.3. *$|\cdot|_p$ is an absolute value.*

Proof. We go through the 3 conditions in Definition 1.1. They are all easy. □

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

Definition 1.4. Let $|\cdot|, |\cdot|'$ be two absolute values on K. We say that they are equivalent if they induce the same topology.

Definition 1.5. An equivalence class of absolute values is called a *place.*

Proposition 1.6. *Let $|\cdot|, |\cdot|'$ be two absolute values on K. The following are equivalent:*

(i) $|\cdot|$ and $|\cdot|'$ are equivalent.

(ii) $|x| < 1$ if and only if $|x|' < 1$ (unit balls are the same).

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

Proof. (i) $\implies$ (ii): We have that $|x| < 1$ if and only if $x^n \to 0$ with respect to $|\cdot|$ if and only if $x^n \to 0$ with respect to $|\cdot|'$ (by (i)) if and only if $|x'| < 1$.

(ii) $\implies$ (iii): We have that $|x|^c = |x|'$ if and only if $c \log |x| = \log |x|'$. Let $a \in K^\times$ such that $|a| > 1$, which exists because $|\cdot|$ is nontrivial. We need that for all $x \in K$ that

$$\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}. \tag{1.4}$$

Assume that

$$\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}. \tag{1.5}$$

Choose $m, n \in \mathbb{Z}, n > 0$ such that

$$\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}. \tag{1.6}$$

Then $n \log|x| < m \log|a|$ and $n \log|x|' > m \log|a|'$, so

$$\left|\frac{x^n}{a^m}\right| < 1, \quad \left|\frac{x^n}{a^m}\right|' > 1, \tag{1.7}$$

which is a contradiction by (ii).

(iii) $\implies$ (i): This is clear because the open balls are the same. □

Remark 1.7. $|\cdot|_\infty^2$ on $\mathbb{C}$ is *not* an absolute value by our definition because the triangle inequality does not hold. Some authors replace the triangle inequality by

$$|x+y|^\beta \leq |x|^\beta + |y|^\beta \tag{1.8}$$

for some $\beta \in \mathbb{R}_{>0}$.

Definition 1.8. An absolute value on K is *non-archimedean* if it satisfies the *ultrametric inequality*:

$$|x+y| \leq \max(|x|, |y|) \tag{1.9}$$

If $|\cdot|$ is not non-archimedean, we say that it is *archimedean.*

Example 1.9. $|\cdot|_\infty$ is archimedean, $|\cdot|_p$ is non-archimedean.

Lemma 1.10. *Let $(K, |\cdot|)$ be non-archimedean and $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$.*

Proof. We have that $|x-y| \le \max(|x|,|y|) = |y|$ and $|y| \le \max(|x-y|,|x|) = |x-y|$ so $|x-y| = |y|$. □

Proposition 1.11. *Let $(K, |\cdot|)$ be non-archimedean and (x_n) a sequence. If $|x_n - x_{n+1}| \to 0$, then the sequence is Cauchy. So if K is complete, then $x_n \to x$.*

Proof. We have that

$$|x_m - x_n| \le \max(|x_m - x_{m-1}|, \ldots, |x_{n+1} - x_n|) < \epsilon \tag{1.10}$$

if $|x_{i+1} - x_i| < \epsilon$. □

Example 1.12. Let $p = 5$, and construct a sequence $(x_n)_{n=1}^\infty$ in $\mathbb{Z}$ such that $x_n^2 + 1 \equiv 0 \mod 5^n$ and $x_n \equiv x_{n+1} \mod 5^n$. Then $|x_n - x_{n+1}|_5 \le 5^{-n}$ so the sequence is Cauchy.

Take $x_1 = 2$, and let $x_n^2 + 1 = a5^n$ and set $x_{n+1} = x_n + b5^n$. Then

$$\begin{aligned} x_{n+1}^2 + 1 &= 1 + x_n^2 + 5^n(2bx_n + b^2 5^n) \\ &= a5^n + 5^n(2bx_n + b^2 5^n \end{aligned} \tag{1.11}$$

So we can choose b so that $a + 2bx_n \equiv 0 \mod 5$. The sequence goes $2, 7, 32, \ldots$. Suppose that $x_n \to \ell \in \mathbb{Q}$. Then $x_n^2 \to \ell^2$. But we have that $x_n^2 \to -1$, so $\ell^2 = -1$. So $(\mathbb{Q}, |\cdot|_5)$ is not complete.

Definition 1.13. The 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 field, and for $x \in K$ and $r \in \mathbb{R}_{>0}$ define

$$\begin{aligned} B(x,r) &= \{y \in K \mid |x-y| < r\} \\ \overline{B}(x,r) &= \{y \in K \mid |x-y| \le r\} \end{aligned} \tag{1.12}$$

the open and closed balls around x of radius r.

Lemma 1.14. *Let $z \in B(x,r)$. Then*

(i) $B(z,r) = B(x,r)$.

(ii) $\overline{B}(z,r) = \overline{B}(x,r)$.

(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

$$|z-y| = |(z-x) + (x-y)| \le \max(|x-z|, |x-y|) < r. \tag{1.13}$$

Thus $B(x,r) = B(z,r)$ by symmetry.

(ii) The same argument as above holds.

(iii) Let $y \notin B(x,r)$. If $z \in B(x,r) \cap B(y,r)$, then $B(x,r) = B(z,r) = B(y,r)$. So $y \in B(x,r)$, which is a contradiction. Thus $B(x,r) \cap B(y,r) = \emptyset$. So there exists an open neighborhood around y not containing $B(x,r)$, so $B(x,r)$ is closed.

(iv) If $z \in \overline{B}(x,r)$, then $B(z,r) \subseteq \overline{B}(z,r) = \overline{B}(x,r)$ so $B(z,r)$ is an open neighborhood in $B(x,r)$, and

$$\overline{B}(x,r) = \bigcup_{z \in \overline{B}(x,r)} B(z,r) \tag{1.14}$$

□

2 Valuation rings

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

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

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

Fix $0 < \alpha < 1$. If v is a valuation on K, then define

$$|x| = \begin{cases} \alpha^{v(x)} & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{2.1}$$

which determines a non-archimedean absolute value. Conversely, given an absolute value $|\cdot|$, we can define a valuation

$$v(x) = \log_\alpha |x|. \tag{2.2}$$

Remark 2.2. We ignore the trivial valuation $v(x) = 0$ for all x, which induces the trivial absolute value.

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

Example 2.3. 1. Let $K = \mathbb{Q}$, and $v_p(x) = \log_p |x|_p = n$, where $x = p^n \cdot \frac{r}{s}$ with $p \nmid rs$.

2. Let k be a field, and $K = k(t) = \mathrm{Frac}(k[t])$ the function field of k. Then we can define a valuation

$$v\left(t^n \frac{f(t)}{g(t)}\right) = n \tag{2.3}$$

where $f(0), g(0) \neq 0$. This is the t-adic evaluation.

3. Let $K = k((t)) = \mathrm{Frac}(k[[t]])$ the ring of formal Laurent series, and let $v(P(t))$ be the smallest nonzero index. We have that $k((t))$ is the t-adic completion of $k(t)$, and

$$\mathbb{Q}_p = \mathbb{Z}((t))/(t-p) \tag{2.4}$$

Definition 2.4. Let $(K, |\cdot|)$ be a non-archimedean field. The *valuation ring* is defined to be

$$\begin{aligned} \mathcal{O}_K &= \{x \in K \mid |x| \leq 1\} = \overline{B}(0,1) \\ &= \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\} \end{aligned} \tag{2.5}$$

Proposition 2.5. *(i) $\mathcal{O}_K$ is an open subring of K.*

(ii) The subsets $\{x \in K \mid |x| \leq r\} = \overline{B}(0,r)$ and $\{x \in K \mid |x| < r\} = B(0,r)$ for $r \leq 1$ are open ideal in $\mathcal{O}_K$.

(iii) The units of the valuation ring are

$$\mathcal{O}_K^\times = \{x \in K \mid |x| = 1\} = \{x \in K \mid v(x) = 0\} \tag{2.6}$$

Proof. (i) We have that $|0| = 0$, and $|1| = 1$, so $0, 1 \in \mathcal{O}_K$. If $x \in \mathcal{O}_k$, then $|-x| = |x|$, so $-x \in \mathcal{O}_K$. If $x, y \in \mathcal{O}_K$, then $|x + y| \leq \max |x|, |y| \leq 1$, so $x + y \in \mathcal{O} - K$. Also $|xy| = |x||y| \leq 1$, so $xy \in \mathcal{O}_K$. Thus $\mathcal{O}_K$ is a ring.

(ii) Same as (i).

(iii) We have that $|x||x^{-1}| = 1$, so $x, x^{-1} \in \mathcal{O}_K$ if and only if $|x| = 1$. □

By the above, we have that

$$\mathfrak{m} := \{x \in \mathcal{O}_K \mid |x| < 1\} \tag{2.7}$$

is the unique maximal ideal of $\mathcal{O}_K$. It is unique because if $x \notin \mathfrak{m}$, then $x \in \mathcal{O}_K^\times$. We have that

$$k := \mathcal{O}_K/\mathfrak{m} \tag{2.8}$$

is the *residue field* of K.

Corollary 2.6. *$\mathcal{O}_K$ is a local ring.*

Example 2.7. Let $K = \mathbb{Q}$ with absolute value $|\cdot|_p$. Then

$$\mathcal{O}_K = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\} \tag{2.9}$$

and $\mathfrak{m} = p\mathbb{Z}_{(p)}$, and $k = \mathbb{F}_p$.

Definition 2.8. Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \cong \mathbb{Z}$, so that $v(K^\times)$ is a discrete subgroup, we say that $|\cdot|$ is a *discrete valuation* on K.

An element $\pi \in \mathcal{O}_K$ is a *uniformizer* if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$.

Example 2.9.

1. $K = \mathbb{Q}$ with v_p is a discrete valuation.
2. $K = k(t)$ with the t-adic valuation is a discrete.
3. $k(t, t^{1/2}, t^{1/4}, \ldots)$ with the t-adic valuation is *not* a discrete valuation as the t-adic valuation has image $\mathbb{Z}[1/2]$, which is not discrete.

Remark 2.10. If v is a discrete valuation, we can rescale so that $v(K^\times) = \mathbb{Z}$ (the normalized valuation) Then the uniformizer has $v(\pi) = 1$.

Lemma 2.11. *Let v be a valuation on K. The following are equivalent:*

(i) v is discrete.

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

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

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

Proof. (i) $\implies$ (ii): $\mathcal{O}_K$ is an integral domain because $\mathcal{O}_K \subset K$. Let $I \subset \mathcal{O}_K$ be a nonzero ideal. Let $x \in I$ be such that $v(x)$ is minimal. Such an x exists because v is discrete. We want to show that

$$x\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq v(x)\} = I \tag{2.10}$$

We have that $x\mathcal{O}_K \subset I$ trivially. Let $y \in I$. Then $v(x^{-1}y) \geq 0$, so $y = x(x^{-1}y) \in x\mathcal{O}_K$.

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

(iii) $\implies$ (iv): Write $\mathfrak{m} = x_1\mathcal{O}_K + \cdots + x_n\mathcal{O}_K$. WLOG we have that

$$v(x_1) \leq v(x_2) \leq \cdots \leq v(x_n) \tag{2.11}$$

so $x_2, \ldots, x_n \in x_1\mathcal{O}_K$, so $\mathfrak{m} = x_1\mathcal{O}_K$.

(iv) $\implies$ (i): Let $\mathfrak{m} = \pi\mathcal{O}_K$ for $\pi \in \mathcal{O}_K$, and let $c = v(\pi)$. If $v(x) > 0$, then $x \in \mathfrak{m}$, so $v(x) \geq c$, so $v(K^\times) \cap (0, c) = \emptyset$, so v is discrete.

□

Let v be a discrete valuation on K, and let $\pi \in \mathcal{O}_K$ be a uniformizer so that $v(\pi) = 1$. Then for any $x \in K^\times$, let $n \in \mathbb{Z}$ be such that $v(x) = nv(\pi) = n$. Then if $u = \pi^{-n}x \in \mathcal{O}_K^\times$, then $x = u\pi^n$. Thus

$$K = \mathrm{Frac}(\mathcal{O}_K) = \mathcal{O}_K[\pi^{-1}] \tag{2.12}$$

Definition 2.12. A ring R is a discrete valuation ring (DVR) is it is a PID with exactly one nonzero prime ideal (which is therefore maximal).

A priori we don't know that discrete valuation rings and discrete valuations are connected. The next lemma shows that they are.

Lemma 2.13. *(i) Let v be a discrete valuation on a field K. Then $\mathcal{O}_K$ is a discrete valuation ring.*

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

Proof. (i) $\mathcal{O}_K$ is a PID by Lemma 2.11, so any nonzero prime ideal is maximal. So $\mathcal{O}_K$ is a DVR because it is local.

(ii) Let R be a DVR with maximal ideal $\mathfrak{m} = (\pi)$ for some $\pi \in R$. Since every PID is a UFD, we can write any $x \in R \setminus \{0\}$ uniquely as $\pi^n u$, $u \in R^\times$. So any $y \in K^\times$ can be written as $\pi^m u$ with $m \in \mathbb{Z}$. So define $v(\pi^m u) = m$. Then $\mathcal{O}_K = R$. □

It's now clear that many of the examples above are discrete valuation rings.

3 p-adic numbers

Recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic valuation v_p. $\mathbb{Q}_p$ is a field, and $|\cdot|_p$ extends to a discrete valuation on $\mathbb{Q}_p$.

Definition 3.1. The ring of p-adic integers $\mathbb{Z}_p$ is the valuation ring of $\mathbb{Q}_p$, so that

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1,\ v_p(x) \geq 0\} \tag{3.1}$$

By Lemma 2.13, $\mathbb{Z}_p$ is a discrete valuation ring with maximal ideal $p\mathbb{Z}_p$, and all the ideals are of the form $p^n\mathbb{Z}_p$.

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

Proof. We need to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ since $\mathbb{Z}_p$ is closed. By definition $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Since $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is open, $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$. But

$$\mathbb{Z}_p \cap \mathbb{Q} = \{x \in \mathbb{Q} \mid |x|_p \leq 1\} = \mathbb{Z}_{(p)}. \tag{3.2}$$

So we want to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$.

Let $a/b \in \mathbb{Z}_{(p)}$, such that $a, b \in \mathbb{Z}$ with $p \nmid b$. For $n \in \mathbb{N}$, choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \mod p^n$. Then $y_n \to a/b$ as $n \to \infty$. In particular, $\mathbb{Z}_p$ is complete and $\mathbb{Z} \subset \mathbb{Z}_p$ is dense. □

3.1 Inverse limits

Let $(A_n)_{n=1}^{\infty}$ be a sequence of objects (e.g rings) in a category with maps $\varphi_n : A_{n+1} \to A_n$. So we have

$$\begin{tikzcd}\cdots \arrow[r] & A_{n+1} \arrow[r, "\varphi_n"] & A_n \arrow[r, "\varphi_{n-1}"] & A_{n-1} \arrow[r] & \cdots \arrow[r] & A_1 \arrow[r, "\varphi_1"] & A_1\end{tikzcd}$$

The inverse limit of $(A_n)_{n=1}^{\infty}$, if it exists, is an object

$$\varprojlim A_n = \{(a_n)_{n=1}^{\infty} \in \prod A_n \mid \varphi_n(a_{n+1}) = a_n\ \forall n\} \tag{3.3}$$

equipped with projection maps $\theta_m : \varprojlim A_n \to A_m$ which commute with the φ_ns. The inverse limit satisfies the following universal property.

Proposition 3.3. *For any object B with maps $\psi_n : B \to A_n$ such that the commutative diagram below commutes, there exists a unique $\psi : B \to \varprojlim A_n$ such that ψ_n factors thorugh θ_n by ψ so that $\theta_n \circ \psi = \psi_n$. In diagram form we have*

$$\begin{tikzcd}B \arrow[r, dashed, "!\exists\psi"] \arrow[d, "\psi_{n+1}"] \arrow[dr, "\psi_n"] & \varprojlim A_n \arrow[d, "\theta_n"] \\ A_{n+1} \arrow[r, "\varphi_n"] & A_n\end{tikzcd}$$

Proof. Define $\psi : B \to \prod A_n$ by $\psi(b) = \prod \psi_n(b)$. The commutativity of the diagram gives $\psi(b) \in \varprojlim A_n$, and the map is unique because it is determined by $\psi_n = \theta_n \circ \psi$, and it is a map because ψ_n is. □

Definition 3.4. Let $I \subset R$ be an ideal. Then the *I-adic completion* of R is defined to be

$$\widehat{R} = \varprojlim R/I^n, \tag{3.4}$$

where $R/I^{n+1} \to R/I^n$ is given by the obvious $x + I^{n+1} \to x + I^n$ for any $x \in R$.

There exists a natural map $i : R \to \widehat{R}$ by $x \to \prod x + I^n$. We say that R is *I-adically complete* if i is an isomorphism.

Remark 3.5. The kernel of the map $i : R \to \widehat{R}$ is $\bigcap I^n$, which we typically want to be 0 so that i is injective.

Now let $(K, |\cdot|)$ be a non-archimdedean valued field and $\pi \in \mathcal{O}_K$ with $|\pi| < 1$, so that $v(\pi) > 0$.

Proposition 3.6. *Assume that K is complete with respect to $|\cdot|$. Then*

(i) $\mathcal{O}_K \cong \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_k$, so $\mathcal{O}_K$ is π-adically complete.

(ii) Every $x \in \mathcal{O}_K$ can be written uniquely as

$$x = \sum_{i=0}^{\infty} a_i \pi^i, \tag{3.5}$$

where $a_i \in A$, $A \subset \mathcal{O}_K$ are coset representatives for $\mathcal{O}_K/\pi\mathcal{O}_K$.

Proof. (i): Since K is complete and $\mathcal{O}_K$ is closed, $\mathcal{O}_K$ is complete. We have that $\ker i = \bigcap \pi^n\mathcal{O}_K$, so $x \in \ker i$ if and only if $v(x) \geq nv(\pi)$ for all n, so if and only if $x = 0$. So i is injective.

Let $(x_n)_{n=1}^{\infty} \in \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K$ and for each n, let $y_n \in \mathcal{O}_K$ be any lifting of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$. Then $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$ so that $v(y_n - y_{n+1}) \geq nv(\pi) \to \infty$. Thus (y_n) is Cauchy and in $\mathcal{O}_K$ so it converges to some $y \in \mathcal{O}_K$. Then $x_n \to y$ also because $y - x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$, so the map i is surjective as well.

(ii): Example Sheet.

□

Corollary 3.7. *(i) $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.*

(ii) Every element of $x \in \mathbb{Q}_p$ can be written uniquely as

$$x = \sum_{i=n}^{\infty} a_i p^i \tag{3.6}$$

where $n \in \mathbb{Z}$, and $a_i \in \{0, 1, \dots, p-1\}$ and $a_n \neq 0$ (unless $x = 0$). If $n \geq 0$, then $x \in \mathbb{Z}_p$.

Proof. (i): By Proposition 3.6, we have that

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p \tag{3.7}$$

so we just need to show that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Let $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map sending $x \to x + p^n\mathbb{Z}_p$. We have that

$$\ker f_n = \{x \in \mathbb{Z} \mid v_p(x) \geq n\} = p^n\mathbb{Z} \tag{3.8}$$

so we can lift to an injection $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p \to p^n\mathbb{Z}_p$. Let $z \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ and $c \in \mathbb{Z}_p$ be a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there exists $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$ because $p^n\mathbb{Z}_p$ is open. Then $f_n(x) = \tau$.

(ii) Follows from Proposition 3.6 (ii). □

Example 3.8. We have that

$$\frac{1}{1-p} = 1 + p + p^2 + \cdots \tag{3.9}$$

Part II
Complete Valued Fields

4 Hensel's Lemma

Theorem 4.1 (Hensel's Lemma, Version 1). *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) \in \mathcal{O}_K[x]$ and assume that there exists $a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$, where $f'(a)$ is the formal derivative of $f(a)$. Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $|x - a| < |f'(a)|$.*

Proof. Let $\pi \in \mathcal{O}_K$ be a uniformizer and let $r = v(f'(a))$. We inductively construct a sequence $(x_n)_{n=1}^{\infty}$ in $\mathcal{O}_K$ such that

(i) $f(x_n) \equiv 0 \mod \pi^{n+2r}$, so $v(f(x_n)) \geq n + 2r$.

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

Take $x_1 = a$, and then $v(f(x_1)) \geq 2v(f'(a)) + 1 = 2r + 1$ so our base case is done. Now suppose the conditions hold up to x_n, and set

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \tag{4.1}$$

Since $x_n \equiv x_1 \mod \pi^{r+1}$, we have that $v(f'(x_n)) = v(f'(x_1)) = r$ (as $f'(x_n) = f'(x_1 + \pi^{r+1}c)$), so

$$v\left(\frac{f(x_n)}{f'(x_n)}\right) \geq n + r. \tag{4.2}$$

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

To show property (i), note that for X, Y indeterminates, we have that

$$f(X+Y) = f_0(X) + Yf_1(X) + Y^2 f_2(X) + \cdots \tag{4.3}$$

where $f_0(x) = f(x)$ and $f_1(x) = f'(x)$. Thus taking $X = x_n$ and $Y = f(x_n)/f'(x_n)$, we have that

$$f(x_{n+1}) = f(x_n) + f'(x_n)c + c^2(\cdots) \tag{4.4}$$

where $c = -f(x_n)/f'(x_n)$. Since $v(c) \geq n + r$, we have that

$$\begin{aligned} v(f(x_{n+1})) &\geq v(f(x_n) + f'(x_n)c + c^2) \\ &\geq 2n + 2r \\ &\geq n + 1 + 2r \end{aligned} \tag{4.5}$$

Property (ii) implies that (x_n) is Cauchy, and hence convergent. So let $x = \lim x_n$. Then $f(x) = \lim f(x_n) = 0$. By (ii), $a = x_1$ satisfies $|a - x| < |f'(a)|$ so x satisfies the condition of the theorem.

For uniqueness, suppose that x' also satisfies the conditions and set $\delta = x - x' \neq 0$. Then $|x' - a| < |f'(a)|$ and $|x - a| < |f'(a)|$ so the ultrametric inequality implies that

$$|\delta| = |(x - a) - (x' - a)| < |f'(a)| = |f'(x)|. \tag{4.6}$$

But $0 = f(x') = f(x + \delta) = f(x) + f'(x)\delta + \delta^2(\cdots) = f'(x)\delta + \delta^2(\cdots)$. Thus $|f'(x)\delta| \leq |\delta^2|$, so $|f'(x)| \leq \delta$, which contradicts (4.6). □

Essentially what we are doing above is Newton's method. We have a point a where the slope $f'(a)$ is "large" relative to $f(a)$. Then applying Newton's method, the size of the slope stays large, so we are guaranteed to descend to a solution.

We obtain the following corollary in the case where $v(f'(a)) = 0$.

Corollary 4.2. *Let $(K, |\cdot|)$ be a complete disceretely valued field. Let $f(x) \in \mathcal{O}_K[x]$ and $\tau \in k = \mathcal{O}_K/\mathfrak{m}$ be a simple root of*

$$F(x) = f(x) \mod \mathfrak{m} \in k[x]. \tag{4.7}$$

Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $x \equiv \tau \mod \mathfrak{m}$.

Proof. Apply Theorem 4.1 to a lift $c \in \mathcal{O}_K$ of τ. Then $|f(c)| < 1 = |f'(c)|^2$ because c is a simple root, so we can applyg the theorem. □

Example 4.3. $f(x) = x^2 - 2$ has a simple root $\mod 7$. Thus there exists a solution in $\mathbb{Z}_7$, so we have that "$\sqrt{2} \in \mathbb{Z}_7$".

Hensel's lemma gives us an explicit way to study solutions to polynomials in $\mathbb{Q}_p$ using polynomials in $\mathbb{F}_p$, as we promised at the very start of the course. Here is one nice application.

Corollary 4.4. *We have that*

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^3 & p = 2 \end{cases} \tag{4.8}$$

Proof. Let $p > 2$, and let $b \in \mathbb{Z}_p^\times$. Applying Corollary 4.2 to $f(x) = x^2 - b$, we find that $b \in (\mathbb{Z}_p^\times)^2$ if and only if $b \in (\mathbb{F}_p^\times)^2$. Thus

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}. \tag{4.9}$$

We have an isomorphism $\mathbb{Z}_p \times \mathbb{Z} \cong \mathbb{Q}_p^\times$ given by $(u, n) \to up^n$ which gives the deisred result when $p > 2$.

If $p = 2$, then let $b \in \mathbb{Z}_2^\times$, and consider $f(x) = x^2 - b$. Then $f'(x) = 2x = 0 \mod 2$. Let $b \equiv 1 \mod 8$. Then $|f(1)| = 2^{-3} < 2^{-2} = |f'(1)|^2$ so we can apply Hensel's Lemma. Thus we have that $b \in (\mathbb{Z}_2^\times)^2$ if and only if $b \equiv 1 \mod 8$, as if $b \not\equiv 1 \mod 8$, then $x^2 - b$ has no solutions in $\mathbb{Z}/8\mathbb{Z}$, and hence none in $\mathbb{Z}_2$. Thus we have that

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3. \tag{4.10}$$

□

We can prove another version of Hensel's lemma "for polynomials".

Theorem 4.5 (Hensel's Lemma, Version 2)**.** *Let $(K, |\cdot|)$ be a complete discrete valued field and $f(x) \in \mathcal{O}_K[x]$. Suppose that*

$$\overline{f}(x) \coloneqq f(x) \mod \mathfrak{m} \in K[x] \tag{4.11}$$

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

Proof. Example Sheet 1. Cauchy sequence of polynomials. □

Corollary 4.6. *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) = a_n x^n + \cdots + a_0 \in K[x]$ with $a_n, a_0 \neq 0$. If $f(x)$ is irreducible, then $|a_i| \leq \max(|a_0|, |a_n|)$ for all i.*

Proof. After scaling we may assume that $f(x) \in \mathcal{O}_K[x]$ with $\max(|a_i|) = 1$. Thus we need to show that $\max |a_0|, |a_n| = 1$. If not, let r be the minimal value such that $|a_r| = 1$, $0 < r < n$. Thus we have that

$$f(x) = x^r(a_r + \cdots + a_n x^{n-r}) \mod \mathfrak{m}. \tag{4.12}$$

This is a factorisation of $\overline{f}(x)$. Then Theorem 4.5 implies that the factorisation lifts to a factorisation $f(x) = g(x)h(x)$ with $0 < \deg g < n$, which is a contradiction as we have assumed that f is irreducible. □

5 Teichmüller Lifts

Definition 5.1. A ring R of prime characeristic $p > 0$ is a *perfect ring* if the Frobenius map $x \to x^p$. is a bijection.

A field of characteristic $p > 0$ is *perfect* if it is perfect as a ring.

By convention, a field of characteristic 0 is always perfect.

Remark 5.2. Since $\operatorname{char} R = p > 0$, $(x+y)^p = x^p + y^p$ so the Frobenius map is a ring homomorphism.

Example 5.3. (i) F_{p^n} and $\overline{F_{p^n}}$ are perfect fields.

(ii) $\mathbb{F}_p[t]$ is not perfect because $t \notin \operatorname{im}(\operatorname{Frob}_p)$.

(iii) $\mathbb{F}_p(t^{1/p^\infty}) = \mathbb{F}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$ is perfect (we add in all pth roots). This is the "perfection" of $\mathbb{F}_p(t)$, and gives rise to Scholze's thoery of perfectoid spaces.

Remark 5.4. A field of $\operatorname{char} p > 0$ is perfect if and only if any finite extension of K is separable, so that any irreducible polynomial in K has simple roots.

Theorem 5.5. *Let $(K, |\cdot|)$ be a complete discrete value field such that $k = \mathcal{O}_K/\mathfrak{m}$ is perfect of characteristic $\operatorname{char} k = p > 0$. Then there exists a unique map, the* Teichmüller map

$$[\cdot] : k \to \mathcal{O}_K \tag{5.1}$$

such that

(i) $a = [a] \mod \mathfrak{m}$ *for all* $a \in k$.

(ii) $[ab] = [a][b]$ *for all* $a, b \in k$.

Moreover, if $\operatorname{char} \mathcal{O}_K = p$*, then* $[a+b] = [a] + [b]$*, so* $[\cdot]$ *is a ring homomorphism.*

We do a little work before we prove the theorem.

Definition 5.6. The element $[a] \in \mathcal{O}_K$ constructed above is the *Teichm̈uller* lift of a.

Lemma 5.7. *Let* $(K, |\cdot|)$ *be as in Theorem 5.5, and fix a uniformizer* $\pi \in \mathcal{O}_K$*. Let* $x, y \in \mathcal{O}_K$ *such that* $x \equiv y \mod \pi^n$*. Then* $x^p \equiv y^p \mod \pi^{n+1}$*.*

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

$$x^p = y^p + \sum_{i=1}^{p} \binom{p}{i} y^{p-i}(u\pi^n)^i = y^p + py^{p-1}(u\pi^n) \mod \pi^{n+1}. \tag{5.2}$$

Since $\mathcal{O}_K/\pi\mathcal{O}_K$ has characteristic p, we have that $p \in \pi\mathcal{O}_K$, so $py^{p-1}(u\pi^n) \in \pi^{n+1}\mathcal{O}_K$. □

Proof of Theorem 5.5. Let $a \in k$. For each $i \geq 0$, we choose a lift $y_i \in \mathcal{O}_K$ of a^{1/p^i}, which exists because k is perfect. Define $x_i = y_i^{p^i}$.

Claim: (x_i) is Cauchy, and the limit is independent of the choice of y_i.

By construction, $y_i \equiv y_{i+1}^p \mod \pi$. By Lemma 5.7 and induction on n, we have that $y_i^{p^n} \equiv y_{i+1}^{p^{n+1}} \mod \pi^{n+1}$ and hence $x_i \equiv x_{i+1} \mod \pi^{i+1}$. So (x_i) is Cauchy, so $x_i \to x \in \mathcal{O}_K$.

Suppose (x_i') is another sequence arising from some sequence (y_i') of liftings of a_i^{1/p^i}. Then (x_i') is Cauchy and converges to some x'. Let

$$x_i'' = \begin{cases} x_i & i \text{ even} \\ x_i' & i \text{ odd} \end{cases} \tag{5.3}$$

Then x_i'' arises from the liftings

$$y_i'' = \begin{cases} y_i & i \text{ even} \\ y_i' & i \text{ odd} \end{cases} \tag{5.4}$$

Then $x_i'' \to x''$, and we obviously have that $x'' = x = x'$. So we can define $[a] = x$, and the previous argument shows that this is well defined. We want to show that $[a] = x$ is a valid Teichmüller lift. We have that

$$x_i = y_i^{p^i} = (a^{1/p^i})^{p^i} \equiv a \mod \pi \tag{5.5}$$

so $x \equiv a \mod \pi$. Let $b \in k$, so that $[b] = z$ with $z = \lim z_i$, where $z_i = u_i^{p^i}$ and $u_i = b^{1/p^i} \mod \mathfrak{m}$. Then $u_i y_i$ is a lift of $(ab)^{1/p^i}$, so $[ab] = \lim z_i x_i = zx = [a][b]$. If $\operatorname{char} \mathcal{O}_K = p$, then $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$, so $[a+b] = \lim(y_i + u_i)^{p^i} = \lim y_i^{p^i} + u_i^{p^i} = [a] + [b]$.

It's also easy to check that $[0] = 0$ and $[1] = 1$ as we can set $x_i = 0$ or $x_i = 1$, respectively.

For the uniqueness of the Teichmüller map, let $\phi : k \to \mathcal{O}_K$ be another such map. Then for all $a \in k$, $\phi(a^{1/p^i})$ is a lift of a^{1/p^i} and we can define another Teichmüller lift under this condition as before. Then $\phi(a) = [a]$, because

$$[a] = \lim \phi(a^{1/p^i})^{p^i} = \lim \phi(a) = \phi(a). \tag{5.6}$$

□

The key idea is that the Teichmüller map is a lifting of $a \in k$ which gets rid of all the "pth power imperfection". We take a lift of a^{1/p^i}, and then we take the p^ith power. Taking p^ith powers gets rid of all the p^ith root of unity stuff. The proof shows that no matter what lift we take we get the same result.

Example 5.8. If $K = \mathbb{Q}_p$, then $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$. If $a \in \mathbb{F}_p^\times$, then $[a]^{p-1} = [a^{p-1}] = [1] = 1$, so $[a]$ is a $(p-1)$th root of unity. So $\mathbb{Q}_p$ contains all $(p-1)$th roots unity since the Teichmüller lifts are all different as $[a] \equiv a \mod \mathfrak{m}$.

Lemma 5.9. *Let $(K, |\cdot|)$ be a complete discretely valued field. If $k = \mathcal{O}_K/\mathfrak{m} \subset \overline{\mathbb{F}_p}$ and $a \in k^\times$, then $[a]$ is a root of unity.*

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

Theorem 5.10. *Let $(K, |\cdot|)$ be a complete discretely valued field with* $\operatorname{char}(K) = p > 0$ *such that k is perfect. Then $K = k((t))$.*

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

$$\begin{aligned} \varphi : k[[t]] &\to \mathcal{O}_K \\ \varphi\left(\sum_{i=0}^{\infty} a_i t^i\right) &= \sum_{i=0}^{\infty} [a_i]\pi^i. \end{aligned} \tag{5.7}$$

Then φ is a ring homomorphism since $\operatorname{char}(K) = \operatorname{char} k = p$, and it is a bijection by Proposition 3.6 (ii). □

6 Extensions of Complete Value Fields

Let L/K be a finite extension of fields. Then we can think of L as a finite dimensional K vector space. Recall the field norm $N_{L/K} : L \to K$ defined by

$$N_{L/K}(y) = \det_K(\operatorname{mult}(y)), \tag{6.1}$$

where det is the determinant and $\operatorname{mult}(y)$ is the K-linear map given by $x \mapsto xy$. We have that $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$. If $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ is the minimal polynomial of $y \in L$, then $N_{L/K}(y) = \pm a_0^m$ for some a_0^m. So $N_{L/K}(y) = 0$ if and only if $y = 0$.

The following theorem which allows us to extend discrete valuations on K to those on L.

Theorem 6.1. *Let $(K, |\cdot|)$ be a complete discretely valued field and let L/K be a finite extension of degree n. Then*

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

$$|y|_L = |N_{L/K}(y)|^{1/n} \tag{6.2}$$

for all $y \in L$.

(ii) L is complete with respect to $|\cdot|_L$.

We build up some machinery before we prove this theorem.

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

(i) $\|x\| = 0$ if and only if $x = 0$.

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

(iii) $\|x + y\| \leq \max(\|x\|, \|y\|)$ for all $x, y \in V$ (ultrametric).

Example 6.3. If V is a finite dimensional over K and $e_1, \dots, e_n$ is a basis, then the supremum (sup) norm $\|\cdot\|_{\sup}$ on V is defined

$$\|x\|_{\sup} = \max_i |x_i \tag{6.3}$$

where $x = \sum x_i e_i$. It is an easy exercise to show that $\|\cdot\|_{\sup}$ is a norm.

Definition 6.4. Two norms $\|\cdot\|_1$, $\|\cdot\|_2$ on V are *equivalent* if there exists $C, D \in \mathbb{R}_{>0}$ such that

$$C\|x\|_1 \leq \|x\|_2 \leq D\|x\|_1 \tag{6.4}$$

for all $x \in V$.

Its easy to see that a norm defines a topology on V by the induced metric $d(x, y) = \|x - y\|$, and it follows that equivalent norms induce the same topology.

Proposition 6.5. *Let $(K, |\cdot|)$ be a complete, non-archimedean field, and V a finite dimensional vector space over K. Then V is complete with respect to $\|\cdot\|_{\sup}$.*

Proof. Let (v_i) be a Cauchy sequence in V and $e_1, \dots, e_n$ a basis for V. Write $v_i = \sum_j x_j^i e_j$. Then $(x_j^i)_{i=1}^\infty$ is Cauchy in K, so $(x_j^i) \to x_j \in K$. So then $v = \sum x_j e_j$ is the limit of v_i. □

Theorem 6.6. *Let $(K, |\cdot|)$ be a non-archimedean field, and let V be a finite dimensional vector space over K. Then any two norms on V are equivalent. In particular, they are equivalent to the sup norm, and hence V is complete with respect to any norm.*

Proof. Equivalence of norms defines an equivalence relation on the set of norms, so it suffices to show that any norm equivalent to the sup norm. Let $e_1, \dots, e_n$ be a basis for V, and $\|\cdot\|$ a norm on V. Set $D = \max_i \|e_i\| > 0$. Then for $x = \sum x_i e_i$, we have that

$$\|x\| \leq \max \|x_i e_i\| = \max |x_i|\|e_i\| \leq \max |x_i| D = D\|x\|_{\sup}. \tag{6.5}$$

We need to find C such that $C\|x\|_{\sup} \leq \|x\|$ for all $x \in K$. We proceed by induction on $\dim V$. For $n = 1$, we have that $\|x\| = |x_1|\|e_1\| = \|e_1\|\|x\|_{\sup}$ so we may take $C = \|e_1\|$.

For $n > 1$, assume the claim holds up to $n - 1$, and set $V_i = \operatorname{Span}\{e_1, \dots, \hat{e}_i, \dots, e_n\}$. This is an $(n-1)$-dimensional subspace, and $\|\cdot\|_{\sup}$ and $\|\cdot\|$ restrict to each V_i and are equivalent and complete by the inductive hypothesis. Since V_i is complete with respect to $\|\cdot\|$, it is closed. Then the translation $e_i + V_i$ is closed for all i, and hence

$$S = \bigcup_{i=1}^n (e_i + V_i) \tag{6.6}$$

is a closed subset not containing 0. So there exists an open ball around 0 of radius C not containing S.

Let $x = \sum x_i e_i$ and let j be an index where $|x_j| = \max_i |x_i|$. Then $\|x\|_{\sup} = |x_j|$ and $\frac{1}{x_j}x \in e_j + V_j \subset S$. Thus $\|\frac{1}{x_j}x\| \geq C$, so

$$\|x\| \geq C|x_j| = C\|x\|_{\sup} \tag{6.7}$$

as desired. □

We recall some facts about integral elements of rings.

Definition 6.7. Let $R \subset S$ be rings. We say that $s \in S$ is *integral* over R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(s) = 0$.

The *integral closure* $R^{\mathrm{int}(S)}$ of R inside S is the set of all elements of S which are integral over R.

The ring R is *integrally closed* in S if $R^{\mathrm{int}(S)} = R$.

We will sometimes say that R is *integrally closed* if it is integrally closed in $\mathrm{Frac}(R)$.

Proposition 6.8. *$R^{\mathrm{int}(S)}$ is a subring of S. Moreover, $R^{\mathrm{int}(S)}$ is integrally closed in S.*

Proof. Example Sheet 2. □

Lemma 6.9. *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, and assume that $x \neq 0$. Let $x^n + a_{n-1}x^{n-1} + \cdots a_0 = 0$ for some $a_i \in \mathcal{O}_K$. Then

$$x = -a_{n-1}x^0 - a_{n-2}x^{-1} - \cdots - a_0 x^{-n+1}. \tag{6.8}$$

If $|x| > 1$, we have that the RHS has absolute valued less than 1, which is a contradiction. Thus $|x| \leq 1$, so $x \in \mathcal{O}_K$. □

Set

$$\mathcal{O}_L = \{y \in L \mid |y|_L \leq 1\} \tag{6.9}$$

where $|\cdot|_L$ is the map defined in (6.2) (which we do not yet know is an absolute value).

Lemma 6.10. *$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ inside L.*

Proof. Let $y \in L^\times$ and $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$ be the minimal polynomial of y over K.

Claim: y is integral over $\mathcal{O}_K$ if and only if $f(x) \in \mathcal{O}_K[x]$.

If $f(x) \in \mathcal{O}_K[x]$, then y is integral over $\mathcal{O}_K$ by definition.

So let y be integral over $\mathcal{O}_K$, so there exists a monic polynomial $g(x) \in \mathcal{O}_K[x]$ such that $g(y) = 0$. Then $f \mid g$ in $K[x]$ as f is the minimal polynomial of y, so every root of f is a root of g. But then every root of f in $\overline{K}$ is integral over $\mathcal{O}_K$ But then each a_i is integral over $\mathcal{O}_K$ because each a_i is a sum of products of roots (Vieta's formula). But then $a_i \in \mathcal{O}_K$ because $\mathcal{O}_K$ is integrally closed over K by Lemma 6.9, which proves the claim.

Now, by Corollary 4.6 we have that $|a_i| \leq \max(|a_0|, 1)$, and by the properties of the norm, $N_{L/K}(y) = \pm a_0^m$ for some $m \geq 1$. Then

$$\begin{aligned} y \in \mathcal{O}_L &\iff |N_{L/K}(y)| \leq 1 \\ &\iff |a_0| \leq 1 \\ &\iff |a_i| \leq 1 \forall i \\ &\iff a_i \in \mathcal{O}_K \forall i \\ &\iff f(x) \in \mathcal{O}_K[x] \\ &\iff y \text{ is integral over } \mathcal{O}_K \end{aligned} \tag{6.10}$$

which shows that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L. □

It is now fairly easy to prove our big theorem.

Proof of Theorem 6.1. (i) We need to show that $|\cdot|_L = |N_{L/K}(\cdot)|^{1/n}$ satisfies the absolute value axioms.

First we have that $|y|_L = 0$ if and only if $|N_{L/K}(y)| = 0$ if and only if $N_{L/K}(y) = 0$ if and only if $y = 0$.

Next we have that $|y_1 y_2|_L = |N_{L/K}(y_1 y_2)|^{1/n} = |y_1|_L |y_2|_L$ because $N_{L/K}$ is a norm, and hence multiplicative.

Finally, we need to show that ultrametric inequality holds. Let $x, y \in L$ and WLOG assume that $|x|_L \leq |y|_L$. Then $|x/y|_L \leq 1$, so $x/y \in \mathcal{O}_L$. Since $1 \in \mathcal{O}_L$ and $\mathcal{O}_L$ is a ring by Lemma 6.10, we have that $1 + x/y \in \mathcal{O}_L$ and hence $|1 + x/y|_L \leq 1$. Then $|x + y|_L \leq |y|_L = \max |x|_L, |y|_L$ which is the ultrametric inequality so $|\cdot|_L$ is an absolute value.

We have that $N_{L/K}(x) = x^n$ for all $x \in K$, so $|\cdot|_L$ restricts to $|\cdot|$ on K. IF $|\cdot|_L'$ is another absolute value on L extending $|\cdot|$, then $|\cdot|_L, |\cdot|_L'$ are norms on L considered as a K-vector space. By Theorem 6.6, $|\cdot|_L$ and $|\cdot|_L'$ are equivalent norms, so they induce same topology. Thus by Proposition 1.6 we have that $|\cdot|_L' = |\cdot|_L^c$ for some c. Since both norms extend $|\cdot|$, we have that $c = 1$, so $|\cdot|_L' = |\cdot|_L$.

(ii) This also follows from Theorem 6.6. □

Corollary 6.11. *Let L/K be a finite field extension and let $(K, |\cdot|)$ be a complete discretely valued field. Then*

(i) L is discretely valued with respect to $|\cdot|_L$.

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

Proof. (i): Set $[L : K] = n$. Let v be the valuation on K, and v_L the valuation on L which extends v. Then for all $y \in L^\times$, $|y|_L = |N_{L/K}(y)|^{1/n}$, so $v_L(y) = \frac{1}{n}(N_{L/K}(y))$, so $\operatorname{im} v_L(L^\times) \subset \frac{1}{n}\mathbb{Z}$.

(ii): This is Lemma 6.10. □

We can extend our results to the algebraic closure of K, which is the profinite limit of all the finite extensions of K, and hence behaves like a finite extension in many ways.

Corollary 6.12. *Let $\overline{K}/K$ be an algebraic closure of K. Then $|\cdot|$ extends uniquely to $|\cdot|_{\overline{K}}$ on $\overline{K}$.*

Proof. Let $x \in \overline{K}$. Then $x \in L$ for some finite extension L/K, and we can set $|x|_{\overline{K}} = |x|_L$. This is well-defined (independent of the choice of L) by the uniqueness part of Theorem 6.1. In particular, if $x \in L'$, then $x \in LL'$, and $|x|_L = |x|_{L'} = |x|_{LL'}$.

We can check the other axioms similarly using compositums. □

Remark 6.13.

1. $|\cdot|_{\overline{K}}$ on $\overline{K}$ extending $|\cdot|$ on K is never discrete. If $|x| = 1$, then $|x|^{1/n} = 1/n$, and $|x|^{1/n^2} = 1/n^2$, and so on.

2. $\overline{\mathbb{Q}_p}$ is *not* complete with respect to $|\cdot|_{\overline{\mathbb{Q}_p}}$. If $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_{\overline{\mathbb{Q}_p}}$, then $\mathbb{C}_p$ *is* algebraically closed, which ends our tower of alternating completions and algebraic closures:
$$\mathbb{Q} \subset \mathbb{Q}_p \subset \overline{\mathbb{Q}_p} \subset \mathbb{C}_p \tag{6.11}$$

Proposition 6.14. *Let L/K be a finite extension of complete DV fields. Assume that:*

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

(ii) The extension of residue fields k_L/k is finite and separable (in fact this follows from (i)).

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

Proof. We'll choose $\alpha \in \mathcal{O}_L$ such that there exists $\beta \in \mathcal{O}_K[\alpha]$ which is a uniformizer for $\mathcal{O}_L$ and $\mathcal{O}_K[\alpha] \twoheadrightarrow k_L$ is surjective.

Since k_L/k is separable, there exists $\overline{\alpha} \in k_L$ such that $k_L = k(\overline{\alpha})$. Let $\overline{g}(x) \in k[x]$ be the minimal polynomial for $\overline{\alpha}$. Let $\alpha \in \mathcal{O}_L$ be a lift of $\overline{\alpha}$, and let $g(x) \in \mathcal{O}_K[x]$ be a monic lift of $\overline{g}(x)$. Fix a uniformizer $\pi_L \in \mathcal{O}_L$. Then $\overline{g}(x) \in K[x]$ is irreducible and separable, so $g(\alpha) = 0 \mod \pi_L$ and $g'(\alpha) \neq 0 \mod \pi_L$. If $g(\alpha) \neq 0 \mod \pi_L^2$, then we can take $\beta = g(\alpha)$, because $v_L(g(\alpha)) = 1$. If $g(\alpha) = 0 \mod \pi_L^2$, then
$$g(\alpha + \pi_L) = g(\alpha) + \pi_L g'(\alpha) \mod \pi_L^2. \tag{6.12}$$
Thus
$$v_L(g(\alpha + \pi_L)) = v_L(\pi_L g'(\alpha)) = 1. \tag{6.13}$$
$\alpha + \pi_L$ is also a lift of $\overline{\alpha}$, so we may replace α by $\alpha + \pi_L$, and thus we may assume that $v_L(g(\alpha)) = 1$, so that $\beta = g(\alpha)$ is a uniformizer for $\mathcal{O}_L$ in $\mathcal{O}_K[\alpha]$. Then $\mathcal{O}_K[\alpha] \subset L$ is the image of a continuous map
$$\begin{aligned} \mathcal{O}_K^n &\to L \\ (x_0, \dots, x_{n-1}) &\mapsto \sum x_i \alpha^i \end{aligned} \tag{6.14}$$
where $n = [K(\alpha) : K]$. Since $\mathcal{O}_K$ is compact, we have that $\mathcal{O}_K[\alpha] \subset L$ is compact and hence closed. Since $k_L = k(\overline{\alpha})$, $\mathcal{O}_K[\alpha]$ contains a set of coset representatives for $k_L = \mathcal{O}_L/\beta\mathcal{O}_L$. Let $y \in \mathcal{O}_L$. By Proposition 3.6 (ii), $y = \sum \lambda_i \beta^i$ for some $\lambda_i \in \mathcal{O}_K[\alpha]$. But $y_m = \sum_{i=0}^m \lambda_i \beta^i \in \mathcal{O}_K[\alpha]$ for each m, so $y \in \mathcal{O}_K[\alpha]$ because $\mathcal{O}_K[\alpha]$ is closed. □

Part III
Local Fields

7 Basic Properties of Local Fields

A topological space X is said to be *locally compact* if for all $x \in X$, there exists an open set U and a compact set C such that $x \in U \subset C$.

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

For example, $\mathbb{R}$ and $\mathbb{C}$ are local fields under the usual Euclidean absolute value.

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

(i) K is locally compact.

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

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

Proof. (i) $\implies$ (ii): Let U be a compact neighborhood of 0, so that U is open and there is a compact Z such that $0 \in U \subset Z$. Then there exists $x \in \mathcal{O}_K$ such that $x\mathcal{O}_K \subset U$. Since $x\mathcal{O}_K$ is closed, we have that $x\mathcal{O}_K$ is compact, so $\mathcal{O}_K$ is compact.

(ii) $\implies$ (i): $\mathcal{O}_K$ is compact, so $a + \mathcal{O}_K$ is compact, so K is locally compact.

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

$$\mathcal{O}_K = \bigsqcup_{y \in A_x} y + x\mathcal{O}_K \tag{7.1}$$

is a disjoint open cover. But since $\mathcal{O}_K$ is compact, A_x is finite, so $\mathcal{O}_K/x\mathcal{O}_K$ is finite, so k is finite.

Suppose v is not discrete and let $x_1, x_2, \ldots$ be a sequence such that $v(x_1) > v(x_2) > \cdots > 0$. Then $x_1\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq \cdots \subsetneq \mathcal{O}_K$, but the union of $x_i\mathcal{O}_K$ covers $\mathcal{O}_K$, which is a contradiction as $\mathcal{O}_K$ is compact and there is no finite subcover.

(iii) $\implies$ (ii): Since $\mathcal{O}_K$ is a metric space, it suffices to show that $\mathcal{O}_K$ is *sequentially compact*, so that every sequence has a convergent subsequence. Let (x_n) be a sequence in $\mathcal{O}_K$ and π a uniformizer. Since $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong k$, we have that $\mathcal{O}_K/\pi^i\mathcal{O}_K$ is finite for all i. Since $\mathcal{O}_K/\pi\mathcal{O}_K$ is finite, there exists an infinite subsequence such that $x_{1,n} \equiv a_1 \mod \pi$ for all n for some a_1. Continuing, we get subsequences $x_{i,n} \equiv a_i \mod \pi^i$ such that $a_i \equiv a_{i+1} \mod \pi^i$. Setting $y_i = x_{ii}$, we have that $y_i \equiv a_i \equiv a_{i+1} \equiv y_{i+1} \mod \pi^i$, so y_i is Cauchy, and hence convergent. □

The above proposition tells us that a complete DV field with finite residue field is a local field. As a consequence, $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are local fields.

7.1 More on inverse limits

Let (A_n) be a sequence of sets/groups/rings and $\varphi_n : A_{n+1} \to A_n$ a homomorphism between these objects. Assume that each A_n is finite.

Definition 7.3. The *profinite topology* on $A = \varprojlim A_n$ is the weakest topology on A such that $\theta_n : A \to A_n$ is continuous for all n, where A_n has the discrete topology.

When equipped with the profinite topology, $A = \varprojlim A_n$ is compact, totally disconnected, and Hausdorff.

Proposition 7.4. *Let K be a non-archimedean local field. Under the isomorphism*

$$\mathcal{O}_K \cong \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K, \tag{7.2}$$

the topology on $\mathcal{O}_K$ is the same as the profinite topology.

Proof. We can check that the sets

$$B = \{a + \pi^n\mathcal{O}_K \mid n \in \mathbb{N}_{\geq 1}, a \in \mathcal{O}_K\} \tag{7.3}$$

are a basis of open sets for both topologies. For $|\cdot|$ this is clear because the open/closed balls are closed/open. For the profinite topology, $\mathcal{O}_K \to \mathcal{O}_K/\pi^n\mathcal{O}_K$ is continuous if and only if $a + \pi^n\mathcal{O}_K$ is open for all $a \in \mathcal{O}_K$. □

7.2 Classification of Local Fields

It turns out that the property of being a local field is quite restrictive, and in fact we can classify all of them as being one of three simple types in Corollary 7.13

Lemma 7.5. *Let K be a non-archimedean local field and L/K a finite extension. Then L is also a local field.*

Proof. Theorem 6.1 implies that L is complete and discretely valued. So it suffices to show that $k_L \coloneqq \mathcal{O}_L/\mathfrak{m}_L$ is finite and then apply Proposition 7.2. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L as a K-vector space. As the sup norm is equivalent to $|\cdot|_L$, we have that there exists an $r > 0$ such that $\mathcal{O}_L \subset \{x \in L \mid \|x\|_{\sup} \leq r\}$. Take some $a \in K$ such that $|a| \geq r$. Then

$$\mathcal{O}_L \subset \bigoplus_{i=1}^{n} a\alpha_i\mathcal{O}_K \subset L \tag{7.4}$$

which implies that $\mathcal{O}_L$ is finitely generated as a module over $\mathcal{O}_K$, so k_L is finitely generated as a module over k, so k_L is finite because k is. □

Definition 7.6. A non-archimedean valued field $(K, |\cdot|)$ with residue field k has *equal characteristic* if $\text{char}(K) = \text{char}(k)$. Otherwise it has *mixed characteristic.*

Example 7.7. $\mathbb{Q}_p$ has mixed characteristic because $\text{char}(\mathbb{Q}_p) = 0$ but $\text{char}(\mathbb{Z}_p/p\mathbb{Z}_p) = p$.

Remark 7.8. If K is a local field, we always have $\text{char}(k) > 0$ by Proposition 7.2, so K has equal characteristic if and only if $\text{char}(K) > 0$ as well.

Theorem 7.9. *Let K be a non-archimedean local field of equal characteristic $p > 0$. Then $K \cong \mathbb{F}_{p^n}((t))$ for some p and some $n \geq 1$.*

Proof. K is complete, discretely valued, and $\operatorname{char} K > 0$. Moreover $k \cong \mathbb{F}_{p^n}$ is finite, and hence perfect. Then by Theorem 5.10 we have that $K \cong \mathbb{F}_{p^n}((t))$. □

Lemma 7.10. *An absolute value $|\cdot|$ on a field K is non-archimedean if and only if $|n|$ is bounded for all $n \in \mathbb{Z}$.*

Proof. Assume that $|\cdot|$ is non-archimedean. Since $|-1| = |1| = 1$, we have that $|-n| = |n|$, so it suffices to show that result for $\mathbb{Z}_{\geq 1}$. We have that $|n| \leq \max |n-1|, 1$, so by induction $|n| \leq |1| = 1$.

Now suppose $|n| \leq B$ for all $n \in \mathbb{Z}$ for some $B \in \mathbb{R}_{>0}$. Let $x, y \in K$ and WLOG assume that $|x| \leq |y|$. Then we have that

$$\begin{aligned} |x+y|^m &= \left| \sum_{i=0}^{m} \binom{m}{i} x^i y^{m-i} \right| \\ &\leq \sum_{i=0}^{m} \left| \binom{m}{i} x^i y^{m-i} \right| \\ &\leq B(m+1)|y|^m. \end{aligned} \tag{7.5}$$

Taking mth roots gives $|x+y| \leq (B(m+1))^{1/m}|y|$. As $m \to \infty$ we have that $(B(m+1))^{1/m} \to 1$, so $|x+y| \leq |y|$. □

Theorem 7.11 (Ostrowski)**.** *Any non-trivial absolute value on $\mathbb{Q}$ is $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.*

Proof. We divide into the case where $|\cdot|$ is and is not archimedean.

Case 1: $|\cdot|$ is archimedean. By Lemma 7.10, $|\cdot|$ is unbounded on $\mathbb{Z}$. We fix $b > 1$ an integer such that $|b| > 1$. Let $a > 1$ be an integer and write b^n in base a:

$$b^n = c_m a^m + c_{m-1} a^{m-1} + \cdots + c_0 \tag{7.6}$$

for $0 \leq c_i < a$, $c_m \neq 0$, where $m \leq \log_a b^n = n \log_a b$. Let $B = \max_{0 \leq c \leq a-1} |c|$. Then we have that

$$|b^n| \leq (m+1)B \max(|a|^m, 1) \tag{7.7}$$

so

$$|b| \leq [n(\log_a b + 1)B]^{1/n} \max(|a|^{\log_a b}, 1) \tag{7.8}$$

Taking $n \to \infty$, we have that $|b| \leq \max(|a|^{\log_a b}, 1)$. Since $|b| > 1$, we have that $|a| > 1$, so

$$|b| \leq |a|^{\log_a b}. \tag{7.9}$$

Since $|a| > 1$, we can swap a and b and write

$$|a| \leq |b|^{\log_b a} \tag{7.10}$$

Then (7.9) and (7.10) give

$$\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} = \lambda \tag{7.11}$$

for some $\lambda \in \mathbb{R}_{>0}$. Then $|a| = a^\lambda$ for all $a \in \mathbb{Z}_{>1}$. Then by $\mathbb{Q} = \mathbb{Z}^{-1}\mathbb{Z}$, we have that $|x| = x^\lambda$ for all $x \in \mathbb{Q}$, so $|\cdot| = |\cdot|_\infty$.

Case 2: $|\cdot|$ is non-archimedean. As in Lemma 7.10, we have that $|n| \leq 1$ for all $n \in \mathbb{Z}$. But since $|\cdot|$ is nontrivial, there exists $n \in \mathbb{Z}_{>1}$ such that $|n| < 1$. Write $n = p_1^{e_1} \cdots p_r^{e_r}$. Then $|p| < 1$ for some $p = p_i$. Suppose $|q| < 1$ for some $q \neq p$. Then by Bezout's we have that $rp + sq = 1$, so $|1| \leq \max(rp, sq) < 1$, which is a contradiction. So $|sq| = 1$, so $|q| = 1$. So p is the unique prime with $|p| < 1$, so $|\cdot| = |\cdot|_p$. □

Theorem 7.12. *Let $(K, |\cdot|)$ be a non-archimedean local field of mixed characteristic. Then K is a finite extension of $\mathbb{Q}_p$.*

Proof. As K has mixed characteristic, $\operatorname{char} K = 0$. Thus $\mathbb{Q} \subset K$, and since $|\cdot|$ is non-archimedean, $|\cdot|$ restricted to $\mathbb{Q}$ is $|\cdot|_p$ for some p. But K is complete, so $\mathbb{Q}_p \subset K$.

Thus it suffices to show that K is a finite dimensional $\mathbb{Q}_p$ vector space, so it suffices to show that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}_p$-module. Let $\pi \in \mathcal{O}_K$ be a uniformizer, and set $v(p) = e$. Then $\mathcal{O}_K/p\mathcal{O}_k \cong \mathcal{O}_k/\pi^e\mathcal{O}_K$ if finite. WE have that

$$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K, \tag{7.12}$$

so $\mathcal{O}_K/p\mathcal{O}_K$ is a finite dimensional $\mathbb{F}_p$-vector space. Let $x_1, \ldots, x_n \in \mathcal{O}_K$ be coset representatives of $\{e_1, \ldots, e_n\}$, where $\{e_1, \ldots, e_n\}$ is a basis for $\mathcal{O}_K/p\mathcal{O}_K$ over $\mathbb{F}_p$. Then

$$\left\{ \sum_{j=1}^{n} a_j x_j \mid a_i \in \{0, \ldots, p-1\} \right\} \tag{7.13}$$

is a set of coset representatives for $\mathcal{O}_K/p\mathcal{O}_K$. Let $y \in \mathcal{O}_K$. By Proposition 3.6 (ii), for any $y \in \mathcal{O}_K$, we have that

$$y = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{n} a_{ij} x_j \right) p^i = \sum_{j=1}^{n} \left(\sum_{i=0}^{\infty} a_{ij} p^i \right) x_j \in x_1\mathbb{Z}_p + x_2\mathbb{Z}_p + \cdots + x_n\mathbb{Z}_p \tag{7.14}$$

so $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}_p$-module with generators $(x_1, \ldots, x_n)$. □

On Example Sheet 2, we show that if K is complete and archimedean, then either $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$. This completes the classification, which we summarize below.

Corollary 7.13. *If K is a local field, then either*

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

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

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

8 Global Fields

Although the term "global field" sounds like the opposite of "local field", the two are closely connected. In fact, a local field is just the completion of a global field under some absolute value (Theorem 8.5), so we can think of global fields as "incomplete" local fields.

Definition 8.1. A *global field* is a field which is either

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

Proof. Since $x \to |\sigma(x)|_L$ is another absolute value on L extending $|\cdot|_K$, this follows from the uniqueness of $|\cdot|_L$. □

The next lemma is very useful.

Lemma 8.3 (Krasner). *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(x) \in K[x]$ a separable and irreducible polynomial with roots $\alpha_1, \ldots, \alpha_n \in K^{\mathrm{sep}}$ the separable closure of K. Suppose we have $\beta \in K^{\mathrm{sep}}$ with $|\beta - \alpha_1| < |\beta - \alpha_i|$ for $i = 2, \ldots, n$. Then $\alpha_1 \in K(\beta)$.*

Proof. Let $L = K(\beta)$, $L' = L(\alpha_1, \ldots, \alpha_n)$. Then L'/L is a Galois extension. Let $\sigma \in \mathrm{Gal}(L'/L)$. We have that $|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1|$ by Lemma 8.2. But $\sigma(\alpha_1) = \alpha_i$ for some i, and $|\beta - \alpha_i| \neq |\beta - \alpha_1|$ unless $i = 1$, so $\sigma(\alpha_1) = \alpha_1$, so $\alpha_1 \in L = K(\beta)$. □

The next proposition is very important. It tells us, roughly, that "nearby polynomials define the same extension".

Proposition 8.4. *Let $(K, |\cdot|)$ be a complete DV field and let $f(x) = \sum a_i x^i \in \mathcal{O}_K[x]$ be separable, irreducible, and monic. Let $\alpha \in K^{\mathrm{sep}}$ be a root of f. Then there exists $\epsilon > 0$ such that for any $g(x) = \sum b_i x^i \in \mathcal{O}_K[x]$ monic with $|a_i - b_i| < \epsilon$, $g(x)$ has a root β such that $K(\alpha) = K(\beta)$.*

Proof. Let $\alpha_1, \ldots, \alpha_n \in K^{\mathrm{sep}}$ be the roots of f. These are distinct because f is separable, so $f'(\alpha_1) \neq 0$. We choose ϵ small enough so that $|g(\alpha_1)| < |f'(\alpha_1)|^2$ and $|f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha_1)|$, and hence $|f'(\alpha_1)| = |g'(\alpha_1)|$ by the reverse ultrametric inequality Lemma 1.10. We can choose ϵ small enough because g is a continuous function in its coefficients and $|f(\alpha_1)| = 0$.

Then we have that $|g(\alpha_1)| < |f'(\alpha_1)|^2 = |g'(\alpha_1)|^2$, so we can apply Hensel's lemma. Applying Hensel's lemma to $K(\alpha_1)$, we have that there exists $\beta \in K(\alpha_1)$ such that $g(\beta) = 0$ and $|\beta - \alpha_1| < |g'(\alpha_1)|$. Then

$$\begin{aligned} |g'(\alpha_1)| &= |f'(\alpha_1)| \\ &= \prod_{i=2}^{n} |\alpha_1 - \alpha_i| \\ &\leq |\alpha_1 - \alpha_i \qquad (8.1) \end{aligned}$$

because $|\alpha_1 - \alpha_i| \leq 1$ because the α_i are integral. Since $|\beta - \alpha_1| < |\alpha_1 - \alpha_i| = |\beta - \alpha_i|$, we can apply Krasner's Lemma 8.3 which gives that $\alpha_1 \in K(\beta)$, so $K(\beta) = K(\alpha_1)$. □

Theorem 8.5. *Let $(K, |\cdot|)$ be a local field. Then K is the completion of a global field.*

Proof. We divide into three cases as in the classification of local fields.

Case 1: $|\cdot|$ is archimedean. We have that $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$, so $K = \hat{\mathbb{Q}}$ or $K = \widehat{\mathbb{Q}(i)}$.

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

Case 3: $|\cdot|$ is non-archimedean, mixed characteristic. We have that $K = \mathbb{Q}_p(\alpha)$, where α is the root of a monic, irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, then we can approximate $f(x)$ be $g(x) \in \mathbb{Z}[x]$ by Proposition 8.4. Then $K = \mathbb{Q}_p(\beta)$, where β is a root of $g(x)$. Since $\mathbb{Q}(\beta)$ is dense in $\mathbb{Q}_p(\beta)$, K is the completion of $\mathbb{Q}(\beta)$ with respect to v_p by the unique extension of v_p to $\mathbb{Q}(\beta)$. □

Part IV
Dedekind Domains

9 Basic Theory

Definition 9.1. A Dedekind domain is a ring R satisfying

(i) R is a Noetherian integral domain.

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

(iii) Every nonzero prime ideal is maximal.

Example 9.2. Here are a couple examples of Dedekind domains.

1. $\mathcal{O}_K$, where K is a number field.
2. Any PID (and hence any DVR).

We have the following important theorem connected DVRs and Dedekind domains.

Theorem 9.3. *A ring R is a DVR if and only if R is a Dedekind domain with exactly one nonzero prime ideal.*

We need to develop some theory from commutative algebra before we prove this.

Lemma 9.4. *Let R be a Noetherian ring and $I \subset R$ a nonzero ideal. Then there exists nonzero prime ideal $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset I$.*

Proof. Suppose not. Then since R is Noetherian, there exists a maximal ideal I satisfying this property. Then I is not prime, so there exists $x, y \in R \setminus I$ such that $xy \in I$. But then $I_1 = I + (x)$ and $I_2 = I + (y)$ are ideals which properly contain I. Then by the maximality of I, there exists $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I_1$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I_2$, so

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I_1 I_2 \subset I, \tag{9.1}$$

which is a contradiction. □

Lemma 9.5. *Let R be an integral domain which is integrally closed. Let $0 \neq I \subset R$ be a finitely generated ideal and let $x \in K = R^{-1}R$. Then if $xI \subset I$, then $x \in R$.*

Proof. Let $I = (c_1, \ldots, c_n)$ and suppose $xI \subset I$. We write $xc_i = \sum_j a_{ij}c_j$ for some $a_{ij} \in R$. Let A be the matrix $A = (a_{ij})$ and set $B = x\,\mathrm{id}_n - A \subset \mathrm{Mat}_{n\times n}(K)$. Then $B \cdot \vec{c_i} = 0$ in K^n. Let $\mathrm{Adj}(B)$ be the adjugate matrix for B, so that $\mathrm{Adj}(B) \cdot B \cdot \vec{c_i} = \det B\, \mathrm{id}_n\, \vec{c_i} = 0$, so $\det B = 0$. But $\mathrm{Det}\, B$ is a monic polynomial in x with coefficients in R. So $x \in R$ because R is integrally closed. □

We are now ready to prove our big theorem.

Proof of Theorem 9.3. First R be a Dedekind with exactly one prime. We just need to show that R is a PID. Let $\mathfrak{m}$ be the unique maximal ideal of R.

Claim 1: $\mathfrak{m}$ is principal. Let $0 \neq x \in \mathfrak{m}$. By Lemma 9.4, $(x) \supset \mathfrak{m}^n$ for some $n \geq 1$. Let n be the minimal value such that this is true. Then we can choose $y \in \mathfrak{m}^{n-1}$ such that $y \notin (x)$. Set $\pi = x/y \in K$. Then we have that $y\mathfrak{m} \subset \mathfrak{m}^n \subset (x)$, so $\pi^{-1}\mathfrak{m} \subset R$. Thus $\pi^{-1}\mathfrak{m}$ is an ideal of R. If $\pi^{-1}\mathfrak{m} \subset m$, then $\pi^{-1} \in R$ by Lemma 9.5, so $y \in (x)$, which is a contradiction. Thus $\pi^{-1}\mathfrak{m} = R$ since $\mathfrak{m}$ is the unique maximal ideal, so $\mathfrak{m} = \pi R$ is principal.

Claim 2: R is a PID. Let $I \subset R$ be any nonzero ideal. Consider the sequence of fractional ideals

$$I \subset \pi^{-1}I \subset \pi^{-2}I \subset \cdots \tag{9.2}$$

in K. These are all finitely generated as $\mathcal{O}_K$-modules. Then since $\pi^{-1} \notin R$, we have that $\pi^{-k}I \neq \pi^{-(k+1)}I$ by Lemma 9.5. Therefore, since R is Noetherian, we may choose a maximal n such that $\pi^{-n}I \subset R$ (since R is Noetherian and we have an infinite chain of fractional ideals, eventually this chase must exit R). If $\pi^{-n}I \subset \mathfrak{m} = (\pi)$, then $\pi^{-(n+1)} \subset R$. So we must have that $\pi^{-n}I = R$ because $\mathfrak{m}$ is maximal, so then $I = (\pi^n)$. □

The Localization of a Dedekind domain is a DVR.

This fact is very nice, and helps one understand Dedekind domains (or DVRs).

We recall some facts about localizations. Let R be an integral domain and S a multiplicatively closed set. Recall the localization $S^{-1}R$, and if $S = R \setminus \mathfrak{p}$ for $\mathfrak{p}$ a prime ideal, then we write $S^{-1}R = R_{\mathfrak{p}}$.

Example 9.6. If $R = \mathbb{Z}$, then

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid a \in \mathbb{Z}, (b,p) = 1\right\} \tag{9.3}$$

If R is Noetherian, then $S^{-1}R$ is Noetherian. The prime ideals in $S^{-1}R$ are in bijection with the prime ideals of R such that $S \cap \mathfrak{p} = \emptyset$.

Corollary 9.7. *Let R be a Dedekind domain and $\mathfrak{p} \subset R$ a nonzero prime ideal. Then $R_{(\mathfrak{p})}$ is a DVR.*

Proof. By the properties of localization, $R_{(p)}$ is a Noetherian integral domain and has a unique nonzero prime ideal. It suffices to show that $R_{\mathfrak{p}}$ is integrally closed in $\mathrm{Frac}(R_{\mathfrak{p}}) = \mathrm{Frac}(R)$ and then apply Theorem 9.3. Let $x \in \mathrm{Frac}(R)$ be integral over $R_{\mathfrak{p}}$. Then $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for some

$a_i = b_i/s_i \in \mathbb{R}_{\mathfrak{p}}$. Then multiplying by $s = s_1 \cdots s_{n-1}$, we have that $sx^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$ for some $c_i \in R$. Multiplying by s^{n-1}, we have that xs is integral over R, so $xs \in R$, so $x \in R_{\mathfrak{p}}$ since $s \in R \setminus \mathfrak{p}$. □

Definition 9.8. If R is a Dedekind domain and $\mathfrak{p} \subset R$ is a nonzero prime ideal, we write $v_{\mathfrak{p}}$ for the normalized valuation on $\mathrm{Frac}(R) = \mathrm{Frac}(R_{\mathfrak{p}})$ corresponding to the DVR $R_{\mathfrak{p}}$, given by $v(x/y) = v(x) - v(y)$ for $x, y \in R_{\mathfrak{p}}$.

Example 9.9. If $R = \mathbb{Z}$, then $v_p = v_{(p)}$ is the p-adic valuation.

Theorem 9.10. *Let R be a Dedekind domain. Then every nonzero ideal $I \subset R$ can be written uniquely as a product of prime ideals*

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \tag{9.4}$$

where $e_i \geq 1$ and the $\mathfrak{p}_i$ are distinct.

This theorem is immediate if R is a PID, as any PID is a UFD. We also need the following results on localizations.

Lemma 9.11. *Let I, J be ideals in a commutative ring R. Then $I = J$ if and only if $IR_{\mathfrak{m}} = JR_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m} \subset R$.*

Lemma 9.12. *If R is a Dedekind domain, and $\mathfrak{p}_1, \mathfrak{p}_2$ are two nonzero prime ideals, then*

$$\mathfrak{p}_1 R_{\mathfrak{p}_2} = \begin{cases} \mathfrak{p}_2 R_{\mathfrak{p}_2} & \mathfrak{p}_1 = \mathfrak{p}_2 \\ R_{\mathfrak{p}_2} & \textit{otherwise.} \end{cases} \tag{9.5}$$

Proof of Theorem 9.10. Let $I \subset R$ be a nonzero ideal. By Lemma 9.4 there are distinct prime ideal $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_r^{\beta_r} \subset I$, where $\beta_i > 0$. Let $\mathfrak{p} \neq 0$ be such that $\mathfrak{p} \neq \mathfrak{p}_i$ for all i. Then by Lemma 9.12, we have that $\mathfrak{p}_i R_{\mathfrak{p}} = R_{\mathfrak{p}}$, so $IR_{\mathfrak{p}} = R_{\mathfrak{p}}$. Since $R_{\mathfrak{p}_i}$ is a DVR by Corollary 9.7, we have that $IR_{\mathfrak{p}_i} = (\mathfrak{p}_i R_{\mathfrak{p}_i})^{\alpha_i} = \mathfrak{p}_i^{\alpha_i} R_{\mathfrak{p}_i}$ for some $0 \leq \alpha_i \leq \beta_i$. Thus $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ because $IR_{\mathfrak{p}} = (\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}) R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec} R$. If $I = \mathfrak{p}_1^{\gamma_1} \cdots \mathfrak{p}_r^{\gamma_r}$, then $\mathfrak{p}_i^{\alpha_i} R_{\mathfrak{p}_i} = \mathfrak{p}_i^{\gamma_i} R_{\mathfrak{p}_i}$ so $\alpha_i = \gamma_i$ by the unique factorization property of DVRs. □

10 Dedekind domains and extensions

Let L/K be a finite extension. For $x \in L$, we write $\mathrm{Tr}_{L/K}(x) \in K$ to be the trace of the K-linear map $L \to L$ given by $x \mapsto xy$. If L/K is a separable extension of degree n and $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ are the set of embeddings of L into an algebraic closure of K, then

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x). \tag{10.1}$$

This is invariant under any K-automorphism of $\overline{K}$ (any element of $\mathrm{Gal}(\overline{K}/K)$, so $\mathrm{Tr}_{L/K}(x) \in K$.

Lemma 10.1. *Let L/K be a finite separable extension of fields of degree n. Then the symmetric bilinear form*

$$\begin{aligned} (\cdot,\cdot) : L \times L &\to K \\ (x, y) &\mapsto \mathrm{Tr}_{L/K}(xy) \end{aligned} \tag{10.2}$$

is called the trace form, *and is nondegenerate.*

Proof. L/K is separable, so $L = K(\alpha)$ for some $\alpha \in L$. Then consider the matrix for $(\cdot,\cdot)$ in the K-basis for L given by $\{1, \alpha, \dots, \alpha^{n-1}\}$. Then

$$\begin{aligned} A_{ij} &= \mathrm{Tr}_{L/K}(\alpha^{i+j}) \\ &= \sum_{i=1}^{n} \sigma_i(\alpha)^{i+j} \\ &= [BB^T]_{ij} \end{aligned} \tag{10.3}$$

where

$$B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \cdots & \sigma_n(\alpha) \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_1(\alpha)^{n-1} & \sigma_2(\alpha)^{n-1} & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix} \tag{10.4}$$

This is a Vandermonde matrix, so its determinant is

$$\mathrm{Det}\, B = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha)). \tag{10.5}$$

Thus

$$\mathrm{Det}\, A = (\mathrm{Det}\, B)^2 = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \neq 0 \tag{10.6}$$

because the extension is separable. Thus $(\cdot,\cdot)$ is nondegenerate. □

On Example Sheet 3 we will prove the converse, so that L/K is separable if and only if the trace form is nondegenerate.

Theorem 10.2. *Let $\mathcal{O}_K$ be a Dedekind domain and L a finite separable extension of $K = \mathrm{Frac}(\mathcal{O}_K)$. Then $\mathcal{O}_L$, the integral closure of $\mathcal{O}_K$ in L, is a Dedekind domain.*

Proof. $\mathcal{O}_L$ is a subring of L so $\mathcal{O}_L$ is an integral domain. We need to show that

(i) $\mathcal{O}_L$ is Noetherian.

(ii) $\mathcal{O}_L$ is integrally closed in L.

(iii) Every nonzero prime ideal $\mathfrak{p}$ in $\mathcal{O}_L$ is maximal.

(i): We want to construct a finitely generated $\mathcal{O}_K$-submodule of L containing $\mathcal{O}_L$, and then since $\mathcal{O}_K$ is Noetherian we are done. Let $e_1, \dots, e_n \in L$ be a K-basis for L. Upon rescaling by K, we may assume that $e_i \in \mathcal{O}_L$. This is because $e_i \in L$, so it satisfies a polynomial in K, which after rescaling can be monic with coefficients in $\mathcal{O}_K$, so that $e_i \in \mathcal{O}_L$ since $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L. Let $f_i \in L$ be the dual basis with respect to the trace form $(\cdot,\cdot)$. Let $x \in \mathcal{O}_L$, and write $x = \sum \lambda_i f_i$ with $\lambda_i \in K$. Then $\lambda_i = \mathrm{Tr}_{L/K}(xe_i)$. If $z \in \mathcal{O}_L$, then $\mathrm{Tr}_{L/K}(z)$ is a sum of elements in $\overline{K}$ which are integral over $\mathcal{O}_K$, and $\mathrm{Tr}_{L/K}(z) \in K$, so $\mathrm{Tr}_{L/K}(z) \in \mathcal{O}_K$, so $\lambda_i \in \mathcal{O}_K$. Then $\mathcal{O}_L \subset \mathcal{O}_K f_1 + \cdots + \mathcal{O}_K f_n \subset L$. Since $\mathcal{O}_K$ is Noetherian, $\mathcal{O}_L$ is finitely generated as a $\mathcal{O}_K$-module, so $\mathcal{O}_L$ is Noetherian.

(ii): Example sheet 2.

(iii): Let $\mathfrak{P}$ be a nonzero prime ideal of $\mathcal{O}_L$, and let $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ be a prime ideal in $\mathcal{O}_K$. Let $0 \neq x \in \mathfrak{P}$. Then x satisfies an equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_0 \neq 0$, $a_i \in \mathcal{O}_K$. Then $a_0 \in \mathfrak{P}$, so $a_0 \in \mathfrak{p}$, so $\mathfrak{p} \neq 0$, so $\mathfrak{p}$ is maximal because $\mathcal{O}_K$ is Dedekind. We have an injection $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$, so $\mathcal{O}_L/\mathfrak{P}$ is a finite dimensional $\mathcal{O}_K/\mathfrak{p}$ vector space. Since $\mathcal{O}_L/\mathfrak{P}$ is an integral domain, it is a field. This is because if $x \in (\mathcal{O}_L/\mathfrak{P})^\times$, then $y \mapsto xy$ is an injection, so it is a bijection, so there exists y such that $xy = 1$ by rank-nullity. □

Remark 10.3. Theorem 10.2 holds without the assumption that L/K is a separable extension.

Corollary 10.4. *The ring of integers of a number field is a Dedekind domain.*

Proof. If $K/\mathbb{Q}$ is a number field, then $\mathcal{O}_K$ is the integral closure of $\mathbb{Z} = \mathcal{O}_\mathbb{Q}$ in K. □

If $\mathcal{O}_K$ is the ring of integers of a number field and $\mathfrak{p} \subset \mathcal{O}_K$ is a nonzero prime, we normalize $|\cdot|_\mathfrak{p}$ by

$$|x|_\mathfrak{p} = (\mathcal{N}\mathfrak{p})^{v_\mathfrak{p}(x)} \tag{10.7}$$

where $\mathcal{N}\mathfrak{p} = \#\mathcal{O}_K/\mathfrak{p}$.

Let $\mathcal{O}_K$ be a Dedekind domain and $K = \mathrm{Frac}(\mathcal{O}_K)$. Let L/K be a finite, separable extension, and $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L. Then $\mathcal{O}_L$ is a Dedekind domain by Theorem 10.2.

Lemma 10.5. *Let $0 \neq x \in \mathcal{O}_K$. Then*

$$(x) = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_\mathfrak{p}(x)} \tag{10.8}$$

Proof. Consider $x(\mathcal{O}_K)_\mathfrak{p} = (\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p})^{v_\mathfrak{p}(x)}$ by the definition of $v_\mathfrak{p}(x)$. The lemma then follows from Lemma 9.11. □

Let $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{p} \subset \mathcal{O}_K$ be nonzero prime ideal. We write $\mathfrak{P} \mid \mathfrak{p}$ if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and $\mathfrak{P} = \mathfrak{P}_i$ for some i.

Theorem 10.6. *Let $\mathcal{O}_K, \mathcal{O}_L, K, L$ be as above. For $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}_K$, we write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Then the absolute values on L extending $|\cdot|_\mathfrak{p}$ (up to equivalence) are precisely $|\cdot|_{\mathfrak{P}_1}, \ldots, |\cdot|_{\mathfrak{P}_r}$.*

Proof. First, for any $0 \neq x \in \mathcal{O}_K$ and any i, we have that $v_{\mathfrak{P}_i}(x) = e_i v_\mathfrak{p}(x)$. Hence, up to equivalence, $|\cdot|_{\mathfrak{P}_i}$ extends $|\cdot|_\mathfrak{p}$. Now, suppose $|\cdot|$ is an absolute value on L extending $|\cdot|_\mathfrak{p}$. Then $|\cdot|$ is bounded on $\mathcal{O}_K$ and hence on $\mathbb{Z}$, so it is non-archimedean. Let

$$R = \{x \in L \mid |x| \leq 1\} \tag{10.9}$$

be the valuation ring for L with respect to $|\cdot|$. Then $\mathcal{O}_K \subset R$ because $|\cdot|$ extends $|\cdot|_\mathfrak{p}$, and since R is integrally closed in L by Lemma 6.9, we have that $\mathcal{O}_L \subset R$. Set

$$\mathfrak{P} = \{x \in \mathcal{O}_L \mid |x| < 1\} = \mathfrak{m}_R \cap \mathcal{O}_L \tag{10.10}$$

where $\mathfrak{m}_R$ is the maximal ideal of R. Then $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_L$, and it is nonzero since $\mathfrak{p} \subset \mathfrak{P}$. Then $(\mathcal{O}_L)_\mathfrak{P} \subset R$ since if $s \in \mathcal{O}_L \setminus \mathfrak{P}$ then $|s| = 1$. But $(\mathcal{O}_L)_\mathfrak{P}$ is a DVR, and hence a maximal subring of L, so $(\mathcal{O}_L)_\mathfrak{P} = R$.

Hence $|\cdot|$ is equivalent to $|\cdot|_\mathfrak{P}$ because the closed unit balls are the same (Proposition 1.6). Since $|\cdot|$ extends $|\cdot|_\mathfrak{p}$, we have that $\mathcal{O}_K \cap \mathfrak{P} = \mathfrak{p}$. But then $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subset \mathfrak{P}$, so $\mathfrak{P} = \mathfrak{P}_i$ for some i. □

Remark 10.7. Let K be a number field. If $\sigma : K \to \mathbb{R}, \mathbb{C}$ is an embedding, then $x \mapsto |x|_\sigma = |\sigma(x)|_\infty$ defines an absolute value on K.

Corollary 10.8. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then any absolute value on K is equivalent to either*

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

(ii) $|\cdot|_\sigma$ *for some embedding* $\sigma : K \to \mathbb{R}, \mathbb{C}$.

Proof. We divide into archimedean and non-archimedean cases.

Case 1: $|\cdot|$ is non-archimedean. We have that $|\cdot|$ restricted to $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some $p \in \mathbb{Q}$ by Ostrowski's Theorem 7.11. Theorem 10.6 then implies that $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ such that $p \mid \mathfrak{p}$.

Case 2: $|\cdot|$ is archimedean. Example Sheet. □

10.1 Completions

Let $\mathcal{O}_K$ be a Dedekind domain and L/K a finite separable extension. Let $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{P} \subset \mathcal{O}_L$ be nonzero prime ideals such that $\mathfrak{P} \mid \mathfrak{p}$. We write $K_{\mathfrak{p}}$ and $L_{\mathfrak{P}}$ for the completions of K and L with respect to $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathfrak{P}}$, respectively.

Lemma 10.9. *(i) The natural map* $\pi_{\mathfrak{P}} : L \otimes_K K_{\mathfrak{p}} \to L_{\mathfrak{P}}$ *given by* $\ell \otimes x \mapsto \ell x$ *is surjective.*

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

Proof. Let $M = LK_{\mathfrak{p}} = \mathrm{Im}(\pi_{\mathfrak{P}}) \subset L_{\mathfrak{P}}$ be the subfield generated by $LK_{\mathfrak{p}}$, and write $L = K(\alpha)$. Then $M = K_{\mathfrak{p}}(\alpha)$, so M is a finite extension of $K_{\mathfrak{p}}$, and $[M : K_{\mathfrak{p}}] \leq [L : K]$ because the minimal polynomial has smaller degree. Moreover, M is complete by Theorem 6.1, and since $L \subset M \subset L_{\mathfrak{P}}$, we have that $M = L_{\mathfrak{P}}$. □

Lemma 10.10 (Chinese Remainder Theorem)**.** *Let R be a ring and $I_1, \ldots, I_r$ be ideals such that $I_i + I_j = R$ for all $i \neq j$. Then*

(i) $\bigcap I_i = \prod I_i = I$.

(ii) $R/I \cong \bigoplus R/I_i$

Proof. Example sheet. □

Theorem 10.11. *The natural map*

$$L \otimes_K K_{\mathfrak{p}} \to \prod_{\mathfrak{P} \mid \mathfrak{p}} L_{\mathfrak{P}} \tag{10.11}$$

is an isomorphism.

Proof. Write $L = K(\alpha)$ and let $f(x) \in K[x]$ be the minimal polynomial of α. Then we have that $f(x) = f_1(x) \cdots f_r(x)$ in $K_{\mathfrak{p}}[x]$, where $f_i(x) \in K_{\mathfrak{P}}[x]$ are distinct because of separability. Since $L \cong K[x]/(f(x))$, we have that

$$\begin{aligned} L \otimes_K K_{\mathfrak{p}} &\cong K_{\mathfrak{p}}(x)/(f(x)) \\ &\cong \prod K_{\mathfrak{p}}(x)/f_i(x) \\ &= \prod L_i \end{aligned} \tag{10.12}$$

Now, L_i contains both $K_{\mathfrak{p}}$ and L, since $K[x]/f(x) \to K_{\mathfrak{p}}[x]/f_i(x)$ is injective. Moreover, L is dense inside L_i, as we can approximate the coefficients of some $f(x) \in K_{\mathfrak{p}}[x]/f_i(x)$ with some $g \in K[x]/f(x)$. The theorem follows from the following three claims:

(i) $L_i \cong L_{\mathfrak{P}}$ for some prime $\mathfrak{P}$ of $\mathcal{O}_L$ dividing $\mathfrak{p}$.

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

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

(i): Since $[L_i : K_{\mathfrak{p}}] < \infty$, there exists a unique valuation on L_i extending $|\cdot|_{\mathfrak{p}}$. Theorem 10.6 implies that $|\cdot|$ restricted to L is $|\cdot|_{\mathfrak{P}}$ for some $\mathfrak{P} \mid \mathfrak{p}$. Since L is dense in L_i and L_i is complete, we have that $L_i \cong L_{\mathfrak{P}}$.

(ii)If $L_i \cong L_{\mathfrak{P}} \cong L_j$, then $f_i = f_j$,

Suppose $\varphi : L_i \to L_j$ is an isomorphism preserving L and $K_{\mathfrak{p}}$. Then

$$\varphi : K_{\mathfrak{p}}[x]/f_i(x) \to K_{\mathfrak{p}}[x]/f_j(x) \tag{10.13}$$

takes x to x, so $f_i = f_j$.

(iii) By Lemma 10.9, $\pi_{\mathfrak{P}} : L \otimes_K K_{\mathfrak{p}} \to L_{\mathfrak{P}}$ is surjective, and since $L_{\mathfrak{P}}$ is a field, $\pi_{\mathfrak{P}}$ must factor through L_i for some i. But then ψ injective because it is a field map, so $L_i \cong L_{\mathfrak{P}}$. Furthermore $\pi_{\mathfrak{P}}$ sends $L \to L$ and $K_{\mathfrak{p}} \to K_{\mathfrak{p}}$, so ψ is also an L-algebra and $K_{\mathfrak{p}}$-algebra homomorphism. □

Example 10.12. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, and $f(x) = x^2 + 1$. Then

$$\mathbb{Q}(i) \otimes \mathbb{Q}_5 \cong \prod_{\mathfrak{P}|5} \mathbb{Q}(i)_{\mathfrak{P}} \tag{10.14}$$

Hensel's lemma shows that $f(x)$ has a root in $\mathbb{Q}_5$, so that (5) splits in $\mathbb{Q}(i)$.

Corollary 10.13. *Let $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. If $x \in L$, then*

$$N_{L/K}(x) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x). \tag{10.15}$$

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and $B_1, \ldots, B_r$ be bases for $L_{\mathfrak{P}_1}, \ldots, L_{\mathfrak{P}_r}$ as $K_{\mathfrak{p}}$ vector spaces. Then $B = \bigcup B_i$ is a basis for $L \otimes K_{\mathfrak{p}} \cong \prod L_{\mathfrak{P}_i}$ over $K_{\mathfrak{p}}$. Let $[\mathrm{mult}(x)]_B$ be the matrix for the map

$$\begin{aligned} \mathrm{mult}(x) : L \otimes_K K_{\mathfrak{p}} &\to L \otimes K_{\mathfrak{p}} \\ \ell \otimes k &\mapsto x(\ell \otimes k) \end{aligned} \tag{10.16}$$

with respect to the basis B and let $[\mathrm{mult}(x)]_{B_i}$ be the matrix for the analogous map $L_{\mathfrak{P}_i} \to L_{\mathfrak{P}_i}$ with respect to the basis B_i. Because of the decomposition $L \otimes K_{\mathfrak{p}} \cong \prod L_{\mathfrak{P}_i}$, we have that $[\mathrm{mult}(x)]_B$ is the block diagonal matrix of $[\mathrm{mult}(x)]_{B_i}$s. We then have that

$$N_{L/K}(x) = \mathrm{Det}[\mathrm{mult}(x)]_B = \prod \mathrm{Det}[\mathrm{mult}(x)]_{B_i} = \prod N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}} \tag{10.17}$$

□

11 Decomposition groups

If we want to study the Galois group of a global field, part of it looks like the Galois group of a local field.

Let $0 \neq \mathfrak{p}$ be a prime in $\mathcal{O}_K$ and let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where the $\mathfrak{P}_i$ are distinct primes in $\mathcal{O}_L$ and $e_i > 0$.

Definition 11.1. (i) e_i is the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$.

(ii) We say that $\mathfrak{p}$ *ramifies* in L if some $e_i > 1$.

Example 11.2. Let $\mathcal{O}_K = \mathbb{C}[t]$, and $\mathcal{O}_L = \mathbb{C}[T]$, and let $\mathcal{O}_K \to \mathcal{O}_L$ be the map sending $t \mapsto T^n$. Then (t) is a prime in $\mathcal{O}_K$, and $t\mathcal{O}_L = (T^n) = (T)^n$. The ramification of (T) over (t) is n.

This corresponds geometrically to a degree n covering of Riemann surfaces $\mathbb{C} \to \mathbb{C}$ sending $x \mapsto x^n$.

Definition 11.3. $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is the residue class degree of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Theorem 11.4. *We have that*

$$\sum_{i=1}^{r} e_i f_i = [L : K]. \tag{11.1}$$

Proof. Let $S = \mathcal{O}_K \setminus \mathfrak{p}$. The following three basic facts about localization are an exercise:

(i) $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K$ in L.

(ii) $(S^{-1}\mathfrak{p})S^{-1}\mathcal{O}_L \cong S^{-1}(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r})$.

(iii) $S^{-1}\mathcal{O}_L/S^{-1}\mathfrak{P}_i \cong \mathcal{O}_L/\mathfrak{P}_i$ and $S^{-1}\mathcal{O}_K/S^{-1}\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$.

In particular (ii) and (iii) imply that e_i and f_i don't change when we replace $\mathcal{O}_K$ and $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$. Thus we may assume that $\mathcal{O}_K$ is a DVR and hence a PID. By the Chinese remainder theorem, we have that

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod \mathcal{O}_L/\mathfrak{P}_i^{e_i}. \tag{11.2}$$

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

RHS: For each i, there exists a decreasing sequence of k-subspaces

$$0 \subset \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \subset \mathfrak{P}_i^{e_i-2}/\mathfrak{P}_i^{e_i} \subset \cdots \subset \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \subset \mathcal{O}_L/\mathfrak{P}_i^{e_i}. \tag{11.3}$$

We have that $\dim_k \mathcal{O}_L/\mathfrak{P}_i^{e_i} = \sum \dim_k(\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1})$. Note that $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is an $\mathcal{O}_L/\mathfrak{P}_i$-module and $x \in \mathfrak{P}_i^j \setminus \mathfrak{P}_i^{j+1}$ is a generator, which we can prove by localizing at $\mathfrak{P}_i$. So the quotients are 1-dimensional over $\mathcal{O}_L/\mathfrak{P}_i$, so they are f_i-dimensional over k. Then $\dim_k \mathcal{O}_L/\mathfrak{P}_i^{e_i} = e_i f_i$ so the RHS has dimension $\sum e_i f_i$.

LHS: The structure theorem for finitely generated modules ($\mathcal{O}_L$ is a finitely generated module over $\mathcal{O}_K$) and the fact that $\mathcal{O}_L$ is torsion free implies that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $n = [L : K]$. Thus $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_K/\mathfrak{p})^n$ as k-vector spaces, so the LHS has dimension n. □

Remark 11.5. The previous theorem has a geometric analogue: let $f : X \to Y$ be a degree n cover of Riemann surfaces. For $y \in Y$, we have that

$$n = \sum_{x \in f^{-1}(y)} e_x. \tag{11.4}$$

Now assume that the L/K is Galois. The Galois group preserves integral elements, so it acts on $\mathcal{O}_L$. Then for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathfrak{P}_i) \cap \mathcal{O}_K = \mathfrak{p}$ and hence $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ for some j.

Proposition 11.6. *The action of* $\mathrm{Gal}(L/K)$ *on* $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$ *is transitive.*

Proof. Suppose not, so that there exists $i \neq j$ such that $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_j$ for all $\sigma \in \mathrm{Gal}(L/K)$. By the CRT, we may choose $x \in \mathcal{O}_L$ such that $x \equiv 0 \mod \mathfrak{P}_i$ and $x \equiv 1 \mod \sigma(\mathfrak{P}_j)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Then $N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathcal{O}_K \cap \mathfrak{P}_i = \mathfrak{p} \subset \mathfrak{P}_j$. But $\mathfrak{P}_j$ is prime, so there exists $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(x) \in \mathfrak{P}_j$, so $x \in \tau^{-1}(\mathfrak{P}_j)$, so $x \equiv 0 \mod \tau^{-1}(\mathfrak{P}_j)$, which is a contradiction as $x \equiv 1 \mod \tau^{-1}(\mathfrak{P}_j)$ by assumption. □

Corollary 11.7. *Suppose L/K is Galois. Then $e_1 = \cdots = e_r = e$ and $f_1 = \cdots = f_r = f$, and then $n = efr$.*

Proof. For any $\sigma \in \mathrm{Gal}(L/K)$, we have that $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p})\mathcal{O}_L = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r}$, and by the unique factorization we have that $e_1 = \cdots = e_r = e$.

We have that $\mathcal{O}_L/\mathfrak{P}_i \cong \mathcal{O}_L/\sigma(\mathfrak{P}_i)$ via $x \mapsto \sigma(x)$, so $f_1 = \cdots = f_r = f$. □

In the case where L/K is a extension of DV fields, we have the following.

Corollary 11.8. *Let L/K be an extension of complete DV fields with valuations v_L, v_K, uniformizers π_L, π_K. Then there are unique prime ideals in both, so we can define $e = e_{L/K} = v_L(\pi_K)$ since $\pi_K = \pi_L^e$ for some e. The residue degree is $f = f_{L/K} = [k_L : k]$. Then if L/K is finite, separable, then $[L : K] = ef$.*

Definition 11.9. Let $\mathcal{O}_K$ be a Dedekind domain, L/K finite, Galois. The *decomposition group* at a prime $\mathfrak{P}$ of $\mathcal{O}_L$ is the subgroup of $\mathrm{Gal}(L/K)$ given by

$$G_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}. \tag{11.5}$$

It has size ef, which makes sense if you write down $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$

Proposition 11.10. *Suppose that $\mathfrak{P} \mid \mathfrak{p} \subset \mathcal{O}_K$. Then*

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

(ii) *There is a natural map*

$$\mathrm{res} : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K) \tag{11.6}$$

which is injective and has image $G_{\mathfrak{P}}$.

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

(ii): Let $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. Then $\sigma(L) = L$ since L is L/K is normal (and σ is an embedding of L in $\overline{K}$). Thus we have a map

$$\begin{aligned} \mathrm{res} : \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) &\to \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned} \tag{11.7}$$

Since L is dense in $L_\mathfrak{P}$, res is injective (as is $\mathrm{res}(\sigma) = \mathrm{id}_L$, then σ is constant on a dense subset of $L_\mathfrak{P}$, and hence constant). By Lemma 8.2, we have that $|\sigma(x)|_\mathfrak{P} = |x|_\mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ and all $x \in L_\mathfrak{P}$. But then $\sigma(\mathfrak{P}) = \mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$, so $\mathrm{res}(\sigma) \in G_\mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. To show surjectivity onto $G_\mathfrak{P}$, we compare cardinalities. So that

$$|G_\mathfrak{P}| = |\,\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})| = ef = [L_\mathfrak{P} : K_\mathfrak{p}]. \tag{11.8}$$

Write $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$, and $f = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$. Then $|G_\mathfrak{P}| = ef$. For $[L_\mathfrak{P} : K_\mathfrak{p}]$, apply Corollary 11.8 and note that e and f don't change when we take completions (see the proof of Theorem 11.6). □

Thus a piece of the Galois group of a number field extension L/K corresponds to an extension of local fields $L_\mathfrak{P}/K_\mathfrak{p}$.

Part V

Ramification Theory

Ramification theory studies how prime ideals split in extensions. For example, if $p \in \mathbb{Z}$ is prime, then $p = p_1p_2 \in \mathbb{Z}[i]$ splits if and only if $p = x^2 + y^2$, if and only if $p \equiv 1 \mod 4$.

Let L/K be an extension of algebraic number fields of degree $[L : K] = n$.

12 Different and discriminant

Let $x_1, \ldots, x_n \in L$. Then the discriminant of these elements is

$$\Delta(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{L/K}(x_ix_j)) \in K. \tag{12.1}$$

If $x_1, \ldots, x_n$ form a basis, this is the determinant of the trace form. Now, let $\sigma_\ell : L \to \overline{K}$ for $\ell = 1, \ldots, n$ be the n embeddings of L into $\overline{K}$. Then

$$\Delta(x_1, \ldots, x_n) = \det\left(\sum_{\ell=1}^{n} \sigma_\ell(x_i)\sigma_\ell(x_j)\right) = \det(BB^T) \tag{12.2}$$

where $B = (\sigma_i(x_j))_{ij}$.

Remark 12.1. (i) If $y_j = \sum a_{ij}x_j$ for a_{ij}, then

$$\Delta(y_1, \ldots, y_n) = \det(A)^2\Delta(x_1, \ldots, x_n) \tag{12.3}$$

where $A = (a_{ij})$.

(ii) If $x_1, \ldots, x_n \in \mathcal{O}_L$, $\Delta(x_1, \ldots, x_n) \in \mathcal{O}_K$ because it is a product and sum of elements of $\mathcal{O}_K$ (recall the trace of an element of $\mathcal{O}_L$ is in $\mathcal{O}_K$).

Lemma 12.2. *Let k be a perfect field and let R be a k-algebra which is a finite-dimensional as a k-vector space. The trace form*

$$\begin{aligned}(\cdot,\cdot) : R \times R &\to k \\ (x, y) &\mapsto \mathrm{Tr}_{R/k}(xy) = \mathrm{Tr}_k(\mathrm{mult}(xy)) \end{aligned} \tag{12.4}$$

is nondegenerate if and only if $R \cong k_1 \times \cdots \times k_r$, where k_i/k is a finite separable extension of k.

Proof. Example Sheet? □

Theorem 12.3. *Let $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ be a prime.*

(i) If $\mathfrak{p}$ ramifies in L, then for every $x_1, \ldots, x_n \in \mathcal{O}_L$, we have that $\Delta(x_1, \ldots, x_n) \equiv 0 \mod \mathfrak{p}$.

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

Proof. (i) Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and assume that $\mathfrak{p}$ ramifies so that $e_i > 1$ for some i. Set

$$R = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{P}_i^{e_i}. \tag{12.5}$$

If $\mathfrak{p}$ ramifies, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ has nilpotents, so $\mathcal{O}_L/\mathfrak{P}_i^{e_i}$ is not a finite separable extension of $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. If $\overline{x}_1, \ldots \overline{x}_n$ forms a basis for $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, then by Lemma 12.2 we have that $\Delta(\overline{x}_1, \ldots, \overline{x}_n) = 0$. If $\overline{x}_1, \ldots \overline{x}_n$ does not form a basis, then $\Delta(\overline{x}_1, \ldots \overline{x}_n) = (\det A)^2 \Delta(\overline{y}_1, \ldots, \overline{y}_n) = 0$ where $\overline{y}_1, \ldots, \overline{y}_n$ is a basis and $\overline{x}_j = \sum a_{ij}\overline{y}_i$. Now, we have a commutative diagram

$$\begin{tikzcd}
\mathcal{O}_L \arrow[r] \arrow[d, "\mathrm{Tr}_{L/K}"] & \mathcal{O}_L/\mathfrak{P}\mathcal{O}_L = R \arrow[d, "\mathrm{Tr}_{R/k}"] \\
\mathcal{O}_K \arrow[r] & \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K
\end{tikzcd}$$

Thus if we lift any $\overline{x}_1, \ldots, \overline{x}_n \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ to any $x_1, \ldots, x_n \in \mathcal{O}_L$, we find that $\Delta(x_1, \ldots, x_n) \equiv 0 \mod \mathfrak{p}$.

(ii): If $\mathfrak{p}$ is unramified, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ will be a product of finite extensions of $k = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. Then the trace form will be nondegenerate by Lemma 12.2, so we can find a basis $\overline{x}_1, \ldots, \overline{x}_n$ for $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ such that $\Delta(\overline{x}_1, \ldots, \overline{x}_n) \neq 0$. Then lifting gives $\Delta(x_1, \ldots, x_n) \not\equiv 0 \mod \mathfrak{p}$. □

The discriminant is an ideal which captures all the Δs, and hence all the ramification.

Definition 12.4. The *discriminant ideal* $d_{L/K} \subset \mathcal{O}_K$ is the ideal generated by $\Delta(x_1, \ldots, x_n)$ for all choice of $x_1, \ldots, x_n \in \mathcal{O}_L$.

Corollary 12.5. *$\mathfrak{p}$ ramifies in L if and only if $\mathfrak{p} \mid d_{L/K}$. In particular, only finitely many primes ramify in L.*

Proof. This follows immediately from Theorem 12.3 and the unique factorization of ideals in $\mathcal{O}_K$. □

Next we will define the different. It is the inverse of an inverse.

Definition 12.6. The *inverse different* is

$$D_{L/K}^{-1} \coloneqq \{y \in L \mid \operatorname{Tr}_{L/K}(xy) \in \mathcal{O}_K \forall x \in \mathcal{O}_L\}. \tag{12.6}$$

It is the dual lattice of $\mathcal{O}_L$ with respect to the trace form.

Lemma 12.7. *$D_{L/K}^{-1}$ is a fractional ideal in L.*

Proof. Let $x_1, \ldots, x_n \in \mathcal{O}_L$ be a K-basis for L/K and set

$$d = \Delta(x_1, \ldots, x_n) = \det(\operatorname{Tr}_{L/K}(x_i x_j)) \neq 0 \tag{12.7}$$

as the the trace form is nondegenerate because the extension is separable (Lemma 10.1).

For $x \in D_{L/K}$, we can write $x = \sum \lambda_j x_j$ with $\lambda_j \in K$. We want to show that $\lambda_j \in d^{-1}\mathcal{O}_K$. We have that $\operatorname{Tr}_{L/K}(xx_i) = \sum \lambda_j \operatorname{Tr}_{L/K}(x_i x_j) \in \mathcal{O}_K$. Set $A_{ij} = \operatorname{Tr}_{L/K}(x_i x_j)$. Multiplying by the adjugate matrix $\operatorname{Adj}(A)$, we get the determinant, so

$$\operatorname{Adj}(A)A \begin{pmatrix} \lambda_1 \\ \cdots \\ \lambda_m \end{pmatrix} = \det(A) \begin{pmatrix} \lambda_1 \\ \cdots \\ \lambda_m \end{pmatrix} = d \begin{pmatrix} \lambda_1 \\ \cdots \\ \lambda_m \end{pmatrix} = \operatorname{Adj}(A) \begin{pmatrix} \operatorname{Tr}_{L/K}(xx_1) \\ \cdots \\ \operatorname{Tr}_{L/K}(xx_n) \end{pmatrix} \tag{12.8}$$

$\operatorname{Adj}(A)$ and $\operatorname{Tr}_{L/K}(xx_i)$ are in $\mathcal{O}_K$, so $\lambda_i \in \frac{1}{d}\mathcal{O}_K$, so $x \in \frac{1}{d}\mathcal{O}_L$. Thus $D_{L/K}^{-1} \subset \frac{1}{d}\mathcal{O}_L$, so $D_{L/K}^{-1}$ is a fractional ideal. □

Definition 12.8. The *different ideal* $D_{L/K}$ is the inverse of $D_{L/K}^{-1}$.

We have that $D_{L/K} \subset \mathcal{O}_L$ because $\mathcal{O}_L \subset D_{L/K}^{-1}$ and $D_{L/K}^{-1}$ is a fractional ideal.

Let I_L, I_K be the group of fractional ideals of L, K. By Proposition 9.10, we have that

$$I_L \cong \bigoplus_{0 \neq \mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L} \mathbb{Z}, \qquad I_K \cong \bigoplus_{0 \neq \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K} \mathbb{Z} \tag{12.9}$$

Define $N_{L/K} : I_L \to I_K$ induced by $\mathfrak{P} \mapsto \mathfrak{p}^f$ where $\mathfrak{p} = \mathbb{P} \cap \mathcal{O}_K$ and $f = f(\mathfrak{P}/\mathfrak{p})$. Then the following diagram commutes:

$$\begin{tikzcd}
L^\times \arrow[r] \arrow[d, "N_{L/K}"] & I_L \arrow[d, "N_{L/K}"] \\
K^\times \arrow[r] & I_K
\end{tikzcd}$$

In other words, we have that $N_{L/K}((x)) = (N_{L/K}(x))$. This follows from Corollary 10.13 and the fact that

$$v_{\mathfrak{p}}(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x)) = f_{\mathfrak{P}/\mathfrak{p}} v_{\mathfrak{P}}(x) \tag{12.10}$$

for $x \in L_{\mathfrak{P}}^\times$. In particular, we have that

$$v_{\mathfrak{p}}(N_{L/K}((x))) = \sum_{\mathfrak{P} \mid \mathfrak{p}} f(\mathfrak{P}/\mathfrak{p}) v_{\mathfrak{P}}(x) \tag{12.11}$$

by definition, and

$$\begin{aligned} v_{\mathfrak{p}}((N_{L/K}(x))) &= v_{\mathfrak{p}}\left(\prod_{\mathfrak{P}|\mathfrak{p}}(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x))\right) \\ &= \sum_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{p}}(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x)) \\ &= \sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}} v_{\mathfrak{P}}(x) \end{aligned} \tag{12.12}$$

as desired.

Theorem 12.9. $N_{L/K}(D_{L/K}) = d_{L/K}$.

Proof. First, assume that $\mathcal{O}_K$ and $\mathcal{O}_L$ are PIDs. Let $x_1, \dots, x_n$ be an $\mathcal{O}_K$-basis for $\mathcal{O}_L$. Then $d_{L/K} = (\Delta(x_1, \dots, x_n))$ because any change of basis matrix is a unit in $\mathcal{O}_K$. Let $y_1, \dots, y_n$ be the dual basis with respect to the trace form. Then $y_1, \dots, y_n$ is an $\mathcal{O}_K$-basis for $D_{L/K}^{-1}$ (essentially by the definition of $D_{L/K}^{-1}$). Let $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ be the distinct embeddings of L into $\overline{K}$. Then

$$\sum_{i=1}^{n} \sigma_i(x_j)\sigma_i(y_k) = \mathrm{Tr}(x_j y_k) = \delta_{jk}. \tag{12.13}$$

But $\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$. Thus $\Delta(x_1, \dots, x_n)\Delta(y_1, \dots, y_n) = 1$. Write $D_{L/K}^{-1} = \beta\mathcal{O}_L$ for some $\beta \in \mathcal{O}_L$. Then

$$\begin{aligned} d_{L/K}^{-1} &= (\Delta(x_1, \dots, x_n)^{-1}) \\ &= (\Delta(y_1, \dots, y_n)). \end{aligned} \tag{12.14}$$

Now, since change of basis matrices are invertible in $\mathcal{O}_K$, we have that

$$(\Delta(y_1, \dots, y_n)) = (\Delta(\beta x_1, \dots, \beta x_n)) \tag{12.15}$$

since $\beta x_1, \dots, \beta x_n$ is a basis for $\beta\mathcal{O}_L = D_{L/K}^{-1}$. Now, the change of basis matrix from $x_i \mapsto \beta x_i$ is multiplication by β, which has determinant $N_{L/K}(\beta)$. By (12.3) we then have that

$$(\Delta(\beta x_1, \dots, \beta x_n)) = N_{L/K}(\beta^2)\Delta(x_1, \dots, x_n). \tag{12.16}$$

Putting it all together gives

$$d_{L/K}^{-1} = N_{L/K}(D_{L/K}^{-1})^2 d_{L/K} \tag{12.17}$$

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

To prove the general case, localize at $S = \mathcal{O}_K \setminus \mathfrak{p}$ and use that $S^{-1}D_{L/K} = D_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$ and $S^{-1}d_{L/K} = d_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$. □

Theorem 12.10. *If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and α has monic minimal polynomial $g(x) \in \mathcal{O}_K[x]$, then $D_{L/K} = (g'(\alpha))$.*

Proof. Let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be roots of g. Write $g(x)/(x-\alpha) = \beta_{n-1}x^{n-1} + \cdots + \beta_1 x + \beta_0$, where $\beta_i \in \mathcal{O}_L$ and $\beta_{n-1} = 1$. We claim that

$$\sum_{i=1}^{n} \frac{g(x)}{x-\alpha_i} \cdot \frac{\alpha_i^r}{g'(\alpha_i)} = x^r \tag{12.18}$$

for $0 \leq r \leq n-1$. Indeed, the difference is a polynomial of degree less than n which vanishes at $\alpha_1, \dots, \alpha_n$, so the difference is zero. Comparing coefficients on both sides gives that the x^s coefficient is

$$\mathrm{Tr}_{L/K}\left(\frac{\alpha^r \beta_s}{g'(\alpha)}\right) = \delta_{rs} \tag{12.19}$$

by (10.1). So $1, \alpha, \dots, \alpha^{n-1}$ is a basis for $\mathcal{O}_L$, and we have explicitly constructed the dual basis under the trace form, which will be a basis for $D_{L/K}^{-1}$:

$$\frac{\beta_0}{g'(\alpha)}, \frac{\beta_1}{g'(\alpha)}, \dots, \frac{\beta_{n-1}}{g'(\alpha)} = \frac{1}{g'(\alpha)} \tag{12.20}$$

Since $\beta_i \in \mathcal{O}_L$, $D_{L/K}^{-1}$ is generated as an $\mathcal{O}_L$-module by $1/g'(\alpha)$, so $D_{L/K}$ is generated by $g'(\alpha)$ as an $\mathcal{O}_L$-ideal. □

Now, let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ and $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$. Then we can define $D_{L_\mathfrak{P}/K_\mathfrak{p}}$ analogously to $D_{L/K}$ using $\mathcal{O}_{K_\mathfrak{p}}, \mathcal{O}_{L_\mathfrak{P}}$. $D_{L_\mathfrak{P}/K_\mathfrak{p}}$ is an ideal of the DVR $\mathcal{O}_{L_\mathfrak{P}}$, so it is a power of $\mathfrak{P}$. We identify $D_{L_\mathfrak{P}/K_\mathfrak{p}}$ with a power of $\mathfrak{P}$ in $\mathcal{O}_L$.

Theorem 12.11. *We have that*

$$D_{L/K} = \prod_{0 \neq \mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L} D_{L_\mathfrak{P}/K_\mathfrak{p}}. \tag{12.21}$$

In particular, the right hand side is finite.

Proof. Let $x \in L$ and $\mathfrak{p} \subset \mathcal{O}_K$. Then similarly to Corollary 10.13, we have that

$$\mathrm{Tr}_{L/K}(x) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(x). \tag{12.22}$$

Let $r(\mathfrak{P}) = v_\mathfrak{P}(D_{L/K})$, and $s(\mathfrak{P}) = v_\mathfrak{P}(D_{L_\mathfrak{P}/K_\mathfrak{p}})$. Fix some $x \in L$ with $v_\mathfrak{P}(x) \geq -s(\mathfrak{P})$ for all $\mathfrak{P}$. Then $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_L$ and all primes $\mathfrak{P}$. So $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_L$ and all $\mathfrak{p}$ by (12.22). Thus $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K$ for all $y \in \mathcal{O}_L$. So $x \in D_{L/K}^{-1}$, so $r(\mathfrak{P}) \geq s(\mathfrak{P})$ and $D_{L/K} \subset \prod_\mathfrak{P} D_{L_\mathfrak{P}/K_\mathfrak{p}}$. Fix $\mathfrak{P}$ and let $x \in \mathfrak{P}^{-r(\mathfrak{P})} \backslash \mathfrak{P}^{-r(\mathfrak{P})+1}$. Then $v_\mathfrak{P}(x) = -r(\mathfrak{P})$, and $v_{\mathfrak{P}'}(x) \geq 0$ for all $\mathfrak{P}' \neq \mathfrak{P}$. By (12.22), we have that

$$\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) = \mathrm{Tr}_{L/K}(xy) - \sum_{\mathfrak{P} \neq \mathfrak{P}'|\mathfrak{p}} \mathrm{Tr}_{L_{\mathfrak{P}'}/K_\mathfrak{p}}(xy) \tag{12.23}$$

for all $y \in \mathcal{O}_L$. All the terms on the RHS are in $\mathcal{O}_{K_\mathfrak{p}}$, so we have that $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ for all $y \in \mathcal{O}_{L_\mathfrak{P}}$. Thus $x \in D_{L_\mathfrak{P}/K_\mathfrak{p}}^{-1}$, so $-v_\mathfrak{P}(x) = r(\mathfrak{P}) \leq s(\mathfrak{P})$. This gives the desired result. □

Corollary 12.12.

$$d_{L/K} = \prod_{\mathfrak{P}|\mathfrak{p}} d_{L_\mathfrak{P}/K_\mathfrak{p}}. \tag{12.24}$$

Proof. Take the norm of both sides of (12.21) and use Corollary 10.13. □

13 Unramified and totally ramified extensions of local fields

Let L/K be a finite separable extension of non-archimedean local fields. By Corollary 11.8, we have that $[L : K] = e_{L/K}f_{L/K}$.

Lemma 13.1. *Let $M/L/K$ be finite separable extensions of non-archimedean local fields. Then*

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

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

Proof. (i): We have that $f_{M/K} = [k_M : k] = [k_M : k_L][k_L : k] = f_{M/L}f_{L/K}$.

(ii): This follows from (i) and the fact that $[L : K] = e_{L/K}f_{L/K}$. □

Definition 13.2. The extension L/K is *unramified* if $e_{L/K} = 1$, or equivalently $f_{L/K} = [L : K]$. Otherwise it is *ramified*, so $e_{L/K} > 1$, or $f_{L/K} < [L : K]$. If $e_{L/K} = [L : K]$, so that $f_{L/K} = 1$, the extension is *totally ramified*.

Theorem 13.3. *Let L/K be a finite separable extension of local fields. There exists a field K_0 such that $L/K_0/K$ is a sub extension and*

(i) K_0/K is unramified.

(ii) L/K_0 is totally ramified.

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

Proof. Let $k = \mathcal{O}_K/\mathfrak{m} = \mathbb{F}_q$, so that $k_L = \mathbb{F}_{q^f}$ with $f = f_{L/K}$. Set $m = q^f - 1 = |k_L^\times|$, and let $[\cdot] : \mathbb{F}_{q^f} \to L$ be the Teichmüller map for L. Let $\zeta_m = [\alpha]$ be the Teichmüller lift for α, where α is a generator for $\mathbb{F}_{q^f}^\times$. Then ζ_m is a primitive mth root of unity as $[\alpha]^m = [\alpha^m] = 1$ and $[\alpha^i] \neq 1$ for $i < m$ as α generates $\mathbb{F}_{q^f}^\times$. Set $K_0 = K(\zeta_m) \subset L$. Then K_0/K is Galois and K_0 has residue field $k_0 = \mathbb{F}_q(\alpha) = k_L$. Thus $f_{L/K_0} = 1$ so L/K_0 is totally ramified. Let $\mathrm{res} : \mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_0/k)$ be the restriction map. For $\sigma \in \mathrm{Gal}(K_0/K)$, we have that σ is trivial if and only if $\sigma(\zeta_m) = \zeta_m$ if and only if $\sigma(\zeta_m) \equiv \zeta_m \mod \mathfrak{m}_0$ since $\mu_m(K_0) \cong \mu_m(k_0)$ by Hensel's lemma applied to $x^m - 1$. Hence res is injective. Thus $|\mathrm{Gal}(K_0/K)| \leq |\mathrm{Gal}(k_0/k)| = f_{K_0/K}$, so $[K_0 : K] = f_{K_0/K}$ because $f_{K_0/K} \leq |\mathrm{Gal}(K_0/K)|$ always. Thus $e_{K_0/K} = 1$, so K_0/K is unramified. □

Recall that the Tecihmuüller lift is an element of $\mathcal{O}_K$ without "pth power imperfection". Thus K_0/K is an extension without pth power imperfection, and all the pth power stuff goes into the totally ramified extension L/K_0. We will make this precise later.

Theorem 13.4. *Let K be a local field, and set $k = \mathbb{F}_q$. 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,* $\mathrm{Gal}(L/K) \cong \langle \mathrm{Frob}_{L/K} \rangle$ *is cyclic, where* $\mathrm{Frob}_{L/K}(x) = x^q \mod \mathfrak{m}_L$ *for all $x \in \mathcal{O}_L$.*

Proof. For $n \geq 1$, take $L = K(\zeta_m)$ where $m = q^n - 1$. As in Theorem 13.3, we have that $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Thus $\mathrm{Gal}(L/K)$ is cyclic and generated by a lift of $\mathrm{Frob}_q : x \mapsto x^q$, which is a generator for $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

To show uniqueness, let L/K be a degree n unramified extension. By the Teichmüller lifting, $\zeta_m \in L$, so $L = K(\zeta_m)$ by degree properties. □

Corollary 13.5. *Let L/K be a finite Galois extension of local fields. Then* $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ *is surjective.*

Proof. res factors as $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K_0/K) \cong \mathrm{Gal}(k_0/k) \cong \mathrm{Gal}(k_L/k)$ because $k_L = k_0$. □

Definition 13.6. The *inertia subgroup* is defined to be

$$I_{L/K} = \ker(\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)). \tag{13.1}$$

L/K breaks up into unramified and totally ramified parts, the inertia subgroup captures the ramified part ($\mathrm{Gal}(k_L/k) \cong \mathrm{Gal}(K_0/K)$ captures the unramified part).

Remark 13.7.

1. Since $e_{L/K} f_{L/K} = [L : K]$ and $f_{L/K} = |\mathrm{Gal}(k_L/k)|$, we have that $|I_{L/K}| = e_{L/K}$.
2. We have that $I_{L/K} = \mathrm{Gal}(L/K_0)$ as in Theorem 13.3.

Definition 13.8. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$. Then $f(x)$ is *Eisenstein* if $v_K(a_i) \geq 1$ for all i, and $v_K(a_0) = 1$.

It is a fact that if $f(x)$ is Eisenstein, then it is irreducible.

Theorem 13.9.

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

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

Proof. (i): Suppose L/K is totally ramified, so that $[L : K] = e_{L/K} = e$. Let π_L be a uniformizer, and let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathcal{O}_K[x]$ be the minimal polynomial for π_L. Then $m \leq e$. Since $v_L(K^\times) = e\mathbb{Z}$ and $a_i \in K$, we have that $v_L(a_i\pi^i) = i \mod e$ for $i < m$. Since $i < m < e$, the valuations $v_L(a_i\pi^i)$ are all distinct. As $\pi_L^m = -\sum a_i\pi_L^i$, we have that $m = v_L(\pi^m) = \min v_L(a_i\pi_L^i) = \min(i + ev_K(a_i))$. Since $i < m$, we need $v_K(a_i) \geq 1$ for all i. Also, we need $\min(i + ev_K(a_i)) = m \leq e$, and this can only happen if $m = e$ and $v_K(a_0) = 1$. Thus $f(x)$ is Eisenstein of degree e, so $L = K(\pi_L)$.

If $y \in L$, we can write $y = \sum \pi_L^i b_i$ with $b_i \in K$. We have that $y \in \mathcal{O}_L$ if and only $v_L(y) > 0$, and $v_L(y) = \min(v_L(\pi_L^i b_i)) = \min(i + ev_K(b_i))$. So we need $b_i \in \mathcal{O}_K$, so $y \in \mathcal{O}_K[\pi_L]$.

(ii) Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be Eisenstein. Then $v_L(a_i) = ev_K(a_i) \geq e$ and $v_L(a_0) = e$. Let α be a root of f and set $L = K(\alpha)$. If $v_L(\alpha) \leq 0$, then we would have $v_L(\alpha^n) < v_L(-\sum a_i\alpha^i)$, which is a contradiction. Thus $v_L(\alpha) > 0$. For $i > 0$, we have that $v_L(a_i\alpha^i) > e = v_L(a_0)$. Therefore $v_L(\alpha^n) = v_L(-\sum a_i\alpha^i) = v_L(a_0) = e$. Thus $nv_L(\alpha) = e$. But $e \mid n$, so $n = e$ and $v_L(\alpha) = 1$. □

13.1 Structure of units

Let $[K : \mathbb{Q}_p] < \infty$ be a finite extension of $\mathbb{Q}_p$ and set $e \coloneqq e_{K/\mathbb{Q}_p}$ and let π be a uniformizer of K.

Proposition 13.10. *If $r > \frac{e}{p-1}$ then* $\exp(x) = \sum \frac{x^n}{n!}$ *converges on $\pi^r\mathcal{O}_K$ and induces an isomorphism of groups*

$$(\pi^r\mathcal{O}_K, +) \cong (1 + \pi^r\mathcal{O}_K, \times). \tag{13.2}$$

Proof. To show convergence, we have that

$$\begin{aligned} v_K(n!) &= ev_p(n!) \\ &= e \cdot \frac{n - s_p(n)}{p-1} \\ &\leq e \cdot \frac{n-1}{p-1} \end{aligned} \tag{13.3}$$

where $s_p(n)$ is the base p digit sum of n. For $x \in \pi^r \mathcal{O}_K$ and $n \geq 1$, we have that

$$v_K\left(\frac{x^n}{n!}\right) \geq nr - e \cdot \frac{n-1}{p-1} = r + (n-1)(r - \frac{e}{p-1}). \tag{13.4}$$

This is greater than 0 if $r > \frac{e}{p-1}$, and in this case $v_K(\frac{x^n}{n!} \to 0$ so $\exp(x)$ converges.

Since $v_K(x^n/n!) \geq r$ for all $n \geq 1$, we have that $\exp(x) \in 1 + \pi^r \mathcal{O}_K$. Consider the log map

$$\begin{aligned} \log(1 + \cdot) : 1 + \pi^r \mathcal{O}_K &\to \pi^r \mathcal{O}_K \\ x &\mapsto \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n. \end{aligned} \tag{13.5}$$

This converges as before as $v_K(n) \leq v_K(n!)$. In $\mathbb{Q}[X, Y]$, we have the identities

(i) $\exp(X + Y) = \exp(X)\exp(Y)$.

(ii) $\exp(\log(1 + x)) = 1 + x$.

(iii) $\log(\exp(x)) = x$.

Thus log is the inverse of exp, so exp is an isomorphism. □

Now let K be any local field with uniformizer π, and set $U_K \coloneqq \mathcal{O}_K$.

Definition 13.11. For any $s \in \mathbb{Z}_{\geq 1}$, the *sth unit group* $U_K^{(s)}$ is determined by

$$U_K^{(s)} = (1 + \pi^s \mathcal{O}_K, \times). \tag{13.6}$$

By convention, set $U_K^{(0)} = U_K$. Then we have a filtration

$$U_K = U_K^{(0)} \supset U_K^{(1)} \supset \cdots \tag{13.7}$$

Proposition 13.12.

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

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

Proof. (i): The reduction $\mod \pi$ map $\mathcal{O}_K^\times \to k^\times$ is surjective and has kernel $1 + \pi\mathcal{O}_K \cong U_K^{(1)}$.

(ii): We have a map $f : U_K^{(s)} \to k$ given by $1 + \pi^s x \to x \mod \pi$. As

$$(1 + \pi^s x)(1 + \pi^s y) = 1 + \pi^s(x + y + \pi^s xy) \tag{13.8}$$

we have that f is a group homomorphism. f is clearly surjective with kernel $1 + \pi^{s+1}\mathcal{O}_K = U_K^{(s+1)}$ so we are done. □

Remark 13.13. Let $[K:\mathbb{Q}_p] < \infty$. By Proposition 13.9 and 13.10, we can find some finite index subgroup of $\mathcal{O}_K^\times$ isomorphic to $(\mathcal{O}_K, +)$ by taking $U_K^{(r)}$ with r sufficiently large as in Proposition 13.9.

Example 13.14. Let $\mathcal{O}_K = \mathbb{Z}_p$ for $p > 2$. Then $e = 1$, so we can take $r = 1$. Then

$$\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \tag{13.9}$$

where the first map is given by

$$x \mapsto (x \mod p, x/[x \mod p] \tag{13.10}$$

where $[x \mod p]$ is the Teichmüller lift.

If $p = 2$, then $e = 1$, but we need to take $r = 2$. Then

$$\mathbb{Z}_2^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + 4\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \tag{13.11}$$

where the first isomorphism is given by

$$x \mapsto (x \mod 4, x \cdot \epsilon(x) \tag{13.12}$$

where

$$\epsilon(x) = \begin{cases} 1 & x = 1 \mod 4 \\ -1 & x = 3 \mod 4 \end{cases} \tag{13.13}$$

From this it is apparent that

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^2 & p = 2 \end{cases} \tag{13.14}$$

14 Higher ramification groups

The higher ramification groups are analogous to higher unit groups. Let L/K be a finite Galois extension of local fields and $\pi_L \in \mathcal{O}_L$ a unit.

Definition 14.1. Let v_L be the normalized valuation on $\mathcal{O}_L$. For $s \in \mathbb{R}_{\geq -1}$, the sth *ramification group* is

$$G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid v_L(\sigma(x) - x) \geq s + 1 \ \forall x \in \mathcal{O}_L\}. \tag{14.1}$$

It is the elements of $\mathrm{Gal}(L/K)$ which "reduce to the identity mod π^s".

Remark 14.2. G_s only changes at integers. But we define G_s for any $\mathbb{R}_{\geq -1}$ so that we can later define the "upper numbering" (see the end of these notes).

Example 14.3.

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

2.
$$\begin{aligned} G_0(L/K) &= \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \mod \pi_L \ \forall x \in \mathcal{O}_L\} \\ &= \ker(\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)) \\ &= I_{L/K} \end{aligned} \tag{14.2}$$

For $s \in \mathbb{Z}_{\geq 0}$, we have that

$$G_s(L/K) = \ker(\mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{O}_L/\pi_L^{s+1}\mathcal{O}_L)). \tag{14.3}$$

Thus $G_s(L/K)$ is normal in G, and we have a filtration

$$\mathrm{Gal}(L/K) = G_{-1} \supset G_0 \supset G_1 \supset \cdots \tag{14.4}$$

Theorem 14.4.

(i) For $s \geq 1$,

$$G_s = \{\sigma \in G_0 \mid v_L(\sigma(\pi_L) - \pi_L) \geq s+1\}. \tag{14.5}$$

(ii)

$$\bigcap_{n=0}^{\infty} G_n = \{1\}. \tag{14.6}$$

(iii) There is an injective group homomorphism for $s \in \mathbb{Z}_{\geq 0}$

$$G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}. \tag{14.7}$$

induced by $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$. This map is independent of the choice of π_L.

Proof. Let $K \subset K_0 \subset L$ be the maximal unramified subextension of L/K, upon replacing K by K_0 we may assume that L/K is totally ramified, which we can do because it does not change the inertia group. By Theorem 13.9, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

(i): Suppose that $v_L(\sigma(\pi_L)-\pi_L) \geq s+1$. Let $x \in \mathcal{O}_L$, so then $x = f(\pi_L)$ for some $f(x) \in \mathcal{O}_K[x]$. Then

$$\begin{aligned} \sigma(x) - x &= \sigma(f(\pi_L)) - f(\pi_L) \\ &= f(\sigma(\pi_L)) - f(\pi_L) \\ &= (\sigma(\pi_L) - \pi_L)g(\pi_L) \end{aligned} \tag{14.8}$$

for some $g(x) \in \mathcal{O}_K[x]$ as $\sigma(x)^m - x^m = (\sigma(x) - x)(\sigma(x)^{m+1} + \cdots x^{m+1})$. Thus

$$\begin{aligned} v_L(\sigma(x) - x) &= v_L(\sigma(\pi_L) - \pi_L) + v_L(g(\pi_L)) \\ &\geq s - 1. \end{aligned} \tag{14.9}$$

(ii): Suppose $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \neq 1$. Then $\sigma(\pi_L) - \pi_L \neq 0$, because $L = K(\pi_L)$, so $v_L(\sigma(\pi_L) - \pi_L) < \infty$. Thus $\sigma \notin G_s$ for $s > v_L(\sigma(\pi_L) - \pi_L)$ by (i).

(iii): For $\sigma \in G_s$ with $s \in \mathbb{Z}_{\geq 0}$, we have that $\sigma(\pi_L) \in \pi_L + \pi_L^{s+1}\mathcal{O}_L$ so

$$\frac{\sigma(\pi_L)}{\pi_L} \in 1 + \pi_L^s\mathcal{O}_L = U_L^{(s)}. \tag{14.10}$$

Thus the map $\varphi : G_s \to U_L^{(s)}/U_L^{(s+1)}$ is well-defined.

We want to show φ is a group homomorphism with kernel G_{s+1}. For $\sigma, \tau \in G_s$, let $\tau(\pi_L) = u\pi_L$ with $u \in \mathcal{O}_L^\times$. Then

$$\begin{aligned} \frac{\sigma\tau(\pi_L)}{\pi_L} &= \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)} \cdot \frac{\tau(\pi_L)}{\pi_L} \\ &= \frac{\sigma(u)}{u} \cdot \frac{\sigma(\pi_L)}{\pi_L} \cdot \frac{\tau(\pi_L)}{\pi_L}. \end{aligned} \tag{14.11}$$

In order to show that this is a group homomorphism, we need to show that $\frac{\sigma(u)}{u} \in U_L^{(s+1)}$. But $\sigma(u) \in u + \pi_L^{(s+1)}\mathcal{O}_L$ since $\sigma \in G_s$, so we are done.

Moreover we have that

$$\ker \varphi = \{\sigma \in G_s \mid \sigma(\pi_L) \equiv \pi_L \mod \pi_L^{s+2}\} = G_{s+1} \tag{14.12}$$

since in this case $\sigma(\pi_L)/\pi_L \equiv 1 \mod \pi_L^{s+2}$.

If $\pi_L' = u\pi_L$ is another uniformizer with $u \in \mathcal{O}_L^\times$, then

$$\frac{\sigma(\pi_L')}{\pi_L'} = \frac{\sigma(u)}{u} \cdot \frac{\sigma(\pi_L)}{\pi_L} \tag{14.13}$$

and since $\frac{\sigma(u)}{u} \in U_L^{(s+1)}$, we get the same map. □

Corollary 14.5. Gal(L/K) *is solvable.*

Proof. By Proposition 13.12, Theorem 14.4, and Theorem 13.4, we have that

$$G_s/G_{s+1} \cong \text{ a subgroup of } \begin{cases} \mathrm{Gal}(k_L/k) & s = -1 \\ (k_L^\times, \times) & s = 0 \\ (k_L, +) & s \geq 1 \end{cases} \tag{14.14}$$

These groups are all abelian, and since $\bigcap G_n = \{1\}$, the successive quotients are all abelian and "exhaust" Gal(L/K), so Gal(L/K) is solvable. □

Let char$(k) = p$. Then G_0/G_1 embeds into a group of order $p^m - 1$, so $p \nmid |G_0/G_1|$ and $|G_1| = p^n$. Thus G_1 is the unique (and hence normal) Sylow p-subgroup of $G_0 = I_{L/K}$.

Definition 14.6. G_1 is the *wild inertia group* and G_0/G_1 is the *tame quotient.*

Now let L/K be separable, finite. We say that L/K is *tamely ramified* if char $k \nmid e_{L/K}$. Otherwise it is *wildly ramified.*

Theorem 14.7 (Different measures ramification upstairs)**.** *Let $[K : \mathbb{Q}_p] < \infty$, L/K finite, and $D_{L/K} = (\pi^{\delta(L/K)})$. Then $\delta(L/K) \geq e_{L/K} - 1$, with equality if and only if L/K is tamely ramified. In particular, L/K is unramified if and only if $D_{L/K} = \mathcal{O}_L$.*

Proof. By Sheet 3, $D_{L/K} = D_{L/K_0} D_{K_0/K}$ so it suffices to check the totally ramified and unramified cases.

Case 1: L/K **unramified:** By Proposition 6.14, we have a power basis $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ where $\alpha \in \mathcal{O}_L$ satisfies $k_L = k(\overline{\alpha})$. Let $g(x) = \mathcal{O}_K[x]$ be the monic minimal polynomial of α. Then $[L : K] = [k_L : k]$ because L/K is unramified, so $\overline{g}(x)$ is the minimal polynomial of $\overline{\alpha}$. Thus $\overline{g}(x)$ is separable, so $g'(\alpha) \neq 0 \mod \pi_L$. By Theorem 12.10, we then have that $D_{L/K} = (g'(\alpha)) = \mathcal{O}_L$.

Case 2: L/K totally ramified We have that $[L:K]=e$, $\mathcal{O}_L=\mathcal{O}_K[\pi_L]$, where π_L is a root of $g(x)=x^e+a_{e-1}x^{e-1}+\cdots+a_0\in\mathcal{O}_K[x]$ an Eisenstein polynomial. Then

$$g'(\pi_L)=e\pi_L^{e-1}+\sum_{i=0}^{e-1}ia_i\pi_i^{i-1} \tag{14.15}$$

The first term has valuation v_L greater than $e-1$, and the terms in the sum have valuation v_L greater than e as g is Eisenstein, so $v_L(g'(\pi_L))\geq e-1$, with equality if and only if $v_L(e)=0$, if and only if $p\nmid e$, if and only if L/K is tamely ramified. □

Corollary 14.8. *Let L/K be an extension of number fields, $\mathfrak{P}\subset\mathcal{O}_L$, and $\mathfrak{P}\cap\mathcal{O}_K=\mathfrak{p}$. Then $e(\mathfrak{P}/\mathfrak{p})>1$ if and only if $\mathfrak{P}\mid D_{L/K}$.*

Proof. By Theorem 12.11 $D_{L/K}=\prod_{\mathfrak{P}}D_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$, and $e(\mathfrak{P}/\mathfrak{p})=e_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$. So applying Theorem 14.7 gives the result.

In particular, we have that $e(\mathfrak{P}/\mathfrak{p})>1$ if and only if $\delta(L_{\mathfrak{P}}/K_{\mathfrak{p}})>0$ if and only if $\mathfrak{P}\mid D_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ if and only if $\mathfrak{P}\mid D_{L/K}$. □

Example 14.9. Let $K=\mathbb{Q}_p$, ζ_{p^n} a primitive $p^{n\text{ th}}$ root of unity, and $L=\mathbb{Q}_p(\zeta_{p^n})$. The pth cyclotomic polynomial is

$$\Phi_{p^n}(x)=x^{p^{n-1}(p-1)}+x^{p^{n-1}(p-2)}+\cdots+1=(x^{p^n}-1)(x^p-1)\in\mathbb{Z}_p[x]. \tag{14.16}$$

On sheet 3, we will show that

1. $\Phi_{p^n}(x)$ is irreducible, so Φ_{p^n} is the minimal polynomial of ζ_{p^n}.

2. $L/\mathbb{Q}_p$ is Galois, totally ramified of degree $p^{n-1}(p-1)$.

3. $\pi=\zeta_{p^n}-1$ is a uniformizer of $\mathcal{O}_L$, so $\mathcal{O}_L=\mathbb{Z}_p[\zeta_{p^n}-1]=\mathbb{Z}_p[\zeta_{p^n}]$.

4. $\mathrm{Gal}(L/\mathbb{Q}_p)\cong(\mathbb{Z}/p^n\mathbb{Z})^\times$ is abelian, and the isomorphism is given by $\sigma_m\mapsto m$, where $\sigma_m(\zeta_{p^n})=\zeta_{p^n}^m$.

We want to understand the decomposition groups G_s that σ_m lies in. So we need to understand

$$v_L(\sigma_m(\pi)-\pi)=v_L(\sigma_m(\zeta_{p^n}-1)-(\zeta_{p^n}-1))=v_L(\zeta_{p^n})v_L(\zeta_{p^n}^{m-1}-1)=v_L(\zeta_{p^n}^{m-1}-1). \tag{14.17}$$

Let k be the maximal integer such that $p^k\mid m-1$. Then $\zeta_{p^n}^{m-1}$ is a primitive p^{n-k}th root of unity, so $\pi'=\zeta_{p^n}^{m-1}-1$ is a uniformizer of $L'=\mathbb{Q}_p(\zeta_{p^n}^{m-1})$. So

$$\begin{aligned}v_L(\zeta_{p^n}^{m-1})&=e_{L/L'}\\&=\frac{e_{L/\mathbb{Q}_p}}{e_{L'/\mathbb{Q}_p}}\\&=\frac{[L:\mathbb{Q}_p]}{[L':\mathbb{Q}_p]}\\&=\frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)}=p^k\end{aligned} \tag{14.18}$$

Then by Theorem 14.4 (i), $\sigma_m \in G_i$ if and only if $p^k \geq i+1$. Thus

$$G_i \cong \begin{cases} (\mathbb{Z}/p^n\mathbb{Z})^\times & i = 0 \\ (1+p^k\mathbb{Z})/p^n\mathbb{Z} & p^{k-1}-1 < i \leq p^k - 1 \\ \{1\} & p^{n-1} - 1 < i \end{cases} \tag{14.19}$$

Part VI
Local class field theory

15 Filler section

In my notes there is no Section 15 so we skip to Section 16

16 Infinite Galois theory

Let L/K be an algebraic extension of fields of possibly infinite degree.

Definition 16.1.

(i) L/K is *separable* if for all $x \in L$, the minimal polynomial $f_\alpha(x) \in K[x]$ for α is separable.

(ii) L/K is *normal* if $f_\alpha(x)$ splits in L for all $\alpha \in L$.

(iii) L/K is *Galois* if it is separable and normal.

If L/K is finite and Galois, the Galois correspondence gives us a bijection between subextensions $K \subset K' \subset L$ and subgroups of $\mathrm{Gal}(L/K)$ where normal subgroups correspond to Galois (normal) subextensions.

The infinite case is not exactly the same, as we need to define a topology on $\mathrm{Gal}(L/K)$ so we only look at closed subgroups (general subgroups can get unwieldy very quickly).

Definition 16.2. Let $(I, \leq)$ be a poset. We say that I is a *directed set* if for all $i, j \in I$, there exists $k \in I$ such that $i \leq k$ and $j \leq k$. So i and j always have a join.

Example 16.3. Any total order is a directed set.

Definition 16.4. Let $(I, \leq)$ be a directed set, and $(G_i)_{i\in I}$ a collection of groups with morphisms $\varphi_{ij} : G_j \to G_i$ for all $i \leq j$ such that $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ for all $i \leq j \leq k$ and $\varphi_{ii} = \mathrm{id}_{G_i}$. We say that $((G_i)_{i\in I}, (\varphi_{ij}))$ is an *inverse system*, and the *inverse limit* of $((G_i), (\varphi_{ij}))$ is

$$\varprojlim_{i\in I} G_i = \{(g_i)_{i\in I} \mid \varphi_{ij}(g_i) = g_j\} \tag{16.1}$$

Remark 16.5. We have projection maps $\psi_j : \varprojlim_{i\in I} G_i \to G_j$ given by $(g_i) \mapsto g_j$.

The universal property of inverse limits is that for any objection X with morphisms $\eta_j : X \to G_j$ which are compatible with φ_{ij}, the morphisms η_j factor through ψ_j by some unique morphism η.

The profinite topology on $\varprojlim G_i$ is the weakest topology such that ψ_j are all continuous, where G_j has the discrete topology. So $\psi_j^{-1}(g)$ is clopen for all $g \in G_j$.

Proposition 16.6. *Let L/K be Galois.*

(i) The set $I = \{F/K \text{ finite} \mid F \subset L, F \text{ Galois}\}$ is a directed set under inclusion (the compositum is the join).

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

$$\mathrm{res}_{F,F'} : \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K) \tag{16.2}$$

and the natural map

$$\mathrm{Gal}(L/K) \to \varprojlim_{F' \subset F} \mathrm{Gal}(F/K) \tag{16.3}$$

is an isomorphism.

Theorem 16.7 (Fundamental theorem of infinite Galois theory)**.** *Let L/K be Galois, and endow* $\mathrm{Gal}(L/K)$ *with the profinite topology (which is discrete if L/K is finite). Then there exists a bijection*

$$\begin{aligned} \{\textit{subextensions } L/F/K\} &\Leftrightarrow \{\textit{closed subgroups of } \mathrm{Gal}(L/K)\} \\ F &\mapsto \mathrm{Gal}(L/F) \\ L^H &\leftarrow\!\shortmid H \subset \mathrm{Gal}(L/K) \end{aligned} \tag{16.4}$$

Moreover, F/K is finite if and only if $\mathrm{Gal}(L/F)$ *is open and F/K is Galois if and only if* $\mathrm{Gal}(L/F)$ *is normal.*

Proof. Example Sheet 4. □

Example 16.8. Let $K = \mathbb{F}_q$, and $L = \overline{F}_q$ be the algebraic closure. Then L/K is Galois because $\mathbb{F}_q$ is perfect. The finite subextensions of L are of the form $\mathbb{F}_{q^n}$ for $n \geq 1$, and $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ if and only if $m \mid n$. There exists a commutative diagram (where the vertical maps are $\mathrm{Frob}_q \leftrightarrow 1$)

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \arrow[r, "\mathrm{res}"] \arrow[d, leftrightarrow] & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \arrow[d, leftrightarrow] \\
\mathbb{Z}/n\mathbb{Z} \arrow[r, "\mathrm{proj}"] & \mathbb{Z}/m\mathbb{Z}
\end{tikzcd}$$

So $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \lim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$, the profinite integers. We have that $\langle \mathrm{Frob}_q \rangle$ corresponds to $\mathbb{Z} \subset \hat{\mathbb{Z}}$.

16.1 The Weil Group

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

Definition 16.9.

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

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

Proposition 16.10. *Let L/K be unramified. Then L/K is Galois and* $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$.

Proof. We reduce to the finite case. Every finite subextension F/K is unramified, and hence Galois, so L/K is normal and separable, and hence Galois. Moreover, there exists a diagram

$$\begin{tikzcd}
\mathrm{Gal}(L/K) \arrow[r, "\mathrm{res}"] \arrow[d, leftrightarrow] & \mathrm{Gal}(k_L/k) \arrow[d, leftrightarrow] \\
\varprojlim \mathrm{Gal}(F/K) \arrow[r, "\star"] & \varprojlim \mathrm{Gal}(k'/k)
\end{tikzcd}$$

The map $\star$ exists because finite subextensions of L are in bijection with finite subextensions k'/k. This is because given any $k \subset k' \subset k_L$, we can lift to an unramified subextension $K \subset K' \subset K_L$ by adding roots of unity (this is the basic theory of unramified extensions). Thus the index sets match, so $\star$ exists and res is an isomorphism. □

If $L_1, L_2/K$ are both finite and unramified implies that L_1L_2/K is unramified (Sheet 3). Thus for any L/K there exists a maximal unramified subextension K_0/K which is the compositum of all the unramified subextensions.

Now, let L/K be Galois. Then there exists a surjection

$$\mathrm{res} : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K_0/K) \cong \mathrm{Gal}(k_L/k). \tag{16.5}$$

Set $I_{L/K} \coloneqq \ker(\mathrm{res})$ to be the inertia subgroup. Let $\mathrm{Frob}_{k_L/k} \in \mathrm{Gal}(k_L/k)$ be the Frobenius element $x \mapsto x^{|k|}$ and let $\langle \mathrm{Frob}_{k_L/k} \rangle$ be the subgroup generated by $\mathrm{Frob}_{k_L/k}$.

Definition 16.11. Let L/K Galois. The *Weil group* $W(L/K) \subset \mathrm{Gal}(L/K)$ is $\mathrm{res}^{-1}(\langle \mathrm{Frob}_{k_L/k} \rangle)$.

Remark 16.12. If k_L/k is finite, then $W(L/K) = \mathrm{Gal}(L/K)$. Otherwise $W(L/K) \subsetneq \mathrm{Gal}(L/K)$. There exists a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & I_{L/K} \arrow[r] \arrow[d, "="] & W(L/K) \arrow[r] \arrow[d, hook] & \langle \mathrm{Frob}_{k_L/k} \rangle \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & I_{L/K} \arrow[r] & \mathrm{Gal}(L/K) \arrow[r] & \mathrm{Gal}(k_L/k) \arrow[r] & 0
\end{tikzcd}$$

So $W(L/K)$ is the part of $\mathrm{Gal}(L/K)$ corresponding to $\mathrm{Frob}_{k_L/k}$.

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

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

2. $I_{L/K}$ is an open subgroup of $W(L/K)$

where $I_{L/K} = \mathrm{Gal}(L/K_0)$ has the profinite topology. So $W(L/K)$ has a basis of open sets given by translates of open sets in $I_{L/K}$ by elements of $W(L/K)$. So the basis is of the form $w + U$ with $w \in W(L/K)$ and $U \subset I_{L/K}$ open.

Remark 16.13. Warning! The topology on $W(L/K)$ is *not* the subspace topology induced by $W(L/K) \subset \mathrm{Gal}(L/K)$ if k_L/k is infinite.

For example, $I_{L/K} \subset W(L/K)$ is not open in the subspace topology because $I_{L/K}$ does not have finite index.

Proposition 16.14. *Let L/K be Galois.*

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

(ii) If F/K is a finite subextension of L/K, then

$$W(L/F) \cong W(L/K) \cap \mathrm{Gal}(L/F). \tag{16.6}$$

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

$$\mathrm{Gal}(F/K) \cong W(L/K)/W(L/F) \tag{16.7}$$

Proof. (i): $W(L/K)$ is dense if and only if for all F/K finite Galois, $W(L/K)$ intersects every coset of $\mathrm{Gal}(L/F)$. This is true if and only if for all F/K finite Galois, $W(L/K) \twoheadrightarrow \mathrm{Gal}(F/K)$. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & I_{L/K} \arrow[r] \arrow[d, "a"] & W(L/K) \arrow[r] \arrow[d, "b"] & \langle \mathrm{Frob}_{k_L/k} \rangle \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & I_{F/K} \arrow[r] & W(F/K) = \mathrm{Gal}(F/K) \arrow[r] & \langle \mathrm{Frob}_{k_F/k} \rangle = \mathrm{Gal}(k_F/k) \arrow[r] & 0
\end{tikzcd}$$

Let $L/K_0/K$ be the maximal unramified subextension. Then $K_0 \cap F$ is the maximal unramified subextension of F/K. So $\mathrm{Gal}(L/K_0) \twoheadrightarrow \mathrm{Gal}(FK_0/K_0) = \mathrm{Gal}(F/K_0 \cap F)$, so a is surjective as $I_{F/K} \cong \mathrm{Gal}(F/K_0 \cap F)$ and $I_{L/K} \cong \mathrm{Gal}(L/K_0)$. We have that $\mathrm{Gal}(k_F/k)$ is generated by $\mathrm{Frob}_{k_F/k}$ so c is surjective. So by the snake lemma, b is surjective.

(ii): We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(L/F) \arrow[r, two heads] \arrow[d, hook] & \mathrm{Gal}(k_L/k_F) \arrow[d, hook] & \langle \mathrm{Frob}_{k_L/k_F} \rangle \arrow[l, hook', "\supseteq"'] \arrow[d, hook] \\
\mathrm{Gal}(L/K) \arrow[r, two heads] & \mathrm{Gal}(k_L/k) & \langle \mathrm{Frob}_{k_L/k} \rangle \arrow[l, hook', "\supseteq"']
\end{tikzcd}$$

For $\sigma \in \mathrm{Gal}(L/F)$, $\sigma \in W(L/F)$ if and only if $\sigma|_{k_L} \in \langle \mathrm{Frob}_{k_L/k_F} \rangle$, if and only if $\sigma|_{k_L} \in \langle \mathrm{Frob}_{k_L/k} \rangle$. Now, we have that $\mathrm{Gal}(k_L/k_F) \cap \langle \mathrm{Frob}_{k_L/k} \rangle = \langle \mathrm{Frob}_{k_L/k_F} \rangle$, which follows from the fact that $n\hat{\mathbb{Z}} \cap \mathbb{Z} = n\mathbb{Z}$, so $\sigma|_{k_L} \in \langle \mathrm{Frob}_{k_L/k} \rangle$ if and only if $\sigma \in W(L/K)$.

(iii) We do a messy derivation

$$\begin{aligned}
W(L/K)/W(L/F) &= W(L/K)/(W(L/K) \cap \mathrm{Gal}(L/F)) \\
&\cong W(L/K)\,\mathrm{Gal}(L/F)/\,\mathrm{Gal}(L/F) \\
\star &\cong \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/F) \\
&\cong \mathrm{Gal}(F/K).
\end{aligned} \tag{16.8}$$

$\star$ follows from part (i) and the fact that $\mathrm{Gal}(L/F)$ is an open subgroup. □

17 Statements of local class field theory

Let K be a local field.

Definition 17.1. An extension L/K is *abelian* if it is Galois and $\mathrm{Gal}(L/K)$ is abelian. We have that

(i) If $L_1, L_2/K$ are abelian, then L_1L_2/K is abelian.

(ii) If $L_1 \cap L_2 = K$, then there exists a canonical isomorphism

$$\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K). \tag{17.1}$$

(i) implies that there exists a maximal abelian extension K^{ab} of K by taking the compositum of all abelian extensions.

Example 17.2. Let K^{ab} denote the maximal abelian extension of K inside K^{sep}. Let

$$K^{\mathrm{un}} = \bigcup_{m \geq 1} K(\zeta_{q^m-1}) \tag{17.2}$$

where $|k| = q$. Then K^{un} is the maximal unramified extension of K by the theory of unramified extensions, and $k_{K^{\mathrm{un}}} = \overline{\mathbb{F}}_q$. We have that $\mathrm{Gal}(K^{\mathrm{un}}/K) \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$, so the maximal unramified extension is abelian, and hence contained in K^{ab}. Thus $k_{K^{\mathrm{ab}}} = \overline{\mathbb{F}}_q$, so there exists a SES

$$\begin{tikzcd} 0 \arrow[r] & I_{K^{\mathrm{ab}}/K} \arrow[r] & W(K^{\mathrm{ab}}/K) \arrow[r] & \mathbb{Z} \cong \langle \mathrm{Frob}_{K^{\mathrm{ab}}/K} \rangle \arrow[r] & 0 \end{tikzcd}$$

Theorem 17.3 (Locally Artin reciprocity)**.**

(i) There exists a unique topological isomorphism (a group isomorphism and a homeomorphism)

$$\mathrm{Art}_K : K^\times \to W(K^{\mathrm{ab}}/K) \tag{17.3}$$

which satisfies

(a) $\mathrm{Art}_K(\pi)|_{K^{\mathrm{un}}} = \mathrm{Frob}_{K^{\mathrm{un}}/K}$ *for any uniformizer* $\pi \in K$*.*

(b) For each finite abelian subextension L/K *in* K^{ab}/K*,*

$$\mathrm{Art}_K(N_{L/K}(L^\times))|_L = \{1\} \tag{17.4}$$

(ii) Let L/K *be a finite abelian. Then* Art_K *induces an isomorphism*

$$K^\times/N_{L/K}(L^\times) \cong W(K^{\mathrm{ab}}/K)/W(K^{\mathrm{ab}}/L) \cong \mathrm{Gal}(L/K) \tag{17.5}$$

Remark 17.4.

(i) The local Artin map is used to characterize the global Artin map in global class field theory.

(ii) This is a special case of the local Langlands correspondence. The moral of local Langlands is that the Weil group is hard to study in general, but we can look at representations of the Weil-(Deligne) group, and compare to p-adic groups.

17.1 Properties of the Artin map

Theorem 17.5 (Existence Theorem)**.** *For any $H \subset K^\times$ open, finite index, there exists L/K a finite abelian extension such that $N_{L/K}(L^\times) = H$. In particular, we can understand abelian extensions by studying $K^\times$. The Artin map induces an isomorphism of posets (which is inclusion reversing)*

$$\begin{aligned} \textit{open finite index subsets of } K^\times &\Leftrightarrow \{\textit{finite abelian extensions of } K\} \\ H &\mapsto (K^{\mathrm{ab}})^{\mathrm{Art}_K(H)} \\ N_{L/K}(L^\times) &\leftarrow\!\shortmid L/K \end{aligned} \tag{17.6}$$

Theorem 17.6 (Norm functoriality)**.** *Let L/K be any finite separable extension. Then the following diagram commutes*

$$\begin{tikzcd} L\times \arrow[r, "\mathrm{Art}_L"] \arrow[d, "N_{L/K}"] & W(L^{\mathrm{ab}}/L) \arrow[d, "\mathrm{res}"] \\ K\times \arrow[r, "\mathrm{Art}_K"] & W(K^{\mathrm{ab}}/K) \end{tikzcd}$$

17.2 Construction of the Artin map for $\mathbb{Q}_p$

Recall that

$$\mathbb{Q}_p^{\mathrm{un}} = \bigcup_{m=1}^{\infty} \mathbb{Q}_p(\zeta_{p^m-1}) = \bigcup_{p \nmid m} \mathbb{Q}_p(\zeta_m) \tag{17.7}$$

is the extension of $\mathbb{Q}_p$ obtained by adjoing all roots of unity relatively prime to p. Also, $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$ with isomorphism

$$\theta_n : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \to (\mathbb{Z}/p^n\mathbb{Z})^\times. \tag{17.8}$$

For $n \geq m \geq 1$, there exists a diagram

$$\begin{tikzcd} \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \arrow[r, "\mathrm{res}"] \arrow[d, "\theta_n"] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) \arrow[d, "\theta_m"] \\ (\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r] & (\mathbb{Z}/p^m\mathbb{Z})^\times \end{tikzcd}$$

Set

$$\mathbb{Q}_p(\zeta_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^n}). \tag{17.9}$$

Then $\mathbb{Q}_p(\zeta_{p^\infty})$ is Galois and we have

$$\theta : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \xrightarrow{\cong} \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times \tag{17.10}$$

We have that $\mathbb{Q}_p(\zeta_{p^\infty}) \cap \mathbb{Q}_p^{\mathrm{un}} = \mathbb{Q}_p$ because one is totally ramified, and the other is unramified. So then there exists an isomorphism

$$\mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^\infty})\mathbb{Q}_p^{\mathrm{un}}/\mathbb{Q}_p\right) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times. \tag{17.11}$$

Theorem 17.7.

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{un}}\mathbb{Q}_p(\zeta_{p^\infty}) \tag{17.12}$$

Remark 17.8. $\mathbb{Q}_p(\zeta_{p^\infty})$ is not the *canonical* totally ramified extension, and non exists.

We construct $\mathrm{Art}_{\mathbb{Q}_p}$ as follows: we have that

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times \tag{17.13}$$

which is non-canonical! Then

$$\mathrm{Art}_{\mathbb{Q}_p}(p^n u) = \Big((\mathrm{Frob}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p})^n, \theta^{-1}(u^{-1}) \Big) \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \tag{17.14}$$

We can check that the image lies in $W(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$, which is intuitive as we would expect $W(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \mathbb{Z} \times \mathbb{Z}_p^\times \subset \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$.

We can also check that this map is independent of the choice of totally ramified extension, $\pi \in \mathbb{Q}_p$.

17.3 Construction of Artin map for arbitrary K

Based off of the $\mathbb{Q}_p$ case, our question is how to adjoin p^nth roots of unity to a local field K? Let K be a local field and π a uniformizer. For $n \geq 1$, construct $K_{\pi,n}$ a totally ramified Galois extension such that

(i) $K \subset K_{\pi,1} \subset \cdots$.

(ii) For $n \geq m \geq 1$, there exists a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(K_{\pi,n}/K) \arrow[r, two heads] \arrow[d, leftrightarrow, "\psi_n \cong"] & \mathrm{Gal}(K_{\pi,m}/K) \arrow[d, leftrightarrow, "\psi_m \cong"] \\
\mathcal{O}_K^\times/U_K^{(n)} \arrow[r, "\mathrm{proj}"] & \mathcal{O}_K^\times/U_K^{(m)}
\end{tikzcd}$$

(iii) Setting $K_{\pi,\infty} = \bigcup K_{\pi,n}$, we have that

$$K^{\mathrm{ab}} = K^{\mathrm{un}} K_{\pi,\infty} \tag{17.15}$$

Then (ii) implies that there exists an isomorphism

$$\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \cong \varprojlim \mathcal{O}_K^\times/U_k^{(n)} = \mathcal{O}_K^\times. \tag{17.16}$$

We define Art_K by

$$\begin{aligned} K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times &\to \mathrm{Gal}(K^{\mathrm{un}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \pi^n u &\mapsto (n,u) \mapsto ((\mathrm{Frob}_{K^{\mathrm{un}}/K})^n, \psi^{-1}(u^{-1})) \end{aligned} \tag{17.17}$$

The analogy with the $\mathbb{Q}_p$ case is

$$\begin{tikzcd}
 & \mathbb{Q}_p^{\mathrm{ab}} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_p^{\mathrm{un}} \arrow[dr, dash, "\widehat{\mathbb{Z}}"] & & \mathbb{Q}_p(\zeta_{p^\infty}) \arrow[dl, dash, "\mathbb{Z}_p^\times"] \\
 & \mathbb{Q}_p &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & K^{\mathrm{ab}} \arrow[dl, dash] \arrow[dr, dash] & \\
K^{\mathrm{un}} \arrow[dr, dash, "\widehat{\mathbb{Z}}"] & & K_{\pi,\infty} \arrow[dl, dash, "\mathcal{O}_K^\times"] \\
 & K &
\end{tikzcd}$$

Remark 17.9. Both $K_{\pi,\infty}$ and the isomorphism $K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$ depend on π. For different choice of π, the Artin maps agree, so Art_K is canonical.

So now, our goal is to construct $K_{\pi,n}$. This will take some work.

Part VII
Lubin-Tate theory

The main idea is that ζ_{p^n} are torsion points in $\overline{\mathbb{Q}}_p^\times$.

18 Formal group laws

Let R be a ring, and $R[[x_1, \ldots, x_n]]$ the ring of formal power series.

Definition 18.1. A (1-dimensional, commutative) *formal group law* over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying

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

(ii) $F(X,0) = X$, $F(0,Y) = Y$.

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

Example 18.2.

1. $\widehat{\mathbb{G}}_a(X,Y) = X + Y$ the formal additive group.

2. $\widehat{\mathbb{G}}_m(X,Y) = X + Y + XY$ the formal multiplicative group.

Lemma 18.3. *There exists a unique $i(X) \in R[[X]]$ such that $i(0) = 0$ and $F(X, i(X)) = 0$.*

Proof. Sheet 4. □

Now let K be a complete, non-archimedean valued field. If F is a formal group law over $\mathcal{O}_K$, then $F(X,Y)$ converges for all $x, y \in \mathfrak{m}$ to an element of $\mathfrak{m}$. Define $x \cdot_F y = F(x,y)$, then $(\mathfrak{m}_K, \cdot_F)$ is a commutative group.

Example 18.4. Let $\widehat{\mathbb{G}}_m/\mathbb{Z}_p$ be the formal group $x \cdot_{\widehat{\mathbb{G}}_m} y = x + y + xy$. Then $(p\mathbb{Z}_p, \cdot_{\widehat{\mathbb{G}}_m}) \cong (1 + p\mathbb{Z}_p, \times)$ under $x \mapsto 1 + x$ which is easy to verify.

Definition 18.5. Homorphism of formal groups. Define $\mathrm{End}_R(F)$ to be the set of formal group homomorphisms $f : F \to F$.

Proposition 18.6. *Suppose R is a $\mathbb{Q}$-algebra. There is an isomorphism of formal group laws $\exp(X) : \widehat{\mathbb{G}}_a \to \widehat{\mathbb{G}}_m$ given by*

$$\exp(X) = \sum_{n=1}^{\infty} \frac{X^n}{n!} = e^X - 1. \tag{18.1}$$

Proof. Define

$$\log X = sum_{n=1}^{\infty} \frac{(-1)^{n-1} X^n}{n}. \tag{18.2}$$

Then there exists an equality of formal power series by $\log(\exp(X)) = X = \exp(\log(X))$. We can also check that

$$\exp(\widehat{\mathbb{G}}_a(X,Y)) = \widehat{\mathbb{G}}_m(\exp(X), \exp(Y)). \tag{18.3}$$

□

Lemma 18.7. $\mathrm{End}_R(F)$ *is a ring with*

$$\begin{aligned} (f +_F g)(X) &= F(f(X), g(X)) \\ (f \cdot_F g)(X) &= f \circ g(X) \end{aligned} \tag{18.4}$$

Proof. Let $f, g \in \mathrm{End}_R(F)$. Then

$$\begin{aligned} (f +_F g) \circ F(X,Y) &= F(f(F(X,Y)), g(F(X,Y))) \\ &= F(F(f(X), f(Y)), F(g(X), g(Y))) \\ &= F(F(f(X), g(X)), F(f(Y), g(Y))) \\ &= F(f +_F g(X), f +_F g(Y)) \end{aligned} \tag{18.5}$$

so $f +_F g$ is an endomorphism. We can similarly check that $f \circ g \circ F = f \circ F \circ g = F \circ f \circ g$ so $f \circ g = f \cdot_F g$ is also an endomorphism. The rest is tedious. □

19 Lubin-Tate formal group laws

Let K be a non-archimedean local field, with $|k| = q$.

Definition 19.1. A *formal $\mathcal{O}_K$-module* over $\mathcal{O}_K$ is a formal group law $F(X,Y) \in \mathcal{O}_K[[X,Y]]$ together with a ring homomorphism $[\cdot]_F : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$ such that for all $a \in \mathcal{O}_K$ we have that

$$[a]_F \equiv aX \mod X^2. \tag{19.1}$$

A homomorphism/isomorphism $f : F \to G$ of formal $\mathcal{O}_K$-modules is a homomorphism/isomorphism of formal group laws such that $f \circ [a]_F = [a]_G \circ f$ for all $a \in \mathcal{O}_K$.

Definition 19.2. Let $\pi \in \mathcal{O}_K$ be a uniformizer. A *Lubin-Tate series* for π is a power series $f(X) \in \mathcal{O}_K[[X]]$ such that

(i) $f(X) \equiv \pi X \mod X^2$.

(ii) $f(X) \equiv x^q \mod \pi$.

Theorem 19.3. *Let $f(X)$ be a Lubin-Tate series for π. Then*

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

(ii) There exists a ring homomorphism

$$[\cdot]_f : \mathcal{O}_K \to \operatorname{End}_{\mathcal{O}_K}(F_f) \tag{19.2}$$

such that $[\pi]_f(X) = f(X)$, which makes F_f a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$.

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

F_f is a Lubin-Tate formal group law *for π, and it depends on π up to isomorphism.*

Example 19.4. Let $K = \mathbb{Q}_p$. Then $f(X) = (X+1)^p - 1$ is a Lubin-Tate series for p. We claim that the Lubin-Tate formal group law F_f is $\widehat{\mathbb{G}}_m$. It suffices to show that $f \circ \widehat{\mathbb{G}}_m = \widehat{\mathbb{G}}_m \circ f$, as then $f \in \operatorname{End}_{\mathcal{O}_K}(\widehat{\mathbb{G}}_m)$, and $\widehat{\mathbb{G}}_m = F_f$ is unique. We have that

$$\begin{aligned} f(\widehat{\mathbb{G}}_m(X,Y)) &= ((X+1)(Y+1) - 1 + 1)^p - 1 \\ &= (X+1)^p(Y+1)^p - 1 \\ &= ((X+1)^p - 1 + 1)((Y+1)^p - 1 + 1) - 1 \\ &= \widehat{\mathbb{G}}_m(f(X), f(Y)). \end{aligned} \tag{19.3}$$

In order to prove Theorem 19.3, we use the following key lemma. It tells us that we can uniquely construct a power series with specified degree 1 terms which intertwines with Lubin-Tate series. Thus if two power series are equivalent modulo degree 2 terms and intertwine with Lubin-Tate series, then they are equal.

Lemma 19.5. *Let $f(X)$, $g(X)$ be Lubin-Tate series for π. Suppose $L(X_1, \ldots, X_n) = \sum a_i X_i$ for $a_i \in \mathcal{O}_K$ is some linear form. Then there exists a unique power series $F(X_1, \ldots, X_n) \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ such that*

(i) $F(X_1, \ldots, X_n) = L(X_1, \ldots, X_n) \mod \deg 2$.

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

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

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

(b) $F_m(X_1, \ldots, X_m) = L(X_1, \ldots, X_m) \mod \deg 2$.

(c) $F_m = F_{m+1} \mod \deg(m+1)$.

For $m = 1$ we take $F_1 = L(X_1, \ldots, X_n)$ which immediately satisfies (b). We have that

$$\begin{aligned} f(F_1(X_1, \ldots, X_n)) &= \pi L(X_1, \ldots, X_n) \mod \deg 2 \\ &= F_1(g(X_1), \ldots, g(X_n)) \mod \deg 2 \end{aligned} \tag{19.4}$$

as f, g are both Lubin-Tate series for π. Suppose we have built F_m for some $m \geq 1$. Set $F_{m+1} = F_m + h$, where $h \in \mathcal{O}_K[X_1, \ldots, X_n]$ is homogeneous of degree $m+1$. Since $f(X+Y) = f(X) + f'(X)Y \mod Y^2$ and $f'(X) \equiv \pi \mod X$, we have that

$$f \circ (F_m + h) = f \circ F_m + \pi h \mod \deg(m+2) \tag{19.5}$$

Similarly,

$$\begin{aligned}(F_m + h) \circ g &= F_m \circ g + h \circ g \\ &= F_m \circ g + h(\pi X_1, \ldots, \pi X_n) \mod \deg(m+2) \\ &= F_m \circ g + \pi^{m+1} h \end{aligned} \tag{19.6}$$

as g is a Lubin-Tate series for π. Thus (a), (b), (c) are satisfied if and only if

$$f \circ F_m - F_m \circ g = (\pi - \pi^{m+1})h \mod \deg(m+2) \tag{19.7}$$

We want to "divide" by $\pi - \pi^{m+1}$, but we need to check that the result is still in $\mathcal{O}_K[X_1, \ldots, X_n]$. But $f(X) = g(X) = x^q \mod \pi$, so

$$f \circ F_m - F_m \circ g = F_m(X_1, \ldots, X_n)^q - F_m(X_1^q, \ldots, X_n^q) \mod \pi = 0 \mod \pi \tag{19.8}$$

Thus $f \circ F_m - F_m \circ g \in \pi \mathcal{O}_K[X_1, \ldots, X_n]$. Let $r(X_1, \ldots, X_n)$ be the degree $m+1$ terms of $f \circ F_m - F_m \circ g$. Then we have that

$$h = \frac{1}{(\pi - \pi^{m+1})} r \in \mathcal{O}_K[X_1, \ldots, X_n] \tag{19.9}$$

works. Since h is determined uniquely by (19.7), which is equivalent to (a), (b), (c), F_{m+1} is uniquely determined. Set $F = \lim F_m$, then F satisfies (i), (ii). The uniqueness follows from the uniqueness of F_m, because if G is another such series, then we must have that $G_m = F_m$, where G_m is the mth partial sum of G.

□

Proof of Theorem 19.3. Out proof strategy is to spam Lemma 19.5 until we're sick of it.

(i) By Lemma 19.5, there exists a unique $F_f(X,Y) \in \mathcal{O}_K[X,Y]$ such that

$$\begin{aligned} F_f(X,Y) &= X + Y \mod \deg 2 \\ f(F_f(X,Y)) &= F_f(f(X), f(Y)) \end{aligned} \tag{19.10}$$

We claim that F_f is a formal group law. To show associativity, we have that

$$F_f(X, F_f(Y,Z)) \equiv F_f(F_f(X,Y), Z) \equiv X + Y + Z \mod \deg 2 \tag{19.11}$$

We also have that

$$f \circ F_f(X, F_f(Y,Z)) = F_f(f(X), f(F_f(Y,Z))) = F_f(f(X), F_f(f(Y), f(Z))) \tag{19.12}$$

and

$$f \circ F_f(F_f(X,Y), Z) = F_f(f(F_f(X,Y)), f(Z)) = F_f(F_f(f(X), f(Y)), f(Z)) \tag{19.13}$$

So both $F_f(X, F_f(Y,Z))$ and $F_f(F_f(X,Y),Z)$ satisfy the condition of Lemma 19.5 with $L(X,Y,Z) = X+Y+Z$, so they are equal. Commutativity follows by the same argument, so F_f is a formal group law. (19.10) then shows that $f \in \mathrm{End}_{\mathcal{O}_K}(F_f)$.

(ii) By Lemma 19.5, for $a \in \mathcal{O}_K$ we have that there exists a unique $[a]_{F_f} \in \mathcal{O}_K[[X]]$ such that $[a]_{F_f} = aX \mod X^2$ and $f \circ [a]_{F_f} = [a]_{F_f} \circ f$. Then

$$\begin{aligned} f \circ ([a]_{F_f} \circ F_f) &= ([a]_{F_f} \circ F_f) \circ f \\ f \circ (F_f \circ [a]_{F_f}) &= (F_f \circ [a]_{F_f}) \circ f \end{aligned} \tag{19.14}$$

and $[a]_{F_f} \circ F_f = F_f \circ [a]_{F_f} \mod \deg 2$, so $[a]_{F_f} \circ F_f = F_f \circ [a]_{F_f}$ by Lemma 19.5. Thus $[a]_{F_f} \in \mathrm{End}_{\mathcal{O}_K}(F_f)$. Likewise, the map $[\cdot]_{F_f} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F_f)$ is a ring homomorphism by Lemma 19.5. So F_f is a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$, and $[\pi]_{F_f} = f$ by Lemma 19.5.

(iii) If $g(X)$ is another Lubin-Tate series for π, let $\theta(X) \in \mathcal{O}_K[[X]]$ be the unique power series such that $\theta(X) = X \mod X^2$ and $\theta \circ f = g \circ \theta$. We have that

$$\begin{aligned} (\theta \circ F_f) \circ f &= g \circ (\theta \circ F_f) \\ (F_g \circ \theta) \circ f &= g \circ (F_g \circ \theta) \end{aligned} \tag{19.15}$$

and as $F_f = F_g = X + Y \mod \deg 2$ and $\theta = X \mod \deg 2$, we have that $\theta \circ F_f = F_g \circ \theta$ by Lemma 19.5. Thus$\theta \in \mathrm{Hom}(F_f, F_g)$. Swapping f and g, we get some $\psi \in \mathrm{Hom}(F_g, F_f)$. We have that $\theta \circ \psi = \psi \circ \theta = X$ by Lemma 19.5 (compare with $i(X) = X$). It also follows from Lemma 19.5 that $\theta \circ [a]_{F_f} = [a]_{F_g} \circ \theta$ for all $a \in \mathcal{O}_K$, and hence θ is an isomorphism of formal $\mathcal{O}_K$-modules. □

20 Lubin-Tate Extensions

Let $\overline{K}$ be an algebraic closure of K, and $\overline{\mathfrak{m}} \subset \mathcal{O}_{\overline{K}}$ the maximal ideal. The next lemma justifies the use of the term "formal $\mathcal{O}_K$-module".

Lemma 20.1. *Let F be a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. Then $\overline{\mathfrak{m}}$ is an $\mathcal{O}_K$-module under (for all $x, y \in \overline{\mathfrak{m}}$, $a \in \mathcal{O}_K$)*

$$\begin{aligned} x +_F y &= F(x,y) \\ a \cdot_F x &= [a]_F(x) \end{aligned} \tag{20.1}$$

Proof. It's important to note that $\overline{K}$ is not complete, so we need to be a bit careful.

If $x \in \overline{\mathfrak{m}}$, then $x \in \mathfrak{m}_L$ for some L/K finite. Then $[a]_F \in \mathcal{O}_K[[X]]$, so $[a]_{F_f}(X)$ converges in L and since $\mathfrak{m}_L$ is closed, $[a]_F(x) \in \mathfrak{m}_L \in \overline{\mathfrak{m}}$. Similarly $x +_F y \in \overline{\mathfrak{m}}$. The module structure follows from the definitions. □

Recall that if F_f is a Lubin-Tate formal group law, then $[\pi]_{F_f} = f$.

Definition 20.2. The π^n-torsion subgroup is

$$\begin{aligned} \mu_{f,n} &\coloneqq \{x \in \overline{\mathfrak{m}} \mid \pi^n \cdot_{F_f} x = 0\} \\ &= \{x \in \overline{\mathfrak{m}} \mid f_n(X) = f \circ f \circ \cdots \circ f(X) = 0\}. \end{aligned} \tag{20.2}$$

In fact, $\mu_{f,n}$ is an $\mathcal{O}_K$-submodule, and $\mu_{f,n} \subset \mu_{f,n+1}$ for all $n \geq 1$.

Example 20.3. Let $K = \mathbb{Q}_p$, and $f(X) = (X+1)^p - 1$. Then

$$[p^n]_{F_f}(X) = f \circ f \cdots \circ f(X) = (X+1)^{p^n} - 1. \tag{20.3}$$

Thus

$$\mu_{f,n} = \{\zeta_{p^n}^i - 1 \mid i = 0, 1, \dots, p^n - 1\} \tag{20.4}$$

Thus the $\mu_{f,n}$s seem to be our desired analogues for p-power roots of unity!

Now let $f(X) = \pi X + X^q$ be a Lubin-Tate series for π, and set $f_n = f \circ f_{n-1}(X) = f_{n-1}(X) \cdot (\pi + f_{n-1}(X)^{q-1})$. Then we can define the analogue of the cyclotomic polynomial as

$$h_n(X) = \frac{f_n(X)}{f_{n-1}(X)} = \pi + f_{n-1}(X)^{q-1} \tag{20.5}$$

Proposition 20.4. *$h_n(X)$ is a separable Eisenstein polynomial of degree $q^{n-1}(q-1)$.*

Proof. It is clear that $h_n(X)$ is monic as it is the quotient of monics, and has degree $q^n - q^{n-1} = q^{n-1}(q-1)$.

As $f(X) = X^q \mod \pi$, we have that $f_{n-1}(X)^{q-1} = X^{q^{n-1}q-1} \mod \pi$. Since $f_{n-1}(X)$ has 0 constant term, $h_n(X)$ has constant term π. Thus $h_n(X)$ is Eisenstein.

Since $h_n(X)$ is irreducible, it is separable if and only if $\operatorname{char} K = 0$, or $\operatorname{char} K = p$ and $h_n'(X) \neq 0$. Assume that $\operatorname{char} K = p$ and induct on n. Then $h_1(X) = \pi + X^{q-1}$ is separable. Suppose $h_1(X), \dots, h_{n-1}(X)$ is separable. Then $f_{n-1}(X) = X h_1(X) \cdots h_{n-1}(X)$ is separable as it is the product of separable irreducible polynomials of different degrees. Then $h_n(X) = \pi + f_{n-1}(X)^{q-1}$, so $h_n'(X) = (q-1) f_{n-1}'(X) f_{n-1}(X)^{q-2} \neq 0$, so $h_n(X)$ is separable. □

We need to understand the module structure on $\mu_{f,n}$.

Proposition 20.5.

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

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

Proof. (i): Fix a root α of $h_n(X)$. Since $h_n(X)$ is coprime to $f_{n-1}(X)$, $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$. Then the map

$$\begin{aligned} \tilde{\varphi} : \mathcal{O}_K &\to \mu_{f,n} \\ a &\mapsto a \cdot_{F_f} \alpha \end{aligned} \tag{20.6}$$

is an $\mathcal{O}_K$-module homomorphism. Since α is a π^n torsion point, $\ker \tilde{\varphi} \supset \pi^n \mathcal{O}_K$. Since $\alpha \notin \mu_{f,n-1}$, $\pi^{n-1} \cdot F_f \alpha \neq 0$, so $\pi^{n-1}\mathcal{O}_K \not\subset \ker \tilde{\varphi}$. Since $\ker \varphi$ is an ideal, this means that $\ker \tilde{\varphi} = \pi^n \mathcal{O}_K$. Thus $\tilde{\varphi}$ induces an injection

$$\varphi : \mathcal{O}_K/\pi^n\mathcal{O}_K \to \mu_{f,n}. \tag{20.7}$$

Since $f_n(X)$ is separable, $|\mu_{f,n}| \leq \deg f_n(X) \leq \deg f_n(X) = q^n = |\mathcal{O}_K/\pi^n\mathcal{O}_K|$, so φ is an isomorphism by the pigeon-hole principle.

(ii): Let $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(F_f, F_g)$ be an isomorphism of formal $\mathcal{O}_K$-modules. Then θ induces an isomorphism

$$\tilde{\theta} : (\overline{\mathfrak{m}}, +_{F_f}) \to (\overline{\mathfrak{m}}, +_{F_g}) \tag{20.8}$$

of $\mathcal{O}_K$-modules. This can be seen by a proof similar to that of Lemma 20.1. Hence $\mu_{f,n} \cong \mu_{g,n}$. Since $\mu_{f,n}$ is algebraic, $K(\mu_{f,n})/K$ is finite, hence complete, and as $\tilde{\theta}(X) \in \mathcal{O}_K[[X]]$, we have that for all $\alpha \in \mu_{f,n}$, $\tilde{\theta}(\alpha) \in K(\mu_{f,n})$. So $K(\mu_{g,n}) \subset K(\mu_{f,n})$. Reversing f and g gives $K(\mu_{f,n}) \subset K(\mu_{g,n})$ so we are done. □

Definition 20.6. Set $K_{\pi,n} = K(\mu_{f,n})$. The $K_{\pi,n}$ are *Lubin-Tate extensions.*

Remark 20.7.

1. $K_{\pi,n}$ do not depend on the choice of Lubin-Tate series by Proposition 20.5.
2. $K_{\pi,0} \subset K_{\pi,1} \subset \cdots$

Proposition 20.8. *$K_{\pi,n}/K$ are totally ramified and Galois of degree $q^{n-1}(q-1)$.*

Proof. We may pick a Lubin-Tate series $f(x) = \pi X + X^q$ for π. Then $K_{\pi,n}/K$ is Galois because it is the splitting field of $f_n(X)$. Let α be a root of $h_n(X) = f_n(X)/f_{n-1}(X)$. It suffices to show that $K(\alpha) = K(\mu_{f,n})$, since α is a root of an Eisenstein polynomial. Clearly $K(\alpha) \subset K(\mu_{f,n})$. By Proposition 20.5, if $x \in \mu_{f,n}$ then $x = a \cdot_{F_f} \alpha$ for some $a \in \mathcal{O}_K$. Then since $K(\alpha)$ is complete and $[a]_{F_f}(X) \in \mathcal{O}_K[[X]]$, we have that $x = [a]_{F_f}(\alpha) \in K(\alpha)$. Thus $K(\mu_{f,n}) \subset K(\alpha)$. □

Theorem 20.9. *There exists an isomorphism*

$$\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\cong} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times/U_k^{(n)} \tag{20.9}$$

characterized by

$$\psi_n(\sigma) \cdot_{F_f} x = \sigma(x) \tag{20.10}$$

for all $x \in \mu_{f,n}$, $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. ψ_n does not depend on f.

Proof. Let $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. Then σ preserves $\mu_{f,n}$ and acts continuously on $K_{\pi,n} = K(\mu_{f,n})$. Since $F_f(X,Y) \in \mathcal{O}_K[[X,Y]]$ and $[a]_{F_f} \in \mathcal{O}_K[[X]]$ for all $a \in \mathcal{O}_K$, we have by the continuity of σ that for all $x \in \mu_{f,n}, a \in \mathcal{O}_K$ that (look at the partial sums)

$$\begin{aligned} \sigma(x +_{F_f} y) &= \sigma(x) +_{F_f} \sigma(y) \\ \sigma(a \cdot_{F_f} x) &= a \cdot_{F_f} \sigma(x) \end{aligned} \tag{20.11}$$

Thus $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n})$, so we have a group homomorphism

$$\mathrm{Gal}(K_{\pi,n}/K) \to \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n}) \tag{20.12}$$

which is injective since $K_{\pi,n} = K(\mu_{f,n})$ so $\sigma = \mathrm{id}$ in $\mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n})$ if and only if $\sigma(x) = x$ for all $x \in \mu_{f,n}$, if and only if $\sigma = \mathrm{id}$ in $K_{\pi,n}$. Since $\mu_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$ as $\mathcal{O}_K$-modules, we have that

$$\mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n}) \cong \mathrm{Aut}_{\mathcal{O}_K/\pi^n\mathcal{O}_K}(\mu_{f,n}) = (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times. \tag{20.13}$$

This is true as for any ring R and any free R-module of rank 1 M, we have that $\mathrm{Aut}_R(M) = R^\times$. Thus we get a map ψ_n as described above. Since $[K_{\pi,n} : K] = q^n(q-1) = |(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times|$, ψ_n is an isomorphism since it is an injection.

Now let g be another Lubin-Tate series for π. Then repeating the construction as above, we get a map $\psi' : \mathrm{Gal}(K_{\pi,n}/K) \to (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$. Let $\theta : F_f \to F_g$ be an isomorphism of formal $\mathcal{O}_K$-modules. This induces an isomorphism $\theta : \mu_{f,n} \to \mu_{g,n}$ of $\mathcal{O}_K$-modules and hence for all $x \in \mu_{f,n}$ and all $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$ we have that

$$\theta(\psi_n(\sigma) \cdot_{F_f} x) = \psi_n(\sigma) \cdot_{F_g} \theta(x). \tag{20.14}$$

But $\theta \in \mathcal{O}_K[[X]]$ has coefficients in $\mathcal{O}_K$, so $\theta(\sigma(x)) = \sigma(\theta(x))$. Then

$$\begin{aligned}\theta(\psi_n(\sigma) \cdot_{F_f} x) &= \theta(\sigma(x)) \\ &= \sigma(\theta(x)) \\ &= \psi_n'(\sigma) \cdot_{F_g} \theta(x)\end{aligned} \tag{20.15}$$

Then $\psi_n(\sigma) \cdot_{F_g} \theta(x) = \psi_n'(\sigma) \cdot_{F_g} \theta(x)$ so $\psi_n(\sigma) = \psi_n'(\sigma)$. □

Now, set

$$K_{\pi,\infty} \coloneqq \bigcup_{n\geq 1} K_{\pi,n}. \tag{20.16}$$

The isomorphisms ψ_n are compatible with descending on n (so $\psi_n|_{\mathrm{Gal}(K_{\pi,n-1}/K)} = \psi_{n-1}$), so we an isomorphism

$$\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \cong \varprojlim (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times. \tag{20.17}$$

We conclude by showing that $K_{\pi,\infty}$ is analogous to $\mathbb{Q}_p(\zeta_{p^\infty})$ as totally ramified extensions.

Theorem 20.10 (Generalized local Kronecker-Weber theorem)**.** $K^{\mathrm{ab}} = K_{\pi,\infty}K^{\mathrm{un}}$

The proof of this result is long and difficult. We then have that

$$\begin{aligned}\mathrm{Art}_K : K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times &\to \mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(K^{\mathrm{un}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \\ \pi^n u \mapsto (n,u) &\mapsto (\mathrm{Frob}^n_{K^{\mathrm{un}}/K}, \psi^{-1}(u^{-1}))\end{aligned} \tag{20.18}$$

and the construction of this map is independent of the choice of π.

Part VIII
Non-examinable fun!

Will fill in when I am non-examining.

21 Upper numbering of ramification groups