Part III - Local Fields

Lectured by Rong Zhou

Artur Avameri

Michaelmas 2023

Contents

0 Introduction

This is a first class in graduate algebraic number theory. Something we'd like to do is solve diophantine equations, e.g. $f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$. In general, solving $f(x_1, \ldots, x_r) = 0$ is very difficult. A simpler question we might consider is solving $f(x_1, \ldots, x_r) \equiv 0 \pmod{p}$, or $\pmod{p^2}$, $\pmod{p^3}$, etc. Local fields package all of this information together.

1 Absolute values

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

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

(2) $|xy| = |x||y| \; \forall x, y \in K$.

(3) $|x + y| \leq |x| + |y| \; \forall x, y \in K$ (triangle inequality).

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

- Take $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with the usual absolute value $|a + ib| = \sqrt{a^2 + b^2}$. We call this $|\cdot|_\infty$.

- For K any field, we have the trivial absolute value $|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{else.} \end{cases}$

  We will ignore this in this course.

- Take $K = \mathbb{Q}$ and p a prime. For $0 \neq x \in \mathbb{Q}$, write $x = p^n \frac{a}{b}$ where $(a, p) = (b, p) = 1$. Then the p–**adic absolute value** is defined to be

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

  We can check the axioms:

  (1) The first axiom is clear.

  (2)
$$|xy|_p = \left| p^{n+m} \frac{ac}{bd} \right|_p = p^{-(n+m)} = |x|_p |y|_p.$$

  (3) WLOG let $m \geq n$. Then

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

Any absolute value $|\cdot|$ on K induces a metric $d(x,y)=|x-y|$ on K, hence induces a topology on K.

Definition 1.2. Suppose we have two absolute values $|\cdot|, |\cdot|'$ on K. We say these absolute values are **equivalent** if they induce the same topology. An equivalence class is called a **place**.

Proposition 1.1. Let $|\cdot|, |\cdot|'$ be (nontrivial) absolute values on K. Then the following are equivalent:

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

(ii) $|x|<1 \iff |x|'<1\ \forall x \in K$.

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

Proof. (i) $\implies$ (ii): $|x|<1 \iff x^n \to 0$ with respect to $|\cdot| \iff x^n \to 0$ with respect to $|\cdot|'$ (since the topologies are the same) $\iff |x|'<1$.

(ii) $\implies$ (iii): Note that $|x|^c = |x|' \iff c\log|x| = \log|x|'$. Take $a \in K^\times$ such that $|a|>1$. This exists since $|\cdot|$ is nontrivial. We need to show that $\forall x \in K^\times$,

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

Assume $\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}$. Choose $m,n \in \mathbb{Z}$ such that $\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}$. We then have

$$\begin{cases} n\log|x| < m\log|a| \\ n\log|x|' > m\log|a|' \end{cases}$$
$$\implies \left|\frac{x^n}{a^m}\right| < 1, \left|\frac{x^n}{a^m}\right|' > 1,$$

a contradiction. The other inequality is analogous.

(iii) $\implies$ (i): Clear, since they have the same open balls. □

Remark. $|\cdot|_\infty^2$ on $\mathbb{C}$ is not an absolute value by our definition (doesn't satisfy the triangle inequality). Some authors replace the triangle inquality by the condition $|x+y|^\beta \leq |x|^\beta + |y|^\beta$ for some fixed $\beta \in \mathbb{R}_{>0}$. The equivalence classes are the same in either case.

In this course, we will mainly be interested in the following:

Definition 1.3. An absolute value $|\cdot|$ on K is said to be **non-archimedean** if it satisfies the **ultrametric inequality**

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

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

Example 1.1.

- $|\cdot|_\infty$ on $\mathbb{R}$ is archimedean.
- $|\cdot|_p$ on $\mathbb{Q}$ is non–archimedean.

Lemma 1.2 (All triangles are isosceles)**.** Let $(K, |\cdot|)$ be non–archimedean and $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$.

Proof. On the one hand, $|x - y| \leq \max(|x|, |y|) = |y|$ (using $|x| = |-x|$).

On the other, $|y| \leq \max(|x|, |x - y|) = |x - y|$. □

Convergence is easier in non–archimedean fields:

Proposition 1.3. Let $(K, |\cdot|)$ be non–archimedean and $(x_n)_{n=1}^\infty$ a sequence on K. If $|x_n - x_{n+1}| \to 0$, then $(x_n)_{n=1}^\infty$ is Cauchy. In particular, if K is complete, then the sequence converges.

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

$$|x_n - x_m| = |(x_n - x_{n+1}) + (x_{n+1} - x_{n+2}) + \ldots + (x_{m-1} - x_m)| < \epsilon,$$

so (x_n) is Cauchy. □

Example 1.2. For $p = 5$, we can construct a sequence in $\mathbb{Q}$ satisfying:

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

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

We construct it by induction. Take $x_1 = 2$. Now suppose we've constructed x_n and write $x_n^2 + 1 = a \cdot 5^n$ and set $x_{n+1} = x_n + b \cdot 5^n$. We compute

$$x_{n+1}^2 + 1 = x_n^2 + 2bx_n5^n + b^25^{2n} + 1 = a5^n + 2bx_n5^n + \underbrace{b^25^{2n}}_{\equiv 0 \pmod{5^{n+1}}} + 1.$$

Hence we choose b such that $a + 2bx_n \equiv 0 \pmod 5$ and we're done.

Now (ii) tells us that (x_n) is Cauchy, but we claim it doesn't converge. Suppose it does, $x_n \to l \in \mathbb{Q}$. Then $x_n^2 \to l^2 \in \mathbb{Q}$. But by (i), $x_n^2 \to -1$, so $l^2 = -1$, a contradiction.

This tells us that $(\mathbb{Q}, |\cdot|_5)$ is not complete.

Definition 1.4. The p–adic numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

10 Oct 2022, Lecture 2

Let $(K, |\cdot|)$ be a non–archimedean valued field. For $x \in K$ and $r \in \mathbb{R}_{>0}$, we define $B(x, r) = \{y \in K \mid |y - x| < r\}$ and $\overline{B} = \{y \in K \mid |y - x| \leq r\}$ to be the open and closed balls of radius r.

Lemma 1.4. (i) If $z \in B(x,r)$, then $B(z,r) = B(x,r)$, i.e. open balls don't have centers.

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

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

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

Proof. (i) Let $y \in B(x,r)$. Then $|x-y| < r \implies |z-y| = |(z-x)+(x-y)| \leq \max(|z-x|,|x-y|) < r$, so $B(x,r) \subset B(z,r)$. The reverse inclusion is analogous.

(ii) Analogous to (i) by replacing $<$ with $\leq$.

(iii) Let $y \in K \setminus B(x,r)$. If $z \in B(x,r) \cap B(y,r)$, then $B(x,r) = B(z,r) = B(y,r)$ by (i), so $y \in B(x,r)$, a contradiction. Hence $B(x,r) \cap B(y,r) = \varnothing$. Since y was arbitrary, $K \setminus B(x,r)$ is open, so $B(x,r)$ is closed.

(iv) If $z \in \overline{B}(x,r)$, then $B(z,r) \subset \overline{B}(z,r) \overset{\text{(ii)}}{=} \overline{B}(x,r)$.

□

2 Valuation rings

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

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

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

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

Remark. We ignore the trivial evaluation $v(x) = 0 \,\forall x \in K$, which corresponds to the trivial absolute value.

Definition 2.2. We say valuations v_1, v_2 are equivalent if $\exists c \in \mathbb{R}_{>0}$ such that $v_1(x) = cv_2(x) \,\forall x \in K^\times$.

Example 2.1.

- If $K = \mathbb{Q}$, $v_p(x) = -\log_p |x|_p$ is the p–adic valuation.
- Let k be a field. Let $K = k(t) = \mathrm{Frac}(k[t])$ be a rational function field. We let
$$v\left(t^n \frac{f(t)}{g(t)}\right) = n$$
for $f, g \in k[t]$, $f(0) \neq 0, g(0) \neq 0$. This is called a t–adic valuation.

- Let $K = k((t)) = \mathrm{Frac}(k[[t]]) = \{\sum_{i=n}^{\infty} a_i t^i \mid a_i \in k, n \in \mathbb{Z}\}$, the field of formal Laurent series over k. We define
$$v\left(\sum_i a_i t^i\right) = \min\{i \mid a_i \neq 0\},$$
the t–adic valuation on K.

Definition 2.3. Let $(K, |\cdot|)$ be a non–archimedean valued field. The **valuation ring** of K is defined to be

$$\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}.$$

(i.e. the closed unit ball, $\mathcal{O}_K = \overline{B}(0,1)$, or $\mathcal{O}_K = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$).

Proposition 2.1. (i) $\mathcal{O}_K$ is an open subring of K.

(ii) The subsets $\{x \in K \mid |x| \leq r\}$ and $\{x \in K \mid |x| < r\}$ for $r \leq 1$ are open ideals in $\mathcal{O}_K$.

(iii) $\mathcal{O}_K^\times = \{x \in K \mid |x| = 1\}$.

Proof. (i) We find:

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

Thus $\mathcal{O}_K$ is a subring, and since $\mathcal{O}_K = \overline{B}(0,1)$, it is open.

(ii) As $r \leq 1$, $\{x \in K \mid |x| \leq r\} = \overline{B}(0,r) \subset \mathcal{O}_K$, so it is open. We find:

- If $x, y \in \overline{B}(0,r)$, then $|x+y| \leq \max(|x|, |y|) \leq r$, so $x + y \in \overline{B}_r$.
- If $x \in \mathcal{O}_K, y \in \overline{B}_r$, then $|xy| = |x||y| \leq 1 \cdot |y| \leq r$, so $xy \in \overline{B}_r$.

Hence this is an open ideal. The proof for $\{x \in K \mid |x| < r\}$ is analogous.

(iii) Note that $|x||x^{-1}| = |xx^{-1}| = 1$. Thus $|x| = 1 \iff |x^{-1}| = 1 \iff x, x^{-1} \in \mathcal{O}_K \iff x \in \mathcal{O}_K^\times$.

□

Notation. Let $\mathfrak{m} = \{x \in \mathcal{O}_K \mid |x| < 1\}$. It turns out this is a maximal ideal in $\mathcal{O}_K$. Also let $k = \mathcal{O}_K/\mathfrak{m}$, the residue field.

Corollary 2.2. $\mathcal{O}_K$ is a **local ring** (i.e. a ring with a unique maximal ideal) with unique maximal ideal $\mathfrak{m}$.

Proof. Let $\mathfrak{m}'$ be a maximal ideal. If $\mathfrak{m}' \neq \mathfrak{m}$, then $\exists x \in \mathfrak{m}' \setminus \mathfrak{m}$. Hence $|x| = 1$, so by (iii) above, x is a unit, so $\mathfrak{m}' = \mathcal{O}_K$, a contradiction. □

Example 2.2. $K = \mathbb{Q}$ with $|\cdot|_p$. Then $\mathcal{O}_K = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$. In this case, $\mathfrak{m} = p\mathbb{Z}_{(p)}$ and $k = \mathbb{F}_p$.

Definition 2.4. Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \cong \mathbb{Z}$, then we say v is a **discrete valuation**. In this case, K is said to be a **discretely valued field**.

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

Example 2.3.

- $K = \mathbb{Q}$ with the p–adic valuation and $K = k(t)$ with the t–adic valuation are discretely valued fields.
- $K = k(t)(t^{\frac{1}{2}}, t^{\frac{1}{4}}, t^{\frac{1}{8}}, \ldots)$ with the t–adic valuation is not a discretely valued field.

Remark. If v is a discrete valuation, we can scale v, i.e. replace it with an equivalent valuation such that $v(K^\times) = \mathbb{Z}$. Such v are called **normalized valuations**. Then π is a uniformizer $\iff$ $v(\pi) = 1$.

Lemma 2.3. Let v be a valuation on K. Then 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): $\mathcal{O}_K \subset K$, so $\mathcal{O}_K$ is an integral domain. Let $I \subset \mathcal{O}_K$ be a nonzero ideal and pick $x \in I$ such that $v(x) = \min\{v(a) \mid a \in I, a \neq 0\}$, which exists as v is discrete. Then we claim that $x\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq v(x)\}$ is equal to I. The inclusion $x\mathcal{O}_K \subset I$ is clear, as I is an ideal. For $x\mathcal{O}_K \supset I$, let $y \in I$, then $v(x^{-1}y) = v(y) - v(x) \geq 0 \implies y = x(x^{-1}y) \in x\mathcal{O}_K$.

(ii) $\implies$ (iii): Clear, as being a PID means every ideal is generated by one element, i.e. by finitely many.

(iii) $\implies$ (iv): Write $\mathfrak{m} = x_1\mathcal{O}_K + \ldots + x_n\mathcal{O}_K$ and WLOG assume $v(x_1) \leq v(x_2) \leq \ldots \leq v(x_n)$. Then $x_2, \ldots, x_n \in x_1\mathcal{O}_K$, since $x_1\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq v(x_1)\}$, so $\mathfrak{m} = x_1\mathcal{O}_K$.

(iv) $\implies$ (i): Let $\mathfrak{m} = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$ and let $c = v(\pi)$. Then if $v(x) > 0$, i.e. $x \in \mathfrak{m}$, then $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \varnothing$. Since $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, we have $v(K^\times) = c\mathbb{Z}$. □

12 Oct 2022, Lecture 3

Remark. Let v be a discrete valuation on K, $\pi \in \mathcal{O}_K$ a uniformizer. For $x \in K^\times$, let $n \in \mathbb{Z}$ such that $v(x) = nv(\pi)$. Then $u = x\pi^{-n} \in \mathcal{O}_K^\times$ and $x = u\pi^n$. In particular, $K = \mathcal{O}_K\left[\frac{1}{\pi}\right]$ and hence $K = \mathrm{Frac}(\mathcal{O}_K)$.

Definition 2.5. A ring R is called a **discrete valuation ring** (DVR) if it is a PID with exactly one nonzero prime ideal (which is then necessarily maximal).

Lemma 2.4. (i) Let v be a discrete valuation on K. Then $\mathcal{O}_K$ is a DVR.

(ii) Let R be a DVR. 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 the previous lemma, hence any nonzero prime ideal is maximal. Since $\mathcal{O}_K$ is a local ring, it is a DVR.

(ii) Let R be a DVR with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = (\pi)$ for $\pi \in R$. Since PIDs are UFDs, we can write any nonzero $x \in R$ uniquely as $\pi^n u$ for some $n \geq 0$, u a unit (since π is the only prime). Then any $y \in K^\times$ can be written uniquely as $\pi^m u$, $m \in \mathbb{Z}$. Define $v(\pi^m u) = m$. We can check that this is a valuation with $R = \mathcal{O}_K$.

□

Example 2.4. $\mathbb{Z}_{(p)}$, $R[[t]]$ for R a field are DVRs.

3 p–adic numbers

Recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. It is an exercise on example sheet 1 to show that $\mathbb{Q}_p$ is a field. Moreover, $|\cdot|_p$ extends to $\mathbb{Q}_p$ and the associated valuation is discrete (example sheet again).

Definition 3.1. The **ring of p–adic integers** $\mathbb{Z}_p$ is the valuation ring

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

Facts. $\mathbb{Z}_p$ is a DVR and has a principal maximal ideal $p\mathbb{Z}_p$. In $\mathbb{Z}_p$, all nonzero ideals are given by $p^n\mathbb{Z}_p$.

Proposition 3.1. $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. In particular, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$.

Proof. We need to show $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Note $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Since $\mathbb{Z}_p \subset \mathbb{Q}_p$ is open, $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$. But

$$\mathbb{Z}_p \cap \mathbb{Q} = \{x \in \mathbb{Q} \mid |x|_p \leq 1\} = \left\{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\right\} = \mathbb{Z}_{(p)}.$$

Thus it suffices to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. Let $\frac{a}{b} \in \mathbb{Z}_{(p)}$ with $a, b \in \mathbb{Z}$ and $p \nmid b$. For $n \in \mathbb{N}$, choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \pmod{p^n}$. Then $y_n \to \frac{a}{b}$ as $n \to \infty$.

For the last part, note that $\mathbb{Z}_p$ is complete (as it is a closed subset of a complete space) and $\mathbb{Z} \subset \mathbb{Z}_p$ is dense. □

Inverse limits. Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings together with homomorphisms $\phi_n : A_{n+1} \to A_n$ (called **transition maps**). Then the **inverse limit** of $(A_n)_{n=1}^{\infty}$ is the set/group/ring

$$\varprojlim_n A_n = \left\{ (a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} A_n \mid \phi_n(a_{n+1}) = a_n \ \forall n \right\}.$$

Fact. If A_n is a group/ring, then the inverse limit is also a group/ring. Here the group/ring operations are defined componentwise. Let $\theta_m : \varprojlim_n A_n \to A_m$ denote the natural projection.

The inverse limit satisfies the following universal property:

Proposition 3.2. For any set/group/ring B together with homomorphisms $\psi_n : B \to A_n$ such that the following diagram commutes,

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

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

Proof. Define $\psi : B \to \prod_{n=1}^{\infty} A_n$ by $b \mapsto (\psi_n(b))_{n=1}^{\infty}$. Then $\psi_n = \theta_n \circ \psi_{n+1} \implies \psi(b) \in \varprojlim_n A_n$. This map is clearly unique (determined by $\psi_n = \phi_n \circ \psi_{n+1}$), and is a homomorphism of sets/groups/rings. □

Definition 3.2. Let $I \subset R$ be an ideal (in a ring R). The I–**adic completion of** R is the ring $\hat{R} = \varprojlim_n R/I^n$ where $R/I^{n+1} \to R/I^n$ is the natural projection.

Note that there exists a natural map $i : R \to \hat{R}$ by the universal property (since there exist maps $R \to R/I^n$).

Definition 3.3. We say R is I–**adically complete** if i is an isomorphism.

Fact. $\ker(i : R \to \hat{R}) = \bigcap_{n=1}^{\infty} I^n$ (check!).

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

Proposition 3.3. Assume K is complete with respect to $|\cdot|$. Then:

(i) $\mathcal{O}_K \overset{i}{\cong} \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ (i.e. $\mathcal{O}_K$ is π–adically complete)[1].

(ii) Every $x \in \mathcal{O}_K$ can be written uniquely as $x = \sum_{i=0}^{\infty} a_i \pi^i$ with $a_i \in A$, where $A \subset \mathcal{O}_K$ is a set of coset representatives for $\mathcal{O}_K/\pi\mathcal{O}_K$. Moreover, any such power series converges (in $\mathcal{O}_K$).

Proof. (i) K is complete and $\mathcal{O}_K \subset K$ is closed, so $\mathcal{O}_K$ is complete. If $x \in \bigcap_{n=1}^{\infty} \pi^n\mathcal{O}_K$, then $v(x) \geq nv(\pi)\ \forall n \implies x = 0$, hence the natural map $\mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ is injective.

For surjectivity, let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ and for each n, let $y_n \in \mathcal{O}_K$ be a lifting[2] of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$. Then $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$, thus $(y_n)_{n=1}^{\infty}$ is a Cauchy sequence in $\mathcal{O}_K$. Let $y_n \to y \in \mathcal{O}_K$. Then y maps to $(x_n)_{n=1}^{\infty}$ in $\varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$.

(ii) Left as exercise on example sheet 1.

□

Corollary 3.4. (i) $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

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

14 Oct 2022, Lecture 4

Proof. (i) By the previous proposition we just need to show $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$. Let $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map. Then

$$\ker(f_n) = \{x \in \mathbb{Z} \mid |x|_p \leq p^{-n}\} = p^n\mathbb{Z},$$

thus the natural map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is injective.

For surjectivity, take $\overline{z} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ and $c \in \mathbb{Z}_p$ a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there exists $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$ ($p^n\mathbb{Z}_p$ is open in $\mathbb{Z}_p$). Then $f_n(x) = \overline{z}$, so $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective.

(ii) Follows from Corollary 3.4 (ii) applied to $p^{-n}x \in \mathbb{Z}_p$ for some $n \in \mathbb{Z}$.

□

Example 3.1. We have $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \ldots$ in $\mathbb{Q}_p$.

[1] There a bit of abuse of notation here – really, $\mathcal{O}_K$ is (π)–adically complete.

[2] Given a surjective map $G \to G'$, a lift of an element $x \in G'$ is a choice of $y \in G$ such that $y \mapsto x$ under this map.

4 Complete valued fields

4.1 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 $\exists a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$ for $f'(a)$ the formal derivative. 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 $r = v(f'(a))$ for v a normalized valuation, i.e. $v(\pi) = 1$. We inductively construct a sequence (x_n) in $\mathcal{O}_K$ such that

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

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

Take $x_1 = a$, so $f(x_1) \equiv 0 \pmod{\pi^{1+2r}}$. Now suppose we've constructed $x_1, \ldots, x_n$ satisfying the conditions. Then define $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$. Since $x_n \equiv x_1 \pmod{\pi^{r+1}}$, $v(f'(x_n)) = v(f'(x_1)) = r$ and hence $\frac{f(x_n)}{f'(x_n)} \equiv 0 \pmod{\pi^{n+r}}$ by (i). It follows that $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$, so (ii) holds.

Note that for X, Y indeterminates, we can write $f(X+Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \ldots$, where $f_i \in \mathcal{O}_K[X]$ and $f_0(X) = f(X), f_1(X) = f'(X)$. Thus $f(x_{n+1}) = f(x_n) + f'(x_n)c + f_2(x_n)c^2 + \ldots$ for $c = -\frac{f(x_n)}{f'(x_n)}$. Since $c \equiv 0 \pmod{\pi^{n+r}}$ and $v(f_i(x_n)) \geq 0$, we have $f(x_{n+1}) \equiv f(x_n) + cf'(x_n) \pmod{\pi^{n+2r+1}}$ (since the other terms vanish), but this is $\equiv 0 \pmod{\pi^{n+2r+1}}$, so (i) holds.

This gives the construction of (x_n). Property (ii) implies that (x_n) is Cauchy, so let $x \in \mathcal{O}_K$ be the limit, $x_n \to x$. Then $f(x) = \lim_{n\to\infty} f(x_n) = 0$ by property (i). Moreover, (ii) implies $a = x_1 \equiv x_n \pmod{\pi^{r+1}}$ $\forall n$, so $a \equiv x \pmod{\pi^{r+1}}$, thus $|x - a| < |f'(a)|$.

For uniqueness, suppose x' also satisfies $f(x') = 0$ and $|x' - a| < |f'(a)|$. Set $\delta = x' - x \neq 0$. Then $|x' - a| < |f'(a)|$ and $|x - a| < |f'(a)|$, so the ultrametric inequality implies $|\delta| = |x' - x| < |f'(a)| = |f'(x)|$ (since $a \equiv x \pmod{\pi^{r+1}}$). But

$$0 = f(x') = f(x+\delta) = \underbrace{f(x)}_{=0} + f'(x)\delta + \underbrace{\delta^2 \ldots}_{|\cdot| \leq |\delta|^2}.$$

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

Corollary 4.2. Let $(K, |\cdot|)$ be a complete discretely valued field, let $f(x) \in \mathcal{O}_K[x]$ and let $\overline{c} \in k = \mathcal{O}_K/\mathfrak{m}$ be a simple root of $\overline{f}(x) = f(x) \pmod{\mathfrak{m}} \in k[x]$. Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $x \equiv \overline{c} \pmod{\mathfrak{m}}$.

Proof. Apply Hensel's lemma to a lift $c \in \mathcal{O}_K$ of $\bar{c}$. Then $|f(c)| < 1 = |f'(c)|^2$ since $f'(c)$ is a simple root. □

Example 4.1. Consider $f(x) = x^2 - 2$, which has a simple root mod 7. Thus $\sqrt{2} \in \mathbb{Z}_7 \subset \mathbb{Q}_7$.

Corollary 4.3. $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 \text{ if } p > 2. \\ (\mathbb{Z}/2\mathbb{Z})^3 \text{ if } p = 2. \end{cases}$

Proof. First consider $p > 2$. Let $b \in \mathbb{Z}_p^\times$. Applying the previous corollary 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 $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ has kernel $(\mathbb{Z}_p^\times)^2$, so induces an isomorphism $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})$ (since $\mathbb{F}_p^\times = \mathbb{Z}/(p-1)\mathbb{Z}$).

We have an isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \to \mathbb{Q}_p^\times$ given by $(u, n) \mapsto up^n$. Then $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$.

If $p = 2$, let $b \in \mathbb{Z}_2^\times$. Consider $f(x) = x^2 - b$, so $f'(x) = 2x \equiv 0 \pmod 2$. Instead now let $b \equiv 1 \pmod 8$. Then $|f(1)|_2 \leq 2^{-3} < 2^{-2} = |f'(1)|_2^2$. Hensel's lemma now implies that $b \in (\mathbb{Z}_2^\times)^2 \iff b \equiv 1 \pmod 8$. Thus $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^2$. Again using $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$, we obtain that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. □

Remark. The proof of Hensel's lemma uses the iteration $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$. We can think of the proof as the non–archimedean analogue of the Newton-Raphson method.

Theorem 4.4 (Hensel's lemma, version 2)**.** Let $(K, |\cdot|)$ be a complete discretely valued field and $f(x) \in \mathcal{O}_K[x]$. Suppose $\overline{f}(x) = f(x) \pmod{\mathfrak{m}} \in k[x]$ factorizes as $\overline{f}(x) = \overline{g}(x)\overline{h}(x) \in k[x]$ with $\overline{g}(x), \overline{h}(x)$ coprime. Then there is a factorization $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$ with $\overline{g}(x) \equiv g(x) \pmod{\mathfrak{m}}$, $\overline{f}(x) \equiv f(x) \pmod{\mathfrak{m}}$ and $\deg(\overline{g}) = \deg(g)$.

Proof. Left as an exercise on example sheet 1. □

17 Oct 2022, Lecture 5

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

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

$$\overline{f}(x) = x^r(a_r + \ldots a_n x^{n-r}) \pmod{\mathfrak{m}}.$$

By Hensel's lemma version 2, $f(x) = g(x)h(x)$ with $\deg(g) = r$, contradicting irreducibility. □

5 Teichmüller lifts

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

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

Remark. Since char $R = p$, $(x+y)^p = x^p + y^p$, so the Frobenius map is a ring homomorphism.

Example 5.1. (i) $\mathbb{F}_{p^n}$ is perfect and $\overline{\mathbb{F}_p}$ is perfect.

(ii) Non–example. $\mathbb{F}_p[t]$ is not perfect since $t \notin \mathrm{Im}(\mathrm{Frob})$.

(iii) $\mathbb{F}_p(t^{\frac{1}{p^\infty}}) = \mathbb{F}_p\left(t, t^{\frac{1}{p}}, t^{\frac{1}{p^2}}, \dots\right)$ is a perfect field, known as the **perfection** of $\mathbb{F}_p(t)$.

Fact. A field k of characteristic $p > 0$ is perfect if and only if any finite extension of k is separable.

Theorem 5.1. Let $(K, |\cdot|)$ be a complete discretely valued field such that the residue field $k = \mathcal{O}_K/\mathfrak{m}$ is a perfect field of characteristic $p > 0$. Then there exists a unique map $[] : k \to \mathcal{O}_K$ such that

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

(ii) $[ab] = [a][b]\ \forall a, b \in k$.

Moreover, if char $\mathcal{O}_K = p$, then $[]$ is a ring homomorphism (i.e. it also preserves addition).

Definition 5.2. The element $[a] \in \mathcal{O}_K$ is called the **Teichmüller lift** of a.

Lemma 5.2. Let $(K, |\cdot|)$ be a complete discretely valued field[3] and fix $\pi \in \mathcal{O}_K$ a uniformizer. Let $x, y \in \mathcal{O}_K$ be such that $x \equiv y \pmod{\pi^k}$ for $k \geq 1$. Then $x^p \equiv y^p \pmod{\pi^{k+1}}$.

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

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

Since char $\mathcal{O}_K/\pi\mathcal{O}_K = p$, we have $p \in \pi\mathcal{O}_K$. Thus $\binom{p}{i} y^{p-i}(u\pi^k)^i \in \pi^{k+1}\mathcal{O}_K\ \forall i \geq 1$, so $x^p \equiv y^p \pmod{\pi^{k+1}}$. □

[3] (do we need the residue field to be perfect here? lectures said let $(K, |\cdot|)$ be as in above theorem).

Proof of Theorem 5.1. Let $a \in k$. For each $i > 0$, we choose a lift $y_i \in \mathcal{O}_K$ of $a^{\frac{1}{p^i}}$ and define $x_i = y_i^{p^i}$. We claim that (x_i) is a Cauchy sequence and its limit $x_i \to x$ is independent of the choice of y_i.

By construction, $y_i \equiv y_{i+1}^p \pmod{\pi}$. By our previous lemma and induction on k, we have that $y_i^{p^k} \equiv y_{i+1}^{p^{k+1}} \pmod{\pi^{k+1}}$ and hence $x_i \equiv x_{i+1} \pmod{\pi^{i+1}}$ (by taking $k = i$) and hence (x_i) is Cauchy, so $x_i \to x \in \mathcal{O}_K$.

Suppose (x_i') arises from another choice of y_i' lifting $a_i^{\frac{1}{p^i}}$. Then (x_i') is Cauchy and $x_i' \to x'$. Let

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

Then x_i'' arises from the lifting $y'' = \begin{cases} y_i & i \text{ even.} \\ y_i' & i \text{ odd.} \end{cases}$. Then x_i'' is Cauchy with subsequences converging to both x and x', so $x = x'$, so our limit is independent of the choice of liftings (y_i). We define $[a] = x$. Then $x_i \equiv y_i^{p^i} \equiv \left(a^{\frac{1}{p^i}}\right)^{p^i} \equiv a$ $\pmod{\pi}$, so $x \equiv a \pmod{\pi}$, giving us the first property.

Now let $b \in k$ and choose $u_i \in \mathcal{O}_K$ a lift of $b^{\frac{1}{p^i}}$ and let $z_i = u_i^{p^i}$. Then $[b] = \lim_{i\to\infty} z_i$. Now $u_i y_i$ is a lift of $(ab)^{\frac{1}{p^i}}$, hence

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

giving us the second property.

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

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

Finally, it is easy to check that $[0] = 0$ and $[1] = 1$ (take $y_i = 0$ and $y_i = 1$). So [] is a ring homomorphism.

For uniqueness, let $\phi : K \to \mathcal{O}_K$ be another map of the desired form. Then for $a \in k$, $\phi\left(a^{\frac{1}{p^i}}\right)$ is a lift of $a^{\frac{1}{p^i}}$. It follows that

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

□

Example 5.2. For $K = \mathbb{Q}_p$, what does $[] : \mathbb{F}_p \to \mathbb{Z}_p$ look like? Take $a \in \mathbb{F}_p^\times$, so $[a]^{p-1} = [a^{p-1}] = [1] = 1$. Hence $[a]$ is a $(p-1)^{\text{th}}$ root of unity.

More generally:

Lemma 5.3. Let $(K, |\cdot|)$ be a complete discretely valued field. If $k = \mathcal{O}_K/\mathfrak{m} \subset \overline{\mathbb{F}_p}$ (which implies that k is perfect), then $[a] \in \mathcal{O}_K$ is a root of unity $\forall a \in k^\times$.

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

Theorem 5.4. Let $(K, |\cdot|)$ be a complete discretely valued field of characteristic $p > 0$. Assume $k = \mathcal{O}_K/\mathfrak{m}$ is perfect. Then $K \cong k((t))$.

Proof. Since $K = \mathrm{Frac}(\mathcal{O}_K)$, it suffices to show that $\mathcal{O}_K \cong k[[t]]$. For this, fix $\pi \in \mathcal{O}_K$ a uniformizer and let $[] : k \to \mathcal{O}_K$ be the Teichmüller map. Define $\phi : k[[t]] \to \mathcal{O}_K$ by $\phi\left(\sum_{i=0}^{\infty} a_i t^i\right) = \sum_{i=0}^{\infty} a_i \pi^i$. Then ϕ is a ring homomorphism since $[]$ is a ring homomorphism, but it is also a bijection by Proposition 3.3. □

6 Extensions of complete valued fields

19 Oct 2022, Lecture 6

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

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

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

Recall. If L/K is a finite extension, then $N_{L/K} : L \to K$ is defined by $N_{L/K}(y) = \det_K(\mathrm{mult}(y))$ where $\mathrm{mult}(y) : L \to L$ is the K–linear map given by multiplication by y.

Facts:

- The norm is multiplicative, i.e. $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.
- Let $X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$ be the minimal polynomial of $y \in L$. Then $N_{L/K}(y) = \pm a_0^m$ for some $m \geq 1$. In particular, $N_{L/K}(x) = 0 \iff x = 0$.

Definition 6.1. Let $(K, |\cdot|)$ be a nonarchimedean valued field and V a vector spce over K. Then a **norm** on V is a function $||\cdot|| : V \to \mathbb{R}_{\geq 0}$ satisfying

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

Example 6.1. If V is finite–dimensional and $e_1, \ldots, e_n$ is a basis for V, then the **sup norm** $||\cdot||_{\sup}$ on V is defined by $||x||_{\sup} = \max_i |x_i|$, where $x = \sum_{i=1}^{n} x_i e_i$.

Exercise: $||\cdot||_{\text{sup}}$ is a norm.

Definition 6.2. Two norms $||\cdot||_1, ||\cdot||_2$ on V are **equivalent** if there exist constants $C, D \in \mathbb{R}_{>0}$ such that

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

Fact. A norm defines a topology on V and equivalent norms induce the same topology (since an open ball in one topology is both contained in and contains an open ball in the other topology).

Proposition 6.2. Let $(K, |\cdot|)$ be complete and nonarchimedean and let V be a finite dimensional vector space over K. Then V is complete with respect to $||\cdot||_{\text{sup}}$.

Proof. Let (v_i) be a Cauchy sequence in V and let $e_1, \dots, e_n$ be a basis for V. Write $V_i = \sum_{j=1}^n x_j^i e_j$, then $(x_j^i)_{i=1}^\infty$ is a Cauchy sequence in K. Let $x_j^i \to x_j \in K$, then we can check that $v_i \to v = \sum_{j=1}^n x_j e_j$. □

Theorem 6.3. Let $(K, |\cdot|)$ be complete and nonarchimedean and let V be a finite dimensional vector space over K. Then any two norms on V are equivalent. In particular, V is complete with respect to any norm.

Proof. Since equivalence defines an equivalence relation on the set of norms, it suffices to show that any norm $||\cdot||$ is equivalent to the sup norm $||\cdot||_{\text{sup}}$ with respect to some basis. Let $e_1, \dots, e_n$ be a basis for V.

For the upper bound, set $D = \max ||e_i||$. Then if $x = \sum_{i=1}^n x_i e_i$, then $||x|| = \max_i ||x_i e_i|| = \max_i |x_i| ||e_i|| \leq D \max_i |x_i| = D||x||_{\text{sup}}$.

To find C such that $C||\cdot||_{\text{sup}} \leq ||\cdot||$, we induct on $n = \dim V$. If $n = 1$, then $||x|| = ||x_1 e_1|| = |x_1| ||e_1|| = ||x||_{\text{sup}} ||e_1||$, so take $C = ||e_1||$.

For $n > 1$, set $V_i = \langle e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n \rangle$. By induction, the norm on V_i is equivalent to the sup norm, so V_i is complete with respect to $||\cdot||$, hence closed. Then the translate $e_i + V_i$ is also closed for all i, hence

$$S = \bigcup_{i=1}^n e_i + V_i$$

is a closed subset not containing zero. Hence $\exists C > 0$ such that $S \cap B(0, C) = \varnothing$, where $B(0, c) = \{x \in V \mid ||x|| < C\}$. We claim this C works. To see this, let $0 \neq x = \sum_{i=1}^n x_i e_i$ and suppose $|x_j| = \max_i |x_i|$. Then $||x||_{\text{sup}} = |x_j|$ and $\frac{1}{x_j} x \in S$ (since the j^{th} coefficient will be equal to 1). Thus $||\frac{1}{x_j} x|| \geq C$, so $||x|| \geq C|x_j| = C||x||_{\text{sup}}$.

Finally, V is complete since it is complete with respect to $||\cdot||_{\text{sup}}$. □

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

(i) $|y|_L = 0 \iff |N_{L/K}(y)|^{1/n} = 0 \iff N_{L/K}(y) = 0 \iff y = 0$.

(ii) $|y_1y_2|_L = |N_{L/K}(y_1y_2)|^{1/n} = |N_{L/K}(y_1)|^{1/n}|N_{L/K}(y_2)|^{1/n} = |y_1|_L|y_2|_L$.

(iii) For this, we need some preparation:

Definition 6.3. Let $R \subset S$ be a subring. We say $s \in S$ is **integral** over R if s is a root of a monic polynomial with coefficients in R, i.e. monic $f \in R[X]$ such that $f(s) = 0$.

The **integral closure** $R^{\mathrm{int}(S)}$ of R in S is the set of elements of S that are integral over R, i.e.

$$R \subset R^{\mathrm{int}(S)} = \{s \in S \mid s \text{ is integral over } R\}.$$

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

Proposition 6.4. $R^{\mathrm{int}(S)}$ is a subring of S. Moreover, $R^{\mathrm{int}(S)}$ is integrally closed in S.

Proof. Exercise on example sheet 2. □

Lemma 6.5. Let $(K, |\cdot|)$ be a nonarchimedean valued field. Then $\mathcal{O}_K$ is integrally closed in K.

Proof. Let $x \in K$ be integral over $\mathcal{O}_K$. WLOG assume $x \neq 0$. Let $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathcal{O}_K[X]$ such that $f(x) = 0$. Then

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

If $|x| > 1$, then we have that $\left|-a_{n-1} - \ldots - a_0 \frac{1}{x^{n-1}}\right| \leq 1$ by the ultrametric inequality, contradiction. Thus $|x| \leq 1$, so $x \in \mathcal{O}_K$. □

Now we show (iii): Set $\mathcal{O}_L = \{y \in L \mid |y|_L \leq 1\}$. We claim that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ inside L. In particular, $\mathcal{O}_L$ is a subring of L.

Assuming this, let $x, y \in L$ and WLOG assume $|x|_L \leq |y|_L$. Then we he $\left|\frac{x}{y}\right|_L \leq 1 \implies \frac{x}{y} \in \mathcal{O}_L$. Since $\mathcal{O}_L$ is a ring, $1 \in \mathcal{O}_L$, so $1 + \frac{x}{y} \in \mathcal{O}_L$ and hence $\left|1 + \frac{x}{y}\right|_L \leq 1$, so $|x+y|_L \leq |y|_L = \max(|x|_L, |y|_L)$, giving the ultrametric inequality property.

21 Oct 2022, Lecture 7

To prove the claim, take $0 \neq y \in L$ and let $f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0 \in K[X]$ be the minimal monic polynomial for y. We claim y is integral over $\mathcal{O}_K \iff f(X) \in \mathcal{O}_K[X]$.

($\Longleftarrow$): This direction is clear.

($\Longrightarrow$): Let $g(x) \in \mathcal{O}_K[X]$ be monic such that $g(y) = 0$. Then $f \mid g$ in $K[X]$ and hence every root of f is a root of g. Hence every root of f considered in $\overline{K}$ is integral over $\mathcal{O}_K$. Hence the a_i are integral over $\mathcal{O}_K$ for $0 \leq i \leq d-1$. Hence $a_i \in \mathcal{O}_K$ by a lemma from last time.

By the corollary of the second version of Hensel's lemma, $|a_i| \leq \max(|a_0|, 1)$. By a property of the norm $N_{L/K}$, we have $N_{L/K}(y) = \pm a_0^m \in \mathcal{O}_K$. Hence $y \in \mathcal{O}_L \iff |N_{L/K}(y)| \leq 1 \iff |a_0| \leq 1$, so by our corollary this happens $\iff |a_i| \leq 1\ \forall i$, i.e. $a_i \in \mathcal{O}_K\ \forall i$, so y is integral.

Since $N_{L/K}(x) = x^n$ for $x \in K$, $|x|_L$ extends $|\cdot|$ on K. If $|\cdot|_L'$ is another absolute value on L extending $|\cdot|$, then $|\cdot|_L, |\cdot|_L'$ are norms on L, which are equivalent and hence induce the same topology on L, so $|\cdot|_L' = |\cdot|_L^c$ for some $c > 0$. But since they both extend $|\cdot|$ on K, we must have $c = 1$.

(ii): Theorem 6.3 implies the result, as L is complete with respect to the sup norm. □

Corollary 6.6. Let $(K, |\cdot|)$ be a complete, nonarchimedean discretely valued field and L/K a finite extension. 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) Fix v, the valuation on K responding to our absolute value, and let v_L be the valuation on L extending v. Let $n = [L : K]$. For $y \in L^\times$, $|y|_L = |N_{L/K}(y)|^{1/n}$, so $v_L(y) = \frac{1}{n}v(N_{L/K}(y))$, so $v_L(L^\times) \subset \frac{1}{n}v(K^\times)$. Since $v(K^\times)$ is discrete, so is v_L.

(ii) This was proved in the proof of the previous theorem.

□

Corollary 6.7. Let $(K, |\cdot|)$ be complete, nonarchimedean, and discretely valued and let $\overline{K}/K$ be the algebraic closure of K. Then $|\cdot|$ extends uniquely to an absolute value $|\cdot|_{\overline{K}}$ on $\overline{K}$.

Proof. Let $x \in \overline{K}$, then $x \in L$ for some finite extension L/K. Define $|\cdot|_{\overline{K}} = |x|_L$. This is well–defined (i.e. independent of L) by uniqueness in Theorem 6.1 (for any L, L', consider an extension containing both).

The axioms for $|x|_{\overline{K}}$ to be an absolute value can be checked over finite extensions.

Uniqueness again follows from the finite case: if two absolute values disagree on some value, then consider a finite extension containing that value. □

Remark. $|\cdot|_{\overline{K}}$ on $\overline{K}$ is never discrete. For example, if $K = \mathbb{Q}_p$, then $\sqrt[n]{p} \in \overline{\mathbb{Q}_p}$ and $\forall n \geq 0$, $v_p(\sqrt[n]{p}) = \frac{1}{n} v_p(n) = \frac{1}{n}$, giving a non–discrete valuation. Furthermore, $\overline{\mathbb{Q}_p}$ is not complete with respect to $|\cdot|_{\overline{\mathbb{Q}_p}}$. Showing this is an exercise on example sheet 2. On the sheet we also show that if we take $\mathbb{C}_p$, the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_{\overline{\mathbb{Q}_p}}$, then $\mathbb{C}_p$ is algebraically closed.

Proposition 6.8. Let L/K is a finite extension of complete discretely valued fields with $n = [L : K]$. Assume that

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

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

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

Remark. We will later see that (i) implies (ii).

Proof. We'll choose $\alpha \in \mathcal{O}_L$ such that:

(i) $\exists \beta \in \mathcal{O}_K[\alpha]$ a uniformizer for $\mathcal{O}_L$.

(ii) $\mathcal{O}_K[\alpha] \to k_L$ is surjective.

First note that k_L/k is separable, so $\exists \overline{\alpha} \in k$ such that $k_L = k(\overline{\alpha})$. Let $\alpha \in \mathcal{O}_L$ be a lift of $\overline{\alpha}$ and $g(X) \in \mathcal{O}_K[X]$ a monic lift of the minimal polynomial of $\overline{\alpha}$. Also fix $\pi_L \in \mathcal{O}_L$ a uniformizer. Then $\overline{g}(X) \in k[X]$ is irreducible and separable, so $\overline{\alpha}$ is a simple root of $\overline{g}$, so $g(\alpha) \equiv 0 \pmod{\pi_L}$ and $g'(\alpha) \not\equiv 0 \pmod{\pi_L}$.

If $g(\alpha) \equiv 0 \pmod{\pi_L^2}$, then

$$g(\alpha + \pi_L) \equiv g(\alpha) + \pi_L g'(\alpha) \pmod{\pi_L^2}.$$

Thus $v_L(g(\alpha + \pi_L)) = v_L(\pi_L g'(\alpha)) = v_L(\pi) = 1$ for v_L the normalized valuation on L. Hence either $v_L(g(\alpha)) = 1$ or $v_L(\gamma(\alpha + \pi_L)) = 1$. Possibly replacing α by $\alpha + \pi_L$, we may assume that $g(\alpha)$ is a uniformizer, i.e. $v_L(g(\alpha)) = 1$.

Now set $\beta = g(\alpha) \in \mathcal{O}_K[\alpha]$, a uniformizer. Then $\mathcal{O}_K[\alpha] \subset L$ is the image of a continuous map $\mathcal{O}_K^n \to L$ given by $(x_0, \ldots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_i \alpha^i$. Since $\mathcal{O}_K$ is compact, $\mathcal{O}_K[\alpha]$ is compact, hence closed.

We have a closed subring of $\mathcal{O}_L$, so to show it is $\mathcal{O}_L$, it is enough to show it is dense. Since $k_L = k(\overline{\alpha})$, $\mathcal{O}_K[\alpha]$ contains a set of coset representatives for the residue field $k_L = \mathcal{O}_L/\beta\mathcal{O}_L$. Take $y \in \mathcal{O}_L$. By Proposition 3.3, we can write $y = \sum_{i=0}^{\infty} \lambda_i \beta^i$ with $\lambda_i \in \mathcal{O}_K[\alpha]$. Then $y_m = \sum_{i=0}^{m} \lambda_i \beta^i \in \mathcal{O}_K[\alpha]$ gives a Cauchy sequence converging to y. Then $y \in \mathcal{O}_K[\alpha]$ since $\mathcal{O}_K[\alpha]$ is closed. □

7 Local fields

Definition 7.1. Let $(K, |\cdot|)$ be a valued field. We say K is a **local field** if it is complete and locally compact (i.e. every point contains a compact neighborhood).

Example 7.1. $\mathbb{R}$ and $\mathbb{C}$ are local fields.

Proposition 7.1. Let $(K, |\cdot|)$ be a nonarchimedean complete valued field. Then the following are equivalent:

(i) K is locally compact (so K is a nonarchimedean local field).

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

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

24 Oct 2022, Lecture 8

Proof. (i) $\implies$ (ii): Let $\mathcal{U} \ni 0$ be a compact neighborhood of 0 (i.e. $0 \in \mathcal{U} \subset K$ for U open, K compact). Then $\exists x \in \mathcal{O}_K$ such that $x\mathcal{O}_K \subset \mathcal{U}$. Since $x\mathcal{O}_K$ is closed, it is compact, so $\mathcal{O}_K$ is compact (as it is homeomorphic to $x\mathcal{O}_K$ by the homeomorphism $x\mathcal{O}_K \overset{\times x^{-1}}{\to} \mathcal{O}_K$).

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

(ii) $\implies$ (iii): Let $x \in \mathfrak{m}$ and let $A_x \subset \mathcal{O}_K$ be the set of coset representatives for $\mathcal{O}_K/x\mathcal{O}_K$. Then $\mathcal{O}_K = \bigcup_{y \in A_x}(y + x\mathcal{O}_K)$, which is a disjoint open cover. By compactness, A_x is finite. Hence $\mathcal{O}_K/x\mathcal{O}_K$ is finite and so $\mathcal{O}_K/\mathfrak{m}$ is finite. Now suppose v is not discrete. Then let $x = x_1, x_2, x_3, \ldots$ be elements such that $v(x_1) > v(x_2) > \ldots > 0$. Then $x\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq x_3\mathcal{O}_K \subsetneq \ldots \subsetneq \mathcal{O}_K$. But $\mathcal{O}_K/x\mathcal{O}_K$ is finite, so it can only have finitely many subgroups, a contradiction.

(iii) $\implies$ (ii): Since $\mathcal{O}_K$ is a metric space, it suffices to show that $\mathcal{O}_K$ is sequentially compact, i.e. that every sequence has a convergent subsequence. Let (x_n) be a sequence in $\mathcal{O}_K$ and fix $\pi \in \mathcal{O}_K$ a uniformizer. Note that $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong k$, so $\mathcal{O}_K/\pi^i\mathcal{O}_K$ is finite $\forall i$ (as $\mathcal{O}_K \supset \pi\mathcal{O}_K \supset \ldots \supset \pi^i\mathcal{O}_K$ are all finite). Since $\mathcal{O}_K/\pi\mathcal{O}_K$ is finite, $\exists a_1 \in \mathcal{O}_K/\pi\mathcal{O}_K$ and a subsequence $(x_{1,n})_{n=1}^{\infty}$ such that $x_{1,n} \equiv a_1 \pmod{\pi}$. Since $\mathcal{O}_K/\pi^2\mathcal{O}_K$ is finite, $\exists a_2 \in \mathcal{O}_K/\pi^2\mathcal{O}_K$ and a subsequence $(x_{2,n})_{n=1}^{\infty}$ of $(x_{1,n})$ such that $x_{2,n} \equiv a_2 \pmod{\pi^2}$. Continuing in this fashion, we obtain sequences $(x_{i,n})_{n=1}^{\infty}$ for $i = 1, 2, 3, \ldots$ such that

(i) $(x_{i+1,n})$ is a subsequence of $(x_{i,n})$ for all i.

(ii) For any i, $\exists a_i \in \mathcal{O}_K/\pi^i\mathcal{O}_K$ such that $x_{i,n} \equiv a_i \pmod{\pi^i}$ for all n.

Then $a_i \equiv a_{i+1} \pmod{\pi^i}$. Now choose $y_i = x_{i,i}$. This defines a subsequence of (x_n) with $y_i \equiv a_i \equiv a_{i+1} \equiv y_{i+1} \pmod{\pi^i}$. Thus (y_i) is Cauchy, hence converges by completeness. □

Example 7.2. (i) $\mathbb{Q}_p$ is a local field, as it is discretely valued and has finite residue field $\mathbb{F}_p$.

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

More on inverse limits: Again let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings and let $\phi_n : A_{n+1} \to A_n$ be homomorphisms (transition maps).

Definition 7.2. Assume each A_n is finite. Then the **profinite topology** on $A = \varprojlim_n A_n$ is the weakest topology on A such that the projection maps $\theta_n : A \to A_n$ are continuous for all n, where all A_n are equipped with the discrete topology.

Fact. $A = \varprojlim_n A_n$ with the profinite topology is compact, totally disconnected and Hausdorff.

Proposition 7.2. Let K be a nonarchimedean local field. Under the isomorphism $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ (for $\pi \in \mathcal{O}_K$ a uniformizer), the topology on $\mathcal{O}_K$ coincides with the profinite topology.

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

For the topology arising from $|\cdot|$, this is clear (for any open ball, we can find a closed ball of smaller radius contained inside it).

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 $\forall a \in \mathcal{O}_K$. □

Lemma 7.3. Let K be a nonarchimedean local field and L/K a finite extension. Then L is a local field.

Proof. Theorem 6.1 shows that L is complete and discretely valued, so it suffices to show that $k_L = \mathcal{O}_L/\mathfrak{m}_L$ is finite. Let $\alpha_1, \dots, \alpha_n \in L$ be a basis for L as a K–vector space. Then $||\cdot||_{\text{sup}}$, the sup norm, is equivalent to $|\cdot|_L$, so there exists $r > 0$ such that $\mathcal{O}_L \subset \{x \in L \mid ||x||_{\text{sup}} \leq r\}$. Then take $a \in K$ such that $|a| \geq r$, then $\mathcal{O}_L \subset \bigoplus_{i=1}^n a\alpha_i\mathcal{O}_K \subset L$. But this is a finitely generated module over a PID, hence noetherian, so $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$–module, so k_L is finitely generated over k. □

Definition 7.3. A nonarchimedean valued field $(K, |\cdot|)$ has **equal characteristic** if $\text{char}(K) = \text{char}(k)$. Otherwise, K has **mixed characteristic**.

Example 7.3. $\mathbb{Q}_p$ has mixed characteristic, whereas $\mathbb{F}_p((t))$ has equal characteristic $p > 0$.

It turns out equal characteristic local fields are very easy to classify:

Theorem 7.4. Let K be a nonarchimedean local field of equal characteristic $p > 0$.[4] Then

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

for some $n \geq 1$.

Proof. K is complete and discretely valued with $\mathrm{char}(K) > 0$. Moreover, k is finite, so $k \cong \mathbb{F}_{p^n}$ for some n, so k is perfect. Now by Theorem 5.4, $K \cong \mathbb{F}_{p^n}((t))$. □

Lemma 7.5. An absolute value $|\cdot|$ on a field K is nonarchimedean $\iff$ $|n|$ is bounded $\forall n \in \mathbb{Z}$.

Proof. ($\implies$): Since $|-1| = |1|$, $|-n| = |n|$. Thus it suffices to show that $|n|$ is bounded for $n \geq 1$, but $|n| = |1| + \ldots |1| \leq |1| = 1$ by the ultrametric inequality.

($\impliedby$): Suppose $|n| \leq B$ $\forall n \in \mathbb{Z}$. Take $x, y \in K$ with $|x| \leq |y|$. Then we have

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

Take n^{th} roots to get $|x+y| \leq |y| \sqrt[n]{B(m+1)} \overset{n\to\infty}{\to} |y| = \max(|x|, |y|)$. □

26 Oct 2022, Lecture 9

Theorem 7.6 (Ostrowski's Theorem)**.** Any nontrivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or the p–adic absolute value $|\cdot|_p$ for some prime p.

Proof. Case 1: $|\cdot|$ is archimedean. Then fix $b > 1$ such that $|b| > 1$, where such a b exists by the previous lemma. Take $a > 1$ another integer and write b^n in base a, i.e. $b^n = c_m a^m + c_{m-1} a^{m-1} + \ldots + c_0$ for $0 \leq c_i < a$ and $c_m \neq 0$.

Let $B = \max_{0 \leq c < a}(|c|)$, then $|b^n| \leq (m+1) B \max(|a|^m, 1)$. Hence

$$\begin{aligned} |b| &= \underbrace{[(n \log_a b + 1)B]^{1/n}}_{\to 1 \text{ as } n \to \infty} \max(|a|^{\log_a(b)}, 1) \\ &\implies |b| \leq \max(|a|^{\log_a(b)}, 1). \end{aligned}$$

[4] Note the residue field of an an equal characteristic nonarchimedean local field is finite, so the characteristic must be positive.

Then $|a| > 1$ and $|b| \leq |a|^{\log_a(b)}$ (†). Switching the roles of a and b we also find $|a| \leq |b|^{\log_b(a)}$ (‡). Then (†) and (‡) imply $\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} = \lambda \in \mathbb{R}_{>0}$. Hence $|a| = a^\lambda$ $\forall a \in \mathbb{Z}_{\geq 1}$, so $|x| = |x|_\infty^\lambda$ $\forall x \in \mathbb{Q}$, so $|\cdot|$ is equivalent to $|\cdot|_\infty$.

Case 2: $|\cdot|$ is non–archimedean. As in the previous inequality, we have $|n| \leq 1$ $\forall n \in \mathbb{Z}$. Since this absolute value is nontrivial, $\exists n \in \mathbb{Z}_{\geq 1}$ such that $|n| < 1$. Write $n = p_1^{e_1} \dots p_r^{e_r}$. Then $|p| < 1$ for some $p \in \{p_1, \dots, p_r\}$. Now suppose $|q| < 1$ for some prime $q \neq p$. Then write $1 = rp + sq$ for some $r, s \in \mathbb{Z}$. Then $1 = |rp + sq| \leq \max(|rp|, |sq|) < 1$, a contradiction. Thus $|p| = \alpha < 1$ and $|q| = 1$ for all primes $q \neq p$. Hence $|\cdot|$ is equivalent to $|\cdot|_p$. □

Theorem 7.7. Let $(K, |\cdot|)$ be a nonarchimedean local field of mixed characteristic. Then K is a finite extension of $\mathbb{Q}_p$.

Proof. K has mixed characteristic $\implies \mathrm{char}(K) = 0 \implies \mathbb{Q} \subset K$. Also, K is nonarchimedean $\implies |\cdot||_{\mathbb{Q}} \sim |\cdot|_p$ for some p. Since K is complete, $\mathbb{Q}_p \subset K$. Hence it suffices to show that $\mathcal{O}_K$ is finite as a $\mathbb{Z}_p$–module.

Let $\pi \in \mathcal{O}_K$ be a uniformizer and v a normalized valuation on K. Set $v(p) = e$. Then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\pi^e\mathcal{O}_K$, which is finite (since $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong k$ is finite). $\mathbb{F}_p = \mathbb{Z}_p/\mathbb{Z}_p \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K$, so $\mathcal{O}_K/p\mathcal{O}_K$ is a finite–dimensional vector space over $\mathbb{F}_p$. Let $x_1, \dots, x_n \in \mathcal{O}_K$ be coset representatives for the $\mathbb{F}_p$–basis of $\mathcal{O}_K/p\mathcal{O}_K$. Then

$$\left\{ \sum_{i=1}^n a_j x_j \mid a_j \in \{0, \dots, p-1\} \right\}$$

gives a set of coset representatives for $\mathcal{O}_K/p\mathcal{O}_K$.

Now apply Proposition 3.3 (ii) to write (for $a_{ij} \in \{0, \dots, p-1\}$)

$$y = \sum_{i=0}^\infty \left(\sum_{j=1}^n a_{ij} x_j \right) p^i = \sum_{j=1}^n \underbrace{\left(\sum_{i=0}^\infty a_{ij} p^i \right)}_{\in \mathbb{Z}_p} x_j.$$

Hence $\mathcal{O}_K$ is finite over $\mathbb{Z}_p$. □

On example sheet 2, we show that if K is a complete archimedean field, then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.

In summary, if K is a local field, then either:

(i) K is archimedean, so $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.

(ii) K is nonarchimedean of equal characteristic, so $K \cong \mathbb{F}_{p^n}((t))$.

(iii) K is nonarchimedean of mixed characteristic, so K is a finite extension of $\mathbb{Q}_p$.

8 Global fields

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

(i) an algebraic number field.

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

Lemma 8.1. Let $(K, |\cdot|)$ be a complete discretely valued field and L/K 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 $|\sigma(x)|_L = |x|_L$.

Proof. Since $x \mapsto |\sigma(x)|_L$ is an absolute value on L (as we can check) extending $|\cdot|_K$, our result follows from uniqueness of extensions of absolute values. □

Lemma 8.2 (Krasner's lemma)**.** Let $(K, |\cdot|)$ be discretely valued and let $f(X) \in K[X]$ be a separable irreducible polynomial with roots $\alpha_1, \ldots, \alpha_n \in \overline{K}$, the separable closure of K. Suppose $\beta \in \overline{K}$ is such that

$$|\beta - \alpha_1| < |\beta - \alpha_i| \ \forall 2 \leq i \leq n.$$

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

Proof. Let $L = K(\beta)$ and $L' = L(\alpha_1, \ldots, \alpha_n)$. Then L'/L is a Galois extension. Let $\sigma \in \mathrm{Gal}(L'/L)$. We have $|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - a_1|$ by the previous lemma and hence $\sigma(\alpha_1) = \alpha_1$, so $\alpha_1 \in K(\beta)$. □

Proposition 8.3. Let $(K, |\cdot|)$ be a complete discretely valued field and let $f(X) = \sum_{i=0}^n a_i X^i \in \mathcal{O}_K[X]$ be a separable irreducible monic polynomial. Let $\alpha \in \overline{K}$ be a root of f. Then $\exists \epsilon > 0$ such that for any other polynomial $g(x) = \sum_{i=0}^n b_i X^i \in \mathcal{O}_K[X]$ monic with $|a_i - b_i| < \epsilon \ \forall i$, there exists a root β of $g(x)$ such that $K(\alpha) = K(\beta)$.

Informally, ”nearby” polynomials define the same extension.

Proof. Let $\alpha = \alpha_1, \alpha_2, \ldots, a_n \in \overline{K}$ be the roots of f, which are distinct. Then $f'(\alpha_1) \neq 0$. We choose ϵ such that $|g(\alpha_1)| < |f'(\alpha_1)|^2$ and $|f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha_1)|$. Then $|g(\alpha_1)| < |f'(\alpha_1)^2| = |g'(\alpha_1)^2|$ (as all triangles are isosceles). By Hensel's lemma applied to the field $K(\alpha_1)$, there exists $\beta \in K(\alpha_1)$ such that $g(\beta) = 0$ and $|\beta - \alpha_1| < |g'(\alpha_1)|$. But $|g'(\alpha_1)| = |f'(\alpha_1)| = \prod_{i=2}^n |\alpha_1 - \alpha_i| \leq |\alpha_1 - \alpha_i|$ for $2 \leq i \leq n$ (using $|\alpha_1 - \alpha_i| \leq 1$ since α_i is integral as f is monic). Since $|\beta - \alpha_1| < |\alpha_1 - \alpha_i| = |\beta - \alpha_i|$ (again by isosceles condition), Krasner's lemma tells us that $\alpha \in K(\beta)$ and so $K(\alpha) = K(\beta)$. □

29 Oct 2022, Lecture 10

Theorem 8.4. Let K be a local field. Then K is the completion of a global field.

Proof. Case 1: $|\cdot|$ is archimedean. Then $\mathbb{R}, \mathbb{C}$ are the completions of $\mathbb{Q}, \mathbb{Q}(i)$, respectively, with respect to $|\cdot|_\infty$.

Case 2: $|\cdot|$ is non–archimedean and of equal characteristic. Then $K \cong \mathbb{F}_p((t))$, and so K is the completion of $\mathbb{F}_p(t)$ with respect to the t–adic absolute value.

Case 3: $|\cdot|$ is non–archimedean and of mixed characteristic. Then $K = \mathbb{Q}_p(\alpha)$ for α a root of a monic irreducible polynomial $f(X) \in \mathbb{Z}_p[X]$ (primitive element theorem). Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we choose $g(X) \in \mathbb{Z}[X]$ as in Proposition 8.3. Then $K = \mathbb{Q}_p(\beta)$ for β a root of $g(X)$. Since $\mathbb{Q}(\beta)$ is dense in $\mathbb{Q}_p(\beta) = K$, K is the completion of $\mathbb{Q}(\beta)$. □

9 Dedekind domains

Definition 9.1. A Dedekind domain is a ring R such that

(i) R is a Noetherian integral domain.

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

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

Example 9.1. The ring of integers in a number field is a Dedekind domain (we will show this later). This is the prototypical example. Also, any PID (hence DVR) is a Dedekind domain.

Theorem 9.1. *A ring is a DVR $\iff$ R is a Dedekind domain with exactly one nonzero prime ideal.*

We start with two lemmas.

Lemma 9.2. *Let R be a Noetherian ring and $I \subset R$ a nonzero ideal. Then there exist nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset I$.*

Proof. Suppose not. Since R is Noetherian, we can choose I maximal with this property. Then I is not prime, so $\exists x, y \in R \backslash I$ such that $xy \in I$. Let $I_1 = I + (x)$ and $I_2 = I + (y)$. Then by the maximality of I, $\exists \mathfrak{p}_1, \dots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset I_1$ and $\mathfrak{q}_1 \dots \mathfrak{q}_s \subset I_2$, so $\mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \subset I_1 I_2 \subset I$, a contradiction. □

Lemma 9.3. *Let R be an integral domain which is integrally closed in $K = \mathrm{Frac}(R)$. Let $0 \neq I \subset R$ be finitely generated and let $x \in K$. If $xI \subset I$, then $x \in R$.*

Proof. Let $I = (c_1, \dots, c_n)$. We write $xc_i = \sum_{j=1}^n a_{ij} c_j$ for $a_{ij} \in R$. Let $A = (a_{ij})$ be the matrix given by the a_{ij} and set $B = xI - A \in M_{n \times n}(K)$. Let

Adj(B) be the adjugate matrix for B. Then $B\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix} = 0$ in K^n, so multiplying by the adjugate gives $\det(B)I\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix} = 0 \implies \det(B) = 0$. But $\det(B)$ is just a monic polynomial in x with coefficients in R. Thus x is integral over R, so $x \in R$ as R is integrally closed. □

Proof of Theorem 9.1. ($\implies$): This is clear, as any PID, so any DVR, is a Dedekind domain.

($\impliedby$): We need to show that R is a PID. The assumption implies that R is a local ring with unique maximal ideal $\mathfrak{m}$.

Step 1: $\mathfrak{m}$ is principal. Let $0 \neq x \in \mathfrak{m}$. By Lemma 9.2, $(x) \supset \mathfrak{m}^n$ for some $n \geq 1$. Let n be minimal such that $(x) \supset \mathfrak{m}^n$. Then we may choose $y \in \mathfrak{m}^{n-1} \setminus (x)$. Set $\pi = \frac{x}{y}$. Then we have $y\mathfrak{m} \subset \mathfrak{m}^n \subset (x) \implies p^{-1}\mathfrak{m} \subset R$. If π is a proper ideal and not the whole ring, then $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$, so $\pi^{-1} \in R$ by Lemma 9.3. Thus $y \in (x)$, a contradiction. Hence $\pi^{-1}\mathfrak{m} = R \implies \mathfrak{m} = \pi R$ is principal.

Step 2: R is a PID. Let $I \subset R$ be a nonzero ideal. Consider the sequence of fractional ideals $I \subset \pi^{-1}I \subset \pi^{-2}I \subset \ldots$ in K. Since $\pi^{-1} \notin R$, we have $\pi^{-k}I \neq \pi^{-k+1}I$ $\forall k$ by Lemma 9.3. Since R is Noetherian, we may choose n maximal such that $\pi^{-n}I \subset R$. If $\pi^{-n}I \subset \mathfrak{m} = (\pi)$, then $\pi^{-(n+1)}I \subset R$, contradicting the maximality of R. Hence $\pi^{-n}I = R \implies I = \pi^n R$. □

Definition 9.2. Let R be an integral domain and let $S \subset R$ be a multiplicatively closed subset (i.e. $1 \in S$ and $x, y \in S \implies xy \in S$). The **localization** $S^{-1}R$ of R with respect to S is the ring

$$S^{-1}R = \left\{\frac{r}{s} \mid r \in R, s \in S\right\} \subset \mathrm{Frac}(R).$$

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

Example 9.2.

- If $\mathfrak{p} = 0$, then $R_{(\mathfrak{p})} = \mathrm{Frac}(R)$.
- If $R = \mathbb{Z}$, then $\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, (b, p) = 1\right\}$ (as seen before as a valuation ring).

Fact. R Noetherian $\implies$ $S^{-1}R$ Noetherian.

Fact. There exists a bijection between

$$\begin{aligned}\{\text{prime ideals in } S^{-1}R\} \leftrightarrow & \{\text{prime ideals } \mathfrak{p} \text{ in } R \text{ with } \mathfrak{p} \cap S = \varnothing\}. \\ \mathfrak{p}S^{-1}R \hookleftarrow & \ \mathfrak{p}.\end{aligned}$$

Corollary 9.4. Let R be a Dedekind domain and $\mathfrak{p} \subset R$ a nonzero prime ideal. Then $R_{(\mathfrak{p})}$ is a DVR. [5]

Proof. By properties of localization, $R_{(\mathfrak{p})}$ is a Noetherian integral domain with a unique nonzero prime ideal $\mathfrak{p}R_{(\mathfrak{p})}$. It suffices to show that $R_{(\mathfrak{p})}$ is integrally closed in $\mathrm{Frac}(R_{(\mathfrak{p})}) = \mathrm{Frac}(R)$, since then the localization of $\mathfrak{p}$ is a Dedekind domain by Theorem 9.1.

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

$$sx^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

where $a_i \in R, s \in S$. Multiply this by s^{-1} to get that xs is integral over R and hence $xs \in R$, thus $x \in R_{(\mathfrak{p})}$. □

31 Oct 2022, Lecture 11

Definition 9.3. 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 $R_{(\mathfrak{p})}$.

Example 9.3. If $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$, then v_p is the p–adic valuation.

Theorem 9.5. Let R be a Dedekind domain. Then every nonzero prime ideal R can be written uniquely as a product of prime ideals.

Remark. This is clear for PIDs (as PID $\implies$ UFD).

Sketch of proof. We quote the following properties of localization:

(i) $I = J \iff IR_{(\mathfrak{p})} = JR_{(\mathfrak{p})}$ $\forall \mathfrak{p}$ prime ideals (and $I, J \subset R$ ideals).

(ii) If R is a Dedekind domain and $\mathfrak{p}_1, \mathfrak{p}_2$ are nonzero prime ideals, then $\mathfrak{p}_1 R_{(\mathfrak{p}_2)} = \begin{cases} R_{(\mathfrak{p}_2)} & \mathfrak{p}_1 \neq \mathfrak{p}_2. \\ \mathfrak{p}_2 R_{(\mathfrak{p}_2)} & \mathfrak{p}_1 = \mathfrak{p}_2. \end{cases}$

Let $I \subset R$ be a nonzero ideal. Then by Lemma 9.2 there exist distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1^{\beta_1} \ldots \mathfrak{p}_r^{\beta_r} \subset I$, where $\beta_i > 0$. Let $0 \neq \mathfrak{p}$ be a prime ideal, $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Then by (ii), $\mathfrak{p}_i R_{(\mathfrak{p})} = R_{(\mathfrak{p})}$ and hence $IR_{(\mathfrak{p})} = IR_{(\mathfrak{p})}$.

By Corollary 9.4, $IR_{(\mathfrak{p}_i)} = (\mathfrak{p}_i R_{(\mathfrak{p}_i)})^{\alpha_i} = \mathfrak{p}_i^{\alpha_i} R_{(\mathfrak{p}_i)}$ for some $0 \leq \alpha_i \leq \beta_i$. Thus $I = \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_r^{\alpha_r}$ by (i).

[5] This is the correct way to think about Dedekind domains.

For uniqueness, if $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r} = \mathfrak{p}_1^{\gamma_1} \dots \mathfrak{p}_r^{\gamma_r}$, then $\mathfrak{p}_i^{\alpha_i} R_{(p_i)} = \mathfrak{p}_i^{\gamma_i} R_{(\mathfrak{p}_i)} \implies \alpha_i = \gamma_i$ by unique factorization in DVRs. □

10 Dedekind domains and extensions

Let L/K be a finite extension. For $x \in L$, we write $\mathrm{Tr}_{L/K}(x)$ for the trace of the K–linear map $L \to L$ mapping $y \mapsto xy$. If L/K is separable of degree n and $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ are the set of embeddings of L into an algebraic closure $\overline{K}$ of K, then $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x) \in K$.

Lemma 10.1. Let L/K be a finite separable extension of fields. Then the symmetric bilinear pairing $(\cdot,\cdot) : L \times L \to K$ by $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is non–degenerate.

Proof. L/K is separable, so $L = K(\alpha)$ for some $\alpha \in L$. Consider the matrix A for $(\cdot,\cdot)$ in the K–basis for L given by $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. Then $A_{ij} = \mathrm{Tr}_{L/K}(\alpha^{i+j}) = [BB^T]_{ij}$ for $B = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \dots & \sigma_n(\alpha) \\ \vdots & & & \\ \sigma_1(\alpha^{n-1}) & \sigma_2(\alpha^{n-1}) & \dots & \sigma_n(\alpha^{n-1}) \end{pmatrix}$. Then $\det A = (\det B)^2$, but $\det B = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))$, the Vandermonde determinant. Hence $\det A$ is nonzero since $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$ by separabalility. □

The converse is also true and is left as an exercise on example sheet 3: A finite extension 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 the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L is a Dedekind domain.

Proof. $\mathcal{O}_L$ is the subring of L, so $\mathcal{O}_L$ is an integral domain. Hence we need to show:

(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.

We prove:

(i) Let $e_1, \dots, e_n \in L$ be a K–basis for L. Upon scaling by K, we may assume $e_i \in \mathcal{O}_L\ \forall i$. Let $f_i \in L$ be the dual basis with respect to the trace form $(\cdot,\cdot)$. Let $x \in \mathcal{O}_L$ and write $x = \sum_{i=1}^n \lambda_i f_i$ for $\lambda_i \in K$. Then

$\lambda_i = \mathrm{Tr}_{L/K}(xe_i) \in \mathcal{O}_K$. Hence for any $z \in \mathcal{O}_L$, $\mathrm{Tr}_{L/K}(z)$ is a sum of elements in $\overline{K}$ which are integral over $\mathcal{O}_K \implies \mathrm{Tr}_{L/K}(z) \in K$ is integral over $\mathcal{O}_K$, so $\mathrm{Tr}_{L/K}(z) \in \mathcal{O}_K$. Thus $\mathcal{O}_L \subset \mathcal{O}_K f_1 + \ldots + \mathcal{O}_K f_n$. Since $\mathcal{O}_K$ is Noetherian, $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$–module, hence $\mathcal{O}_L$ is Noetherian.

(ii) Left as an exercise on example sheet 2.

(iii) Let P be a nonzero prime ideal in $\mathcal{O}_L$ and define $\mathfrak{p} = P \cap \mathcal{O}_K$, a prime ideal of $\mathcal{O}_K$. Let $0 \neq x \in P$, then x satisfies the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_0$, where $a_i \in \mathcal{O}_K$ and $a_0 \neq 0$. Then $0 \neq a_0 \in \mathcal{O}_K \cap P = \mathfrak{p}$, so $\mathfrak{p}$ is nonzero and hence maximal.

We have an injection $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/P$ and $\mathcal{O}_L/P$ is a finite–dimensional vector space over $\mathcal{O}_K/\mathfrak{p}$. Since $\mathcal{O}_L/P$ is an integral domain, it is a field (e.g. by applying rank–nullity to the multiplication map $y \mapsto zy$). Hence P is maximal.

□

Remark. This theorem holds even without the assumption that L/K is separable.

Corollary 10.3. The ring of algebraic integers in a number field is a Dedekind domain.

Convention. For $\mathcal{O}_K$ the ring of integers of a number field and $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero prime ideal, we normalize $|\cdot|_\mathfrak{p}$ (the absolute value associated to $v_\mathfrak{p}$) by $|x|_\mathfrak{p} = N_\mathfrak{p}^{-v_\mathfrak{p}(x)}$ for $N_\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|$. 02 Nov 2022, Lecture 12

Let us fix $\mathcal{O}_K$ to be a Dedekind domain with fraction field $K = \mathrm{Frac}(\mathcal{O}_K)$. Let L/K be a finite separable extension and $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ inside L (which is a Dedekind domain by Theorem 10.2).

Lemma 10.4. Let $0 \neq x \in \mathcal{O}_K$. Then

$$(x) = \prod_{p \neq 0 \text{ prime}} p^{v_p(x)}.$$

Proof. $x\mathcal{O}_{K,(p)} = (p\mathcal{O}_{K,(p)})^{v_p(x)}$ by definition of $v_p(x)$. In particular, $\{p \neq 0 \mid v_p(x) \neq 0\}$ is finite. Then the lemma follows from properties of localization stated last time: $I = J \iff I\mathcal{O}_{K,(p)} = J\mathcal{O}_{K,(p)}$ $\forall$ prime ideals p. □

Notation. $\mathcal{P} \subset \mathcal{O}_L$ and $\mathfrak{p} \subset \mathcal{O}_K$ will always denote prime ideals. We write $\mathcal{P} \mid \mathfrak{p}$ if $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \ldots \mathcal{P}_r^{e_r}$ and $\mathcal{P} \in \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$ for $e_i > 0$ and $\mathcal{P}_i$ distinct prime ideals.

Theorem 10.5. Let $\mathcal{O}_K, \mathcal{O}_L, K, L$ be as above. For $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}_K$, write $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$. Then the absolute values on L extending $|\cdot|_{\mathfrak{p}}$ (up to equivalence) are precisely $|\cdot|_{\mathcal{P}_1}, \dots, |\cdot|_{\mathcal{P}_r}$.

Proof. By Lemma 10.4, for any $0 \neq x \in \mathcal{O}_K$ and $1 \leq i \leq r$, we have $v_{\mathcal{P}_i}(x) = e_i v_{\mathfrak{p}}(x)$. Hence up to equivalence, $|\cdot|_{\mathcal{P}_i}$ does extend $|\cdot|_{\mathfrak{p}}$.

Conversely, suppose $|\cdot|$ is an absolute value on L which extends $|\cdot|_{\mathfrak{p}}$. Then $|\cdot|_{\mathfrak{p}}$ is bounded on $\mathbb{Z}$ and hence $|\cdot|$ is non–archimedean. Now let

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

be the valuation for L with respect to $|\cdot|$. Then $\mathcal{O}_K \subset R$ and since R is integrally closed in L (by Lemma 6.5), we have $\mathcal{O}_L \subset R$. Set $\mathcal{P} = \{x \in \mathcal{O}_L \mid |x| < 1\} = \mathfrak{m}_R \cap \mathcal{O}_L$. Then $\mathcal{P}$ is a prime ideal in R and it is nonzero as it contains $\mathfrak{p}$. Then $\mathcal{O}_{L,(\mathcal{P})} \subset R$ because $s \in \mathcal{O}_L \setminus \mathcal{P} \implies |s| = 1$. But $\mathcal{O}_{L,(\mathcal{P})}$ is a DVR, hence a maximal subring of $L \implies \mathcal{O}_{L,(\mathcal{P})} = R$. Hence $|\cdot|$ is equivalent to $|\cdot|_{\mathcal{P}}$. Since $|\cdot|$ extends to $|\cdot|_{\mathfrak{p}}$, $\mathcal{P} \cap \mathcal{O}_K = \mathfrak{p}$, so $\mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r} \subset \mathcal{P} \implies \mathcal{P} = \mathcal{P}_i$ for some i. □

Let K be a number field. If $\sigma : K \twoheadrightarrow \mathbb{R}, \mathbb{C}$ is a real or complex embedding, then $x \mapsto |\sigma(x)|_\infty$ defines an absolute value on K, denoted by $|\cdot|_\sigma$. (This is on example sheet 2).

Corollary 10.6. 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 $\mathfrak{p} \subset \mathcal{O}_K$.

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

Proof. Case 1: $|\cdot|$ is non–archimedean. Then $|\cdot|_{\mathbb{Q}}$ is equivalent to $|\cdot|_p$ for some prime p by Ostrowski's theorem (Theorem 7.6). Then by Theorem 10.5, $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}}$ for some $\mathfrak{p} \mid p$ a prime ideal in $\mathcal{O}_K$.

Case 2: $|\cdot|$ is archimedean. This is an exercise on example sheet 2. □

10.1 Completions

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

Lemma 10.7. (i) The natural map $\Pi_p : L \otimes_K K_{\mathfrak{p}} \to L_{\mathcal{P}}$ is surjective.

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

Proof. Let $M = \mathrm{Im}(\Pi_p) = LK_{\mathfrak{P}} \subset L_{\mathcal{P}}$. Write $L = K(\alpha)$, so $M = K_{\mathfrak{p}}(\alpha)$. Hence M is a finite extension of $K_{\mathfrak{p}}$ and $[M : K_{\mathfrak{p}}] \leq [L : K]$. Moreover, M is complete (by Theorem 6.1) and $L \subset M \subset L_{\mathcal{P}}$, hence $M = L_{\mathcal{P}}$, so both results follow. □

Lemma 10.8 (CRT for commutative rings)**.** Let R be a ring and $I_1, \dots, I_n \subset R$ be ideals such that $I_i + I_j = R \ \forall i \neq j$ (i.e. the ideals are pairwise coprime). Then:

(i) $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$ (call this product I).

(ii) $R/I \cong \prod_{i=1}^n (R/I_i)$.

Proof. Exercise on example sheet 2. □

Theorem 10.9. The natural map $L \otimes_K K_{\mathfrak{p}} \to \prod_{\mathcal{P}|\mathfrak{p}} L_{\mathcal{P}}$ is an isomorphism.

Proof. Write $L = K(\alpha)$ and let $f(X) \in K[X]$ be the minimal polynomial of α. Then we have $f(X) = f_1(X) \dots f_r(X)$ in $K_{\mathfrak{p}}[X]$ for $f_i(X) \in K_{\mathfrak{p}}[X]$ distinct and irreducible (also separable). Since $L = K[X]/f(X)$,

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

Set $L_i = K_{\mathfrak{p}}[X]/f_i(X)$, a finite extension of K. Then L_i contains both L and $K_{\mathfrak{p}}$ (using the fact that $K[X]/f(X) \to K_{\mathfrak{p}}[X]/f_i(X)$ is injective, since it is a morphism of fields). Moreover, L is dense inside L_i (since we can approximate coefficients of $K_{\mathfrak{p}}[X]/f_i(X)$ with an element $K[X]/f(X)$ and all norms on this finite–dimensional vector space are equivalent). The theorem now follows from the following three claims:

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

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

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

To prove these:

(i) Since $[L_i : K_{\mathfrak{p}}] < \infty$, there is a unique absolute value $| \cdot |$ on L_i extending $| \cdot |_{\mathfrak{p}}$ on $K_{\mathfrak{p}}$. Then Theorem 10.5 implies that $| \cdot ||_L$ is equivalent to $| \cdot |_{\mathcal{P}}$ for some $\mathcal{P} \mid \mathfrak{p}$. Since L is dense in L_i and L_i is complete, we must have $L = L_{\mathcal{P}}$.

(ii) Suppose $\phi : L_i \to L_j$ is an isomorphism preserving L and $K_{\mathfrak{p}}$. Then $\phi : K_{\mathfrak{p}}[X]/f_i(X) \to K_{\mathfrak{p}}[X]/f_j(X)$ takes X to X and hence $f_i(X) = f_j(X) \implies i = j$.

(iii) By Lemma 10.7, the natural map $\Pi_p : L \otimes_K K_{\mathfrak{p}} \to L_{\mathcal{P}}$ is surjective for any $\mathcal{P} \mid \mathfrak{p}$. Since $L_{\mathcal{P}}$ is a field, Π_p factors through L_i for some i and hence $L_i \cong L_{\mathcal{P}}$ by surjectivity.

□

Example 10.1. If $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, then $f(X) = X^2 + 1$. So either by Hensel or the computation done in the first lecture, $i \in \mathbb{Q}_5$. Hence (5) splits in $\mathbb{Q}(i)$, so $5\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$.

04 Nov 2022, Lecture 13

Corollary 10.10. Take $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ a prime ideal. For $x \in L$,

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

Proof. Let $B_1, \dots, B_r$ be a basis for $L_{\mathcal{P}_1}, \dots, L_{\mathcal{P}_r}$ as $K_{\mathfrak{p}}$–vector spaces (here $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$). Then $B = \bigcup_i B_i$ is a basis for $L \otimes_K K_{\mathfrak{p}}$ over $K_{\mathfrak{p}}$. Let $[\mathrm{mult}(x)]_B$ (respectively $\mathrm{mult}(x)_{B_i}$) denote the matrix for the multiplication by x map $\mathrm{mult}(x) : L \otimes_K K_{\mathfrak{p}} \to L \otimes_K K_{\mathfrak{p}}$ (respectively $L_{\mathcal{P}_i} \to L_{\mathcal{P}_i}$) with respect to B (respectively the B_i). Then we get a block matrix

$$[\mathrm{mult}(x)]_B = \begin{pmatrix} [\mathrm{mult}(x)]_{B_1} & & & \\ & [\mathrm{mult}(x)]_{B_2} & & \\ & & \ddots & \\ & & & [\mathrm{mult}(x)]_{B_r} \end{pmatrix}$$

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

□

11 Decomposition groups

As before, let us work over a finite separable Dedekind domain. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$ and write $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$.

Note. For any i, $\mathfrak{p} \subset \mathcal{P}_i \cap \mathcal{O}_K \subsetneq \mathcal{O}_K$, hence $\mathfrak{p} = \mathcal{P}_i \cap \mathcal{O}_K$.

Definition 11.1. (i) We say $\mathfrak{p}$ **ramifies** in L if $e_i > 1$ for some i.

(ii) The e_i are called the **ramification indices** of $\mathcal{P}_i$ over $\mathfrak{p}$.

Example 11.1. If $\mathcal{O}_K = \mathbb{C}[t], \mathcal{O}_L = \mathbb{C}[T]$, then consider the map $\mathcal{O}_K \to \mathcal{O}_L$ by $t \mapsto T^n$. Then $t\mathcal{O}_L = T^n\mathcal{O}_L$, so the ramification index of (T) over (t) is n.

This corresponds geometrically to the degree n covering of Riemann surfaces $\mathbb{C} \to \mathbb{C}$ by $x \mapsto x^n$. This map is ramified at 0 with ramification index n.

Definition 11.2. We define $f_i = [\mathcal{O}_L/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$, called the **residue class degree** of $\mathcal{P}_i$ over $\mathfrak{p}$.

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

Proof. Let $S = \mathcal{O}_K/\mathfrak{p}$. The following properties of localization are left as an exercise:

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

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

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

In particular, (2) and (3) imply that e_i, 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 CRT, we have

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

Now it suffices to count dimensions on both sides as $k = \mathcal{O}_K/\mathfrak{p}$–vector spaces.

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

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

Note that $\mathcal{P}_i^j/\mathcal{P}_i^{j+1}$ is an $\mathcal{O}_L/\mathcal{P}_i$ module that is generated by $x \in \mathcal{P}_i^j/\mathcal{P}_i^{j+1}$. (For example, we can prove this after localizing at $\mathcal{P}_i$). Then $\dim_k(\mathcal{P}_i^j/\mathcal{P}_i^{j+1}) = f_i$ and we have $\dim_k(\mathcal{O}_L/\mathcal{P}_i^{e_i}) = e_i f_i$. Hence $\dim_k(\text{RHS}) = \sum_{i=1}^r e_i f_i$.

LHS: The structure theorem for finitely generated modules over PID's tells us that $\mathcal{O}_L$ is a free module over $\mathcal{O}_K$ of rank $[L : K]$. Thus $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_K/\mathfrak{p})^n$ as $\mathcal{O}_K$–modules and hence $\dim_k(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = n$. □

Geometric analogue: Let $X \to Y$ be a degree n cover of compact Riemann surfaces. For $y \in Y$, $n = \sum_{x \in f^{-1}(y)} e_x$ for e_x the ramification index of x.

Now assume $[L : K]$ is Galois. Then for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathcal{P}_i) \cap \mathcal{O}_K = \mathfrak{p}$, hence $\sigma(\mathcal{P}_i) \in \{\mathcal{P}_1, \dots, \mathcal{P}_r\}$, i.e. $\mathrm{Gal}(L/K)$ acts on $\{\mathcal{P}_1, \dots, \mathcal{P}_r\}$.

Proposition 11.2. The action of $\mathrm{Gal}(L/K)$ on $\{\mathcal{P}_1, \dots, \mathcal{P}_r\}$ is transitive.

Proof. Suppose not, so $\exists i \neq j$ such that $\sigma(\mathcal{P}_i) \neq \mathcal{P}_j$ $\forall \sigma \in \mathrm{Gal}(L/K)$. By CRT, we may choose $x \in \mathcal{O}_L$ such that $x \equiv 0 \pmod{\mathcal{P}_i}$ and $x \equiv 1 \pmod{\sigma(\mathcal{P}_j)}$ $\forall \sigma \in \mathrm{Gal}(L/K)$. Then

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

Since $\mathcal{P}_j$ is prime, there must exist some $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(x) \in \mathcal{P}_j \implies x \in \tau^{-1}(\mathcal{P}_j)$, so $x \equiv 0 \pmod{\tau^{-1}(\mathcal{P}_j)}$, a contradiction. □

Corollary 11.3. Suppose L/K is Galois. Then $e_1 = e_2 = \ldots = e_r = e$, $f_1 = \ldots = f_r = f$ and hence $n = efr$.

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

(i) $\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathcal{P}_1)^{e_1} \ldots \sigma(\mathcal{P}_r)^{e_r}$. Hence $e_1 = \ldots = e_r$ since the Galois group acts transitively.

(ii) $\mathcal{O}_L/\mathcal{P}_i \cong \mathcal{O}_L/\sigma(\mathcal{P}_i)$ via σ, so $f_1 = \ldots = f_r$.

The formula now follows from Theorem 11.1. □

If L/K is an extension of complete discretely valued fields with normalized valuations v_L and v_K with uniformizers π_L, π_K, then the ramification index is $e = e_{L/K} = v_L(\pi_K)$ (i.e. $\pi_K \mathcal{O}_L = \pi_L^e \mathcal{O}_L$). The residue class degree is $f = f_{L/K} = [k_L : k]$.

Corollary 11.4. Let L/K be finite and separable. Then $[L : K] = ef$.

Remark. This corollary holds even if L/K is not separable.

Now let $\mathcal{O}_K$ be a Dedekind domain again.

Definition 11.3. Let L/K be a finite Galois extension. The **decomposition group** at a prime $\mathcal{P}$ of $\mathcal{O}_L$ is the subgroup of $\mathrm{Gal}(L/K)$ defined by

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

By Proposition 11.2, for any $\mathcal{P}, \mathcal{P}'$ dividing $\mathfrak{p}$, $G_{\mathcal{P}}$ and $G_{\mathcal{P}'}$ are conjugate and hence have size ef by the orbit–stabilizer theorem.

07 Nov 2022, Lecture 14

Proposition 11.5. Suppose $\mathcal{P} \mid \mathfrak{p} \subset \mathcal{O}_K$. Then

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

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

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

(ii) Let $\sigma \in \mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$. Then $\sigma(L) = L$ since L/K is normal. Hence we have a map $\mathrm{res} : \mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$ by $\sigma \mapsto \sigma|_L$. Since L is dense in $L_{\mathcal{P}}$, res is injective. By Lemma 8.1, $|\sigma(x)|_{\mathcal{P}} = |x|_{\mathcal{P}}$ $\forall \sigma \in$

$\mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}}), x \in L_{\mathcal{P}}$. Hence $\sigma(\mathcal{P}) = \mathcal{P}\ \forall \sigma \in \mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$ and thus $\mathrm{res}(\sigma) \in G_{\mathcal{P}}\ \forall \sigma \in \mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$.

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

- $|G_{\mathcal{P}}| = ef$ follows from Proposition 11.2, corollary 11.3 and the orbit–stabilizer theorem.
- $[L_{\mathcal{P}} : K_{\mathfrak{p}}] = ef$ follows from Corollary 11.4, noting that e and f don't change when we take completions.

□

12 Ramification theory

12.1 The different and discriminant

In this section, assume that L/K is an extension of algebraic number fields with $[L : K] = n$ and $\mathcal{O}_K, \mathcal{O}_L$ are the rings of integers.

Notation. For $x_1, \dots, x_n \in L$, set $\Delta(x_1, \dots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)) \in K$. We can show that $\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$ for $\sigma_i : L \to \overline{K}$ the embeddings.

Note that if $y_i = \sum_{j=1}^n a_{ij} x_j$ for $a_{ij} \in K$, then

$$\Delta(y_1, \dots, y_n) = (\det A)^2 \Delta(x_1, \dots, x_n).$$

If $x_1, \dots, x_n \in \mathcal{O}_L$, then $\Delta(x_1, \dots, x_n) \in \mathcal{O}_K$.

Lemma 12.1. Let k be a perfect field and R a k–algebra which is finite–dimensional as a k–vector space. Then the trace form $(\cdot,\cdot) : R \times R \to R$ given by $(x, y) \mapsto \mathrm{Tr}_{R/k}(xy) = \mathrm{Tr}_k(\mathrm{mult}(xy))$ is nondegenerate if and only if $R = k_1 \times \ldots \times k_n$ where k_i/k are finite (hence separable) field extensions.

Proof. This is on example sheet 3. □

Theorem 12.2. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime ideal.

- If $\mathfrak{p}$ ramifies in L, then $\forall x_1, \dots, x_n \in \mathcal{O}_L$, $\Delta(x_1, \dots, x_n) \equiv 0 \pmod{\mathfrak{p}}$.
- If $\mathfrak{p}$ is unramified in L, then $\exists x_1, \dots, x_n \in \mathcal{O}_L$ such that $\mathfrak{p} \nmid \Delta(x_1, \dots, x_n)$.

Proof. (i) Let $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \ldots \mathcal{P}_r^{e_r}$ with the $\mathcal{P}_i$ distinct and $e_i > 0$. CRT implies that

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

If $\mathfrak{p}$ ramifies in L, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ has nilpotent elements. By Lemma 12.1, the trace form $\mathrm{Tr}_{R/k}$ (for k the residue field at $\mathfrak{p}$) is degenerate, so

$\Delta(\overline{x_1}, \ldots, \overline{x_n}) = 0 \ \forall \overline{x_i} \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Hence $\Delta(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}$ for any $x_1, \ldots, x_n \in \mathcal{O}_L$ through the commutativity of the diagram

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

(ii) If $\mathfrak{p}$ is unramified in L, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a product of finite extensions of k, so by Lemma 12.1 the trace form is nondegenerate. Hence we can pick a basis $\overline{x_1}, \ldots, \overline{x_n}$ of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ as a k–vector space, so $\Delta(\overline{x_1}, \ldots, \overline{x_n}) \neq 0$. Hence $\exists x_1, \ldots, x_n \in \mathcal{O}_L$ such that $\Delta(x_1, \ldots, x_n) \not\equiv 0 \pmod{\mathfrak{p}}$.

□

Definition 12.1. The **discriminant** is the ideal $d_{L/K} \subset \mathcal{O}_K$ generated by $\Delta(x_1, \ldots, x_n)$ for all choices $x_1, \ldots, x_n \in \mathcal{O}_L$.

Corollary 12.3. A prime ideal $\mathfrak{p}$ ramifies in $L \iff \mathfrak{p} \mid d_{L/K}$.

In particular, only finitely many ideals ramify in L.

Definition 12.2. The **inverse different** is

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

which is an $\mathcal{O}_L$–submodule of $\mathcal{O}_L$.

Lemma 12.4. $D_{L/K}^{-1}$ is a fractional ideal in L containing $\mathcal{O}_L$.

Proof. Let $x_1, \ldots, x_n \in \mathcal{O}_L$ be a K–basis for L/K. Set $d = \Delta(x_1, \ldots, x_n) = \det(\mathrm{Tr}(x_i x_j)) \neq 0$ (as an extension of number fields is separable). For $x \in D_{L/K}^{-1}$, write $x = \sum_{j=1}^n \lambda_j x_j$ for $\lambda_j \in K$. Then $\mathrm{Tr}(x x_j) = \sum_{j=1}^n \lambda_j \mathrm{Tr}(x_i, x_j) \in \mathcal{O}_K$. Set $A_{ij} = \mathrm{Tr}_{L/K}(x_i x_j)$. Multiplying by $\mathrm{Adj}(A) \in M_n(\mathcal{O}_K)$ gives

$$d \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \mathrm{Adj}(A) \begin{pmatrix} \mathrm{Tr}_{L/K}(x x_1) \\ \vdots \\ \mathrm{Tr}_{L/K}(x x_n) \end{pmatrix}.$$

Hence $\lambda_i \in \frac{1}{d}\mathcal{O}_K$, so $x \in \frac{1}{L}\mathcal{O}_L$, so $D_{L/K}^{-1} \subset \frac{1}{d}\mathcal{O}_L$, so $D_{L/K}^{-1}$ is a fractional ideal.

Finally, $\mathrm{Tr}(x) \in \mathcal{O}_K \ \forall \in \mathcal{O}_L$, so $\mathcal{O}_L \subset D_{L/K}^{-1}$. □

Definition 12.3. The inverse $D_{L/K} \subset \mathcal{O}_L$ of $D_{L/K}^{-1}$ is the **different ideal**.

09 Nov 2022, Lecture 15

Let L/K be a degree n extension of number fields, and let I_L, I_K be the groups of fractional ideals. Then (todo: lectures said Proposition 9.7 – I think that corresponds to Theorem 9.5 in my notes?) Proposition 9.7 gives us that

$$I_L \cong \bigoplus_{\substack{0 \neq \mathfrak{p} \\ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_L}} \mathbb{Z}$$
$$I_K \cong \bigoplus_{\substack{0 \neq \mathfrak{p} \\ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_K}} \mathbb{Z}.$$

Define $N_{L/K} : I_L \to I_K$ induced by $\mathcal{P} \mapsto \mathfrak{p}^f$ for $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$ and $f = f(\mathcal{P}/\mathfrak{p})$.

Then it is a fact that the following diagram commutes:
$$\begin{tikzcd} L^\times \arrow[r] \arrow[d, "N_{L/K}"] & I_L \arrow[d, "N_{L/K}"] \\ K^\times \arrow[r] & I_K \end{tikzcd}$$
. One way to see this is to use Corollary 10.10 and $v_{\mathfrak{p}}(N_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(x)) = f_{\mathcal{P}/\mathfrak{p}} v_{\mathcal{P}}(x)$ for $x \in L_{\mathcal{P}}$ and $v_{\mathfrak{p}}, v_{\mathcal{P}}$ the normalized valuations on $L_{\mathcal{P}}$, $K_{\mathfrak{p}}$. (Remember that here $f = [\mathcal{O}_L/\mathcal{P} : \mathcal{O}_K/\mathfrak{p}]$).

Theorem 12.5. $N_{L/K}(D_{L/K}) = d_{L/K}$.

Proof. First assume that $\mathcal{O}_K, \mathcal{O}_L$ are PIDs. Let $x_1, \ldots, x_n$ be a $\mathcal{O}_K$–basis for $\mathcal{O}_L$ and $y_1, \ldots, y_n$ the dual basis with respect to the trace form. Then $y_1, \ldots, y_n$ gives a basis for $D_{L/K}^{-1}$. Let $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ be the embeddings and consider $\sum_{i=1}^n \sigma_i(x_j)\sigma_i(y_k) = \mathrm{Tr}_{L/K}(x_j y_k) = \delta_{jk}$.

But $\Delta(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2$. Thus $\Delta(x_1, \ldots, x_n)\Delta(y_1, \ldots, y_n) = 1$. Write $D_{L/K}^{-1} = \beta\mathcal{O}_L$ for some $\beta \in \mathcal{O}_L$ (as $\mathcal{O}_L$ is assumed to be a PID). Then the change of basis matrix between $y_1, \ldots, y_n$ and $\beta x_1, \ldots, \beta x_n$ is invertible in $\mathcal{O}_K$, so

$$\begin{aligned} d_{L/K}^{-1} =& \Delta(x_1, \ldots, x_n)^{-1} = \Delta(y_1, \ldots, y_n) \\ =& \Delta(\beta x_1, \ldots, \beta x_n) = N_{L/K}(\beta)^2 \Delta(x_1, \ldots, x_n). \end{aligned}$$

Thus $d_{L/K}^{-1} = N_{L/K}(D_{L/K}^{-1})^2 d_{L/K}$, so $N_{L/K}(D_{L/K}) = d_{L/K}$.

In general, localize at $S = \mathcal{O}_K/\mathfrak{p}$ and note that localizing $\mathcal{O}_K$ gives a DVR (hence a PID), localizing $\mathcal{O}_L$ gives a Dedekind domain with finitely many prime ideals (hence a PID by example sheet 2) and that $S^{-1}D_{L/K} = D_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$ and $S^{-1}d_{L/K} = d_{S^{-1}\mathcal{O}_L/s^{-1}\mathcal{O}_K}$ (details left as exercise). □

Theorem 12.6. If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and α has minimal polynomial $g(X) \in \mathcal{O}_K[X]$, then $D_{L/K} = (g'(\alpha))$.

Proof. Write $\frac{g(X)}{X-\alpha} = \beta_{n-1}X^{n-1} + \ldots + \beta_1 X + \beta_0$ with $\beta_i \in \mathcal{O}_L$ and $\beta_{n-1} = 1$

and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of g. We claim that for $0 \leq r \leq n-1$,

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

Indeed, the difference is a polynomial in X of degree $< n$ which vanishes for $X = \alpha_1, \ldots, \alpha_n$. Equating coefficients of X^s on both sides gives $\delta_{rs} = \mathrm{Tr}_{L/K}\left(\frac{\alpha^r \beta_s}{g'(\alpha)}\right)$. Hence $\mathcal{O}_L$ has $\mathcal{O}_K$–basis $1, \alpha, \ldots, \alpha^{n-1}$, $D_{L/K}^{-1}$ has $\mathcal{O}_K$–basis $\frac{\beta_0}{g'(\alpha)}, \frac{\beta_1}{g'(\alpha)}, \ldots, \frac{\beta_{n-1}}{g'(\alpha)} = \frac{1}{g'(\alpha)}$. Hence the last element generates all the others, so $D_{L/K}^{-1} = \left(\frac{1}{g'(\alpha)}\right)$, so $D_{L/K} = (g'(\alpha))$. □

Take $\mathcal{P}$ a nonzero prime ideal of $\mathcal{O}_L$ and $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$. We can define $D_{L_\mathcal{P}/K_\mathfrak{p}}$ using $\mathcal{O}_{L_\mathcal{P}}$ and $\mathcal{O}_{K_\mathfrak{p}}$. We can identify $D_{L_\mathcal{P}/K_\mathfrak{p}}$ with a power of $\mathcal{P}$.

Theorem 12.7. $D_{L/K} = \prod_\mathcal{P} D_{L_\mathcal{P}/K_\mathfrak{p}}$.

Note that we will later verify that the product is finite.

Proof. Let $x \in L$ and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal. Then $\mathrm{Tr}_{L/K}(x) \overset{(\star)}{=} \sum_{\mathcal{P}|\mathfrak{p}} \mathrm{Tr}_{L_\mathcal{P}/K_\mathfrak{p}}(x)$ (compare with Corollary 10.10). Let $r(\mathcal{P}) = v_\mathfrak{p}(D_{L/K})$ and $s(\mathcal{P}) = v_\mathcal{P}(D_{L_\mathcal{P}/K_\mathfrak{p}})$. We want to show that $r(\mathcal{P}) = s(\mathcal{P})$.

For $\subset$ (i.e. $r(\mathcal{P}) \geq s(\mathcal{P})$), take $x \in L$ with $v_\mathcal{P}(x) \geq -s(\mathcal{P})$ $\forall \mathcal{P}$. Then $\mathrm{Tr}_{L_\mathcal{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in \mathcal{O}_L$ and $\forall \mathcal{P}$. Then $(\star)$ gives $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in \mathcal{O}_L$ and $\forall \mathfrak{p}$. Hence $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K$ $\forall y \in \mathcal{O}_L$, i.e. $x \in D_{L/K}$. Thus $D_{L/K} \subset \prod_\mathcal{P} D_{L_\mathcal{P}/K_\mathfrak{p}}$.

For $\supset$, i.e. $r(\mathcal{P}) \leq s(\mathcal{P})$, fix $\mathcal{P}$ and let $x \in \mathcal{P}^{-r(\mathcal{P})} \setminus \mathcal{P}^{-r(\mathcal{P})+1}$. Then $v_\mathcal{P}(x) = -r(\mathcal{P})$, so $v_{\mathcal{P}'}(x) \geq 0$ $\forall \mathcal{P}' \neq \mathcal{P}$. By $(\star)$,

$$\mathrm{Tr}_{L_\mathcal{P}/K_\mathfrak{p}}(xy) = \underbrace{\mathrm{Tr}_{L/K}(xy)}_{\mathcal{O}_K} - \sum_{\substack{\mathcal{P}'|\mathfrak{p} \\ \mathcal{P}' \neq \mathcal{P}}} \underbrace{\mathrm{Tr}_{L_{\mathcal{P}'}/K_\mathfrak{p}}(xy)}_{\in \mathcal{O}_{K_\mathfrak{p}}} \ \forall y \in \mathcal{O}_L.$$

By continuity, $\mathrm{Tr}_{L_\mathcal{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in \mathcal{O}_{L_\mathcal{P}}$, so $x \in D_{L_\mathcal{P}/K_\mathfrak{p}}^{-1}$, i.e. $-v_\mathcal{P}(x) = r(\mathcal{P}) \leq s(\mathcal{P})$. Hence $D_{L/K} \supset \prod_\mathcal{P} D_{L_\mathcal{P}/K_\mathfrak{p}}$. □

Corollary 12.8. $d_{L/K} = \prod_{\mathcal{P}|\mathfrak{p}} d_{L_\mathcal{P}/K_\mathfrak{p}}$.

Proof. Apply $N_{L/K}$ to $D_{L/K} = \prod_\mathcal{P} D_{L_\mathcal{P}/K_\mathfrak{p}}$. □

13 Unramified and totally ramified extensions of local fields

In this section, let L/K be a finite separable extension of non–archimedean local fields. By Corollary 11.4, $[L : K] = e_{L/K} f_{L/K}$.

Lemma 13.1. Let $M/L/K$ be finite separable extensions of local fields. Then $f_{M/K} = f_{M/L} f_{L/K}$ and $e_{M/K} = e_{M/L} e_{L/K}$.

Proof. $f_{M/K} = [k_M : k] = [k_M : k_L][k_L : k] = f_{M/L} f_{L/K}$. The other result follows from this one and $\operatorname{Tr}_{L/K}(x) = \sum_{\mathcal{P}|\mathfrak{p}} \operatorname{Tr}_{L_{\mathcal{P}}/K_{\mathfrak{p}}}(x)$. □

Definition 13.1. The extension L/K is said to be

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

11 Nov 2022, Lecture 16

Theorem 13.2. Let L/K be a finite separable extension of local fields. Then there exists a field K_0 with $K \subset K_0 \subset L$ such that

(i) K_0/K is unramified.

(ii) L/K_0 is totally ramified.

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

Proof. Let $k = \mathbb{F}_q$, so that $k_L = \mathbb{F}_{q^f}$ for $f = f_L/K$ the residue class degree. Set $m = q^f - 1$ and $[\ ] : \mathbb{F}_{q^f} \to L$ the Teichmüller map for L. Let $\zeta_m = [\alpha]$ for α a generator for $\mathbb{F}_{q^f}^\times$. Then ζ_m is a primitive m^{th} root of unity. Set $K_0 = K(\zeta_m) \subset L$, then K_0/K is Galois and K_0 has residue field $k_0 = \mathbb{F}(\alpha) = k_L$. Hence $f_{L/K_0} = 1$, so L/K_0 is totally ramified.

Let $\operatorname{res} : \operatorname{Gal}(K_0/K) \to \operatorname{Gal}(k_0/k)$ be the natural map. For $\sigma \in \operatorname{Gal}(K_0/K)$, we have $\sigma(\zeta_m) = \zeta_m \iff \sigma(\zeta_m) \equiv \zeta_m \pmod{\mathfrak{m}_0}$, since by Hensel's lemma, we have a bijection between $\mu_m(K_0)$ and $\mu_m(k_0)$. Hence res is injective. Thus $|\operatorname{Gal}(K_0/K)| \leq |\operatorname{Gal}(k_0/k)| = f_{K_0/K}$. Hence $[K_0 : K] = f_{K_0/K}$, so res is an isomorphism and K_0/K is unramified. □

Theorem 13.3. Let K be a local field and let $k = \mathbb{F}_q$. For each $n \geq 1$, there exists a unique unramified extension L/K of degree n. Moreover, L/K is Galois and the natural map $\operatorname{Gal}(L/K) \to \operatorname{Gal}(k_L/k)$ is an isomorphism. In particular, $\operatorname{Gal}(L/K) \cong \langle \operatorname{Frob}_{L/K} \rangle$, where $\operatorname{Frob}_{L/K}(x) \equiv x^q \pmod{\mathfrak{m}_L}\ \forall x \in \mathcal{O}_L$.

Proof. For $n \geq 1$, take $L = K(\zeta_m)$ where $m = q^n - 1$. As in Theorem 13.2, $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Hence $\mathrm{Gal}(L/K)$ is cyclic and generated by a lift of $x \mapsto x^q$.

For uniqueness, we have a degree n unramified extension L/K. By the Teichmüller lift, $\zeta_m \in L$, so $L = K(\zeta_m)$. □

Corollary 13.4. For L/K a finite Galois extension, the map res : $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is surjective.

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

Definition 13.2. For L/K a Galois extension, the **inertia subgroup** is

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

Note that:

- Since $e_{L/K} f_{L/K} = [L : K]$, we have $|I_{L/K}| = e_{L/K}$.
- $I_{L/K} = \mathrm{Gal}(L/K_0)$, where K_0 is as in Theorem 13.2.

Definition 13.3. Let $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathcal{O}_K[X]$. We say f is **Eisenstein** if $v_K(a_i) \geq 1$ and $v_K(a_0) = 1$ for v_K the normalized evaluation on K.

Fact. $f(x)$ Eisenstein $\implies$ $f(x)$ irreducible.

Theorem 13.5. (i) Let L/K be a finite totally ramified extension and let $\pi_L \in \mathcal{O}_L$ be a uniformizer. Then the minimal polynomial of π_L is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ (so $L = K(\pi_L)$).

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

Proof. (i) Let $[L : K] = e = e_{L/K}$ and let $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathcal{O}_K[X]$ be the minimal polynomial for π_L. Then $m \leq e$. Since $v_L(K^\times) = e\mathbb{Z}$, we have $v_L(a_i\pi_L^i) \equiv i \pmod e$ for $i \leq m$. Hence $a_i\pi_L^i$ have distinct valuations. As $\pi_L^m = \sum_{i=0}^{m-1} a_i\pi_L^i$, we have

$$m = v_L(\pi_L^m) = \min_{0\leq i\leq m-1}(i + ev_K(a_i)).$$

Hence $v_K(a_i) \geq 1$ $\forall i$ and hence $v_K(a_0) = 1$ and $m = e$. Thus $f(X)$ is Eisenstein and $L = K(\pi_L)$.

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

$$v_L(y) = \min_{0\leq i\leq e-1}(i + ev_K(b_i)).$$

Thus $y \in \mathcal{O}_L \iff v_L(y) \geq 0 \iff v_K(b_i) \geq 0 \ \forall i \iff y \in \mathcal{O}_K[\pi_L]$.

(ii) Let $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathcal{O}_K[X]$ be Eisenstein and $e = e_{L/K}$ (for $L = K(\alpha)$). Thus $v_L(a_i) \geq e$ and $v_L(a_0) = e$. If $v_L(\alpha) \leq 0$, then $v_L(\alpha^n) \leq v_L\left(\sum_{i=0}^{n-1} a_i\alpha^i\right)$, a contradiction and hence $v_L(\alpha) > 0$. For $i \neq 0$, $v_L(a_i\alpha^i) > e = v_L(a_0)$. Therefore $v_L(\alpha^n) = v_L\left(-\sum_{i=0}^{n-1} a_i\alpha^i\right) = v_L(a_0)$. Hence $nv_L(\alpha) = v_L(a_0) = e$, but $n = [L : K] \geq e$, so $n = e$ and $v_L(\alpha) = 1$.

□

14 Structure of units

Proposition 14.1. Let K be a finite extension of $\mathbb{Q}_p$, write $e = e_{K/\mathbb{Q}_p}$ and let π be a unit in K. If $r > \frac{e}{p-1}$, then $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ converges on $\pi^r\mathcal{O}_K$ and induces an isomorphism $(\pi^r\mathcal{O}_K, +) \cong (1 + \pi^r\mathcal{O}_K, \times)$.

Proof. $v_K(n!) = ev_p(n!) \overset{(\star)}{=} \frac{e(n-s_p(n))}{p-1} \leq e\left(\frac{n-1}{p-1}\right)$ for $(\star)$ from example sheet 1. For $x \in \pi^r\mathcal{O}_K$ and $n \geq 1$, compute $v_K(\frac{x^n}{n!}) \geq nr - e\frac{n-1}{p-1} = r + (n-1)\left(r - \frac{e}{p-1}\right)$, so $v_K(\frac{x^n}{n!}) \to \infty$ as $n \to \infty$. Hence $\exp(x)$ converges on $\pi^r\mathcal{O}_K$. Since $v_K(\frac{x^n}{n!}) \geq r \ \forall n \geq 1$, $\exp(x) \in 1 + \pi^r\mathcal{O}_K$.

Similarly consider $\log(x) : 1+\pi^r\mathcal{O}_K \to \pi^r\mathcal{O}_K$ by $\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}x^n$. We can check the convergence as before (exercise, this is easier than the previous case). Recall the identities in $\mathbb{Q}[[X, Y]] : \exp(X + Y) = \exp(X)\exp(Y)$ and $\exp(\log(1 + X)) = 1 + X$, so $\exp(\log(X)) = X$. These identities together give the isomorphism. □

14 Nov 2022, Lecture 17

When K is a local field, possibly of equal characteristic, write $U_K = \mathcal{O}_K^\times$ and let $\pi \in \mathcal{O}_K$ be a uniformizer.

Definition 14.1. For $s \in \mathbb{Z}_{\geq 1}$, the s^{th} unit group $U_K^{(s)}$ is defined by

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

and $U_K^{(0)} = U_K$. Then we have $\ldots \subset U_K^{(s)} \subset \ldots \subset U_K^{(1)} \subset U_K^{(0)}$.

Proposition 14.2. (i) $U_K^{(0)}/U_K^{(1)} \cong (k^x, \times)$ (for $k = \mathcal{O}_K/\mathfrak{m}$).

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

Proof. (i) The natural map $\mathcal{O}_K^\times \to k^\times$ given by reduction mod π is surjective with kernel $1 + \pi\mathcal{O}_K = U_K^{(1)}$.

(ii) Define $f : U_K^{(s)} \to k$ by $1 + \pi^s x \mapsto x \pmod{\pi}$. This is a homomorphism, as $(1 + \pi^s x)(1 + \pi^s y) = 1 + \pi^s(x + y + \pi^s xy)$ and $x + y + \pi^s xy \equiv x + y \pmod{\pi}$ as desired. f is surjective with $\ker(f) = U_K^{(s+1)}$.

□

Corollary 14.3. Let $[K : \mathbb{Q}_p] < \infty$. Then there exists a finite index subgroup of $\mathcal{O}_K^\times$ isomorphic to $(\mathcal{O}_K, +)$.

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

Remark. This is not true for K of equal characteristic, since exp is not defined.

Example 14.1. Consider $\mathbb{Z}_p^\times$ for $p > 2$, so $e = 1$. Then we can take $r = 1$, so $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$ by $x \mapsto (x \pmod{p}, \frac{x}{[x \pmod{p}]})$. We can rewrite $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \cong \mathbb{F}_p^\times \times \mathbb{Z}_p \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.

If $p = 2$, take $r = 2$ to get $\mathbb{Z}_2^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (1+4\mathbb{Z}_p)$ by $x \mapsto (x \pmod{4}, \frac{x}{\epsilon(x)})$ where $\epsilon(x) = \begin{cases} 1 & x \equiv 1 \pmod{4} \\ -1 & x \equiv 3 \pmod{4} \end{cases}$. Again note $\mathbb{Z}_2^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + 4\mathbb{Z}_p) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

This gives another proof of $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \equiv \begin{cases} \mathbb{Z}/2\mathbb{Z} & p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^2 & p = 2 \end{cases}$.

15 Higher ramification groups

Fix a finite Galois extension L/K of local fields. From now on, assume a local field is non–archimedean. Fix $\pi_L \in \mathcal{O}_L$ a uniformizer.

Definition 15.1. Let v_L be the normalized valuation on L. For $s \in \mathbb{R}_{\geq -1}$, the s^{th} **ramification group** is

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

Remark. G_s only changes at the integers. $s \in R_{\geq -1}$ is used to define upper numbering (to be done later).

Example 15.1. $G_{-1}(L/K) = \mathrm{Gal}(L/K)$ and

$$\begin{aligned} G_0(L/K) &= \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \pmod{\pi} \ \forall x \in \mathcal{O}_L\} \\ &= \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)) = I_{L/K} \end{aligned}$$

Note. For $s \geq 0$, $G_s(L/K) = \ker(\mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{O}_L/\pi_L^{s+1}\mathcal{O}_L))$, hence $G_s(L/K)$ are normal in $\mathrm{Gal}(L/K)$. We have

$$\ldots \subset G_s(L/K) \subset G_{s-1}(L/K) \subset \ldots \subset G_1(L/K) \subset \mathrm{Gal}(L/K).$$

Theorem 15.1. (i) For $s \geq 1$, $G_s = \{\sigma \in G_0 \mid v_L(\sigma(\pi_L) - \pi_L) \geq s+1\}$.

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

(iii) Let $s \in \mathbb{Z}_{\geq 0}$. Then there exists an injective group homomorphism

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

This map is independent of choice of π_L.

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

(i) By Theorem 13.5, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Suppose $v_L(\sigma(\pi_L) - \pi_L) \geq s+1$. Let $x \in \mathcal{O}_L$, then $x = f(\pi_L)$, where $f(X) \in \mathcal{O}_K[X]$. Then compute

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

for $g(X) \in \mathcal{O}_K[X]$, since $X - Y \mid f(X) - f(Y)$. Thus

$$v_L(\sigma(x) - x) = v_L(\sigma(\pi_L) - \pi_L) + v_L(g(\pi_L)) \geq (s+1) + 0 = s+1.$$

(ii) Suppose $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma \neq 1$. Then $\sigma(\pi_L) \neq \pi_L$ as $L = K(\pi_L)$. Hence $v_L(\sigma(\pi_L) - \pi_L) < \infty$. Then $\sigma \notin G_s$ for s large enough by (i).

(iii) Note that for $\sigma \in G_s$, $s \in \mathbb{Z}_{\geq 0}$, we have $\sigma(\pi_L) \in \pi_L + \pi_L^{s+1}\mathcal{O}_L$. This gives us that $\frac{\sigma(\pi_L)}{\pi_L} \in 1 + \pi_L^s\mathcal{O}_L = U_L^{(s)}$. We claim that $\phi : G_s \to U_L^{(s)}/U_L^{(s+1)}$ by $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$ is a group homomorphism with kernel G_{s+1}.

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

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

But $\sigma(u) \in u + \pi_L^{s+1}\mathcal{O}_L$ since $\sigma \in G_s$, so $\frac{\sigma(u)}{u} \in 1 + \pi_L^{s+1}\mathcal{O}_L$ as u is a unit. Hence $\frac{\sigma\tau(\pi_L)}{\pi_L} = \frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L} \pmod{U_L^{(s+1)}}$ is a group homomorphism.

Moreover, the kernel is $\{\sigma \in G_s \mid \sigma(\pi_L) \equiv \pi_L \pmod{\pi_L^{s+2}}\} = G_{s+1}$.

If $\pi'_L = a\pi_L$ is another uniformizer for $a \in \mathcal{O}_L^\times$, then

$$\frac{\sigma(\pi'_L)}{\pi'_L} = \frac{\sigma(a)}{a}\frac{\sigma(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \pmod{U_L^{(s+1)}}.$$

□

Corollary 15.2. $\mathrm{Gal}(L/K)$ is solvable.

Proof. By Proposition 14.2 and Theorem 15.1, for $s \in \mathbb{Z}_{s\geq -1}$, we have

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

Thus G_s/G_{s+1} is solvable as all of the groups on the right are, as they are abelian. We conclude using Theorem 15.1 (ii), which says that the intersection of all of these groups is trivial. □

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

Definition 15.2. The group G_1 is called the **wild inertia group**.

Definition 15.3. The quotient G_0/G_1 is called the **tame inertia group**.

16 Nov 2022, Lecture 18

If L/K is a finite separable extension of local fields, then we say L/K is **tamely ramified** if char $k \nmid e_{L/K}$. Otherwise, we say L/K is **wildly ramified**.

Theorem 15.3. Assume $[K : \mathbb{Q}_p] < \infty$, so L/K is finite, hence separable. Write $D_{L/K} = (\pi_L^{\delta(L/K)})$. 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 $\iff D_{L/K} = \mathcal{O}_L$.

Proof. In example sheet 3 we show $D_{L/K} = D_{L/K_0}D_{K_0/K}$, where K_0 is the subextension of L such that K_0/K is unramified and L/K is totally ramified. Hence it suffices to consider the unramified and totally ramified case separately.

(i) L/K is unramified. Then by Proposition 6.8, $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$ with $k_L = k(\overline{\alpha})$. Let $g(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of α. $[L : K] = [k_L : k] \implies \overline{g}(X) \in k[X]$ is the minimal polynomial of $\overline{\alpha} \implies \overline{g}(X)$ is separable and hence $g'(\alpha) \not\equiv 0 \pmod{\pi_L}$. Now Theorem 12.6 says that $D_{L/K} = (g'(\alpha)) = \mathcal{O}_L$.

(ii) L/K is totally ramified. Let $[L:K]=e$. Then $\mathcal{O}_L=\mathcal{O}_K[\pi_L]$ with π_L a root of $g(X)=X^e+\sum_{i=1}^{e-1}a_iX^i\in\mathcal{O}_K[X]$, which is Eisenstein. Now compute $g'(\pi_L)=\underbrace{e\pi_L^{e-1}}_{v_L\geq e-1}+\underbrace{\sum_{i=0}^{e-1}ia_i\pi_L^{i-1}}_{v_L\geq e}$. Thus $v_L(g'(\pi_L))\geq e-1$ with equality if and only if char $k=p\nmid e$.

□

Corollary 15.4. Let L/K be an extension of number fields and $0\neq\mathcal{P}\subset\mathcal{O}_L$ is a prime ideal with $\mathfrak{p}=\mathcal{P}\cap\mathcal{O}_K$. Then $e(\mathcal{P}/\mathfrak{p})>1$ if and only if $\mathcal{P}\mid D_{L/K}$.

Proof. Theorem 12.7 tells us that $D_{L/K}=\prod_{\mathcal{P}}D_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$. Then use $e(\mathcal{P}/\mathfrak{p})=e_{L_{\mathcal{P}}/K_{\mathfrak{p}}}$ and Theorem 15.3. □

Example 15.2. Take $K=\mathbb{Q}_p$, ζ_{p^n} a primitive $p^{n^{\text{th}}}$ root of unity and $L=\mathbb{Q}_p(\zeta_{p^n})$. The $p^{n^{\text{th}}}$ cyclotomic polynomial is

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

An exercise on example sheet 3 will show that:

- $\Phi_{p^n}(X)$ is irreducible and hence the minimal polynomial of ζ_{p^n}.
- $L/\mathbb{Q}_p$ is Galois and totally ramified of degree $p^{n-1}(p-1)$.
- If we define $\pi=\zeta_{p^n}-1$, then π is a uniformizer of $\mathcal{O}_L$. Hence $\mathcal{O}_L=\mathbb{Z}_p[\zeta_{p^n}-1]=\mathbb{Z}_p[\zeta_{p^n}]$.
- $\text{Gal}(L/\mathbb{Q}_p)\cong(\mathbb{Z}/p^n\mathbb{Z})^\times$ (abelian) by $\sigma_m\leftrightarrow m$ where $\sigma_m(\zeta_{p^n})=\zeta_{p^n}^m$.

To find the higher ramification group, we compute

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

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

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

Now Theorem 15.1 (i) tells us that $\sigma\in G_i\iff p^k\geq i+1$. Thus

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

16 Local class field theory

16.1 Infinite Galois theory

Let L/K be an algebraic extension of fields.

Definition 16.1.
- L/K is separable if $\forall \alpha \in L$, its minimal polynomial $f_\alpha(X) \in K[X]$ is separable.
- L/K is normal if $f_\alpha(X)$ splits in L $\forall \alpha \in L$.
- L/K is Galois if it is normal and separable.

We write $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ in this case.

If L/K is finite and Galois, we have the Galois correspondence

$$\begin{aligned} \{\text{subextensions } K \subset K' \subset L\} &\leftrightarrow \{\text{subgroups of } \mathrm{Gal}(L/K)\} \\ K' &\mapsto \mathrm{Gal}(L/K') \end{aligned}$$

In the infinite case, we have the following definition.

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

Example 16.1. Any total order is a direct set, for example $(\mathbb{N}, \leq)$ or $(\mathbb{Z}_{\geq 1})$ ordered by divisibility.

Definition 16.3. Let $(I, \leq)$ be a directed set and $(G_i)_{i\in I}$ a collection of groups together with group homomorphisms (transition maps) $\phi_{ij} : G_j \to G_i$ such that $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$ $\forall i \leq j \leq k$ and $\phi_{ii} = \mathrm{id}$ $\forall i$. We say $((G_i)_{i\in I}, \phi_{ij})$ is an **inverse system**. The **inverse limit** of this inverse system $((G_i)_{i\in I}, \phi_{ij})$ is

$$\varprojlim_{i\in I} G_i = \{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid \phi_{ij}(g_j) = g_i\}.$$

Remarks.

- Taking $(\mathbb{N}, \leq)$ recovers our previous definition of an inverse limit.
- There exist projection maps $\Psi_j : \varprojlim_{i\in I} G_i \to G_j$.
- $\varprojlim_{i\in I} G_i$ satifies a universal property (defining left as exercise).

Assume G_i is finite. Then the **profinite topology** on $\varprojlim_{i\in I} G_i$ is the weakest topology making these projection maps continuous, i.e. such that the maps Ψ_j are continuous $\forall j \in I$.

Proposition 16.1. Let L/K be a (possibly infinite) Galois extension.

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

(ii) For $F, F' \in I$ with $F \subset F'$, there is a restriction map $\mathrm{res}_{F,F'} : \mathrm{Gal}(F'/K) \twoheadrightarrow \mathrm{Gal}(F/K)$ and the natural map $\mathrm{Gal}(L/K) \to \varprojlim_{F\in I} \mathrm{Gal}(F/K)$ is an isomorphism.

Proof. Exercise on example sheet 4. □

Theorem 16.2 (Fundamental theorem of Galois theory)**.** Let L/K be Galois. By Proposition 16.1, we can endow $\mathrm{Gal}(L/K)$ with the profinite topology (equal to the discrete topology is L/K is finite). Then there exists a bijection

$$\begin{aligned} \{F/K \text{ subextension of } L/K\} &\leftrightarrow \{\text{closed subgroups of } \mathrm{Gal}(L/K)\} \\ F &\mapsto \mathrm{Gal}(L/F) \\ L^H &\leftarrow\!\shortmid H \end{aligned}$$

Moreover:

- F/K is finite $\iff$ $\mathrm{Gal}(L/F)$ is open.
- F/K is Galois $\iff$ $\mathrm{Gal}(L/F)$ is normal in $\mathrm{Gal}(L/K)$.

Proof. Exercise on example sheet 4. The idea is to reduce everything to finite extensions. □

18 Nov 2022, Lecture 19

In other words, for L/K Galois, $\mathrm{Gal}(L/K) \cong \varprojlim_{\substack{K\subset F\subset L \\ F/K \text{ finite Galois}}} \mathrm{Gal}(F/K)$.

Example 16.2. Let $K = \mathbb{F}_q$ and $L = \overline{\mathbb{F}_q}$ the algebraic closure. Then L/K is Galois (for example since $\mathbb{F}_q$ is perfect). Then

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

where on the left we have ordering by containment and on the right by divisibility, i.e. $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n} \iff m \mid n$.

We can show there exists a commutative diagram $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \twoheadrightarrow \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \ni \mathrm{Frob}(q)$ corresponding to $1 \in \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z} \ni 1$. This gives us

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \varprojlim_{n\in(\mathbb{N},|)} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}},$$

where $\hat{\mathbb{Z}}$ is the **profinite completion** of $\mathbb{Z}$. On example sheet 3 we will see $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$. Note further that $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ corresponds to $1 \in \hat{\mathbb{Z}}$.

Let $\langle \mathrm{Frob}_q \rangle \subset \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ generated by Frob_q. Then $\mathrm{Frob}_q \subset \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ corresponds to $\mathbb{Z} \subset \hat{\mathbb{Z}}$.

17 Weil groups

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

Definition 17.1. We say that

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

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

Proposition 17.1. If L/K is unramified, then L/K is Galois and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$.

Proof. We know that every finite subextension F/K is unramified and hence Galois. Hence L/K is normal and separable and hence Galois. Moreover, there exists a commutative diagram $\mathrm{Gal}(L/K) \overset{\mathrm{res}}{\to} \mathrm{Gal}(k_L/k)$ which by Theorem 16.2 are correspondingly isomorphic to $\varprojlim_{\substack{F\subset L \\ F/K \text{ finite}}} \mathrm{Gal}(F/K) \overset{\mathrm{res}}{\to} \varprojlim_{\substack{k'\subset k_L \\ k'/k \text{ finite}}} \mathrm{Gal}(k'/k)$, but the LHS here is isomorphic to $\varprojlim_{\substack{F\subset L \\ F/K \text{ finite}}} \mathrm{Gal}(k_F/k)$. But $k_F = k$ for all F/K finite subextensions, so we get the desired isomorphism. But we have a bijection between $\{F/K \text{ finite}, F \subset K\}$ and $\{k'/k \text{ finite}, k' \subset k_L\}$, which means our restriction map is an isomorphism. □

If L_1/K and L_2/K are finite unramified extensions, then example sheet 3 shows that L_1L_2/K is unramified. Thus for any L/K, we can define a maximal unramified subextension K_0/K.

Now let L/K be any Galois extension. We can show that there exists a surjective map

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

Here we define $I_{L/K} = \ker(\mathrm{res})$ to be the **inertia subgroup**.

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

Definition 17.2. Let L/K be a Galois extension. The **Weil group** $W(L/K) \subset \mathrm{Gal}(L/K)$ is

$$\mathrm{res}^{-1}(\langle \mathrm{Fr}_{k_L/k} \rangle).$$

Remark. If k_L/k is finite, then $W(L/K) = \mathrm{Gal}(L/K)$ (since then the subgroup is cyclic and generated by $\mathrm{Fr}_{k_L/k}$).

Another way to think of this is through a commutative diagram with exact rows:

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

However, the most important property of $W(L/K)$ is its topology. For this, endow $W(L/K)$ with the weakest topology such that:

(i) $W(L/K)$ is a topological group, i.e. a group with a topology such that the multiplication and inversion maps are continuous.

(ii) $I_{L/K}$ is an open subgroup of $W(L/K)$, where $I_{L/K} \subset \mathrm{Gal}(L/K)$ is equipped with the subspace topology (which here in fact is equivalent to the profinite topology).

In other words, a basis of open sets of $W(L/K)$ is just the translates of open sets in $I_{L/K}$ by elements in $W(L/K)$.

Warning. If k_L/k is infinite, then this is not the subspace topology on $W(L/K) \subset \mathrm{Gal}(L/K)$. For example, $I_{L/K} \subset W(L/K)$ is open by definition, but $I_{L/K} \subset \mathrm{Gal}(L/K)$ is not open in the subspace topology.

Proposition 17.2. Let L/K be Galois. Then

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

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

(iii) If F/K is a finite Galois subextension, then $\frac{W(L/K)}{W(L/F)} \cong \mathrm{Gal}(F/K)$.

Proof. (i) $W(L/K)$ is dense in $\mathrm{Gal}(L/K) \iff \forall F/K$ a finite Galois subextension, $W(L/K)$ will intersect every coset of $\mathrm{Gal}(L/F) \iff \forall F/K$ finite Galois, $W(L/K)$ surjects onto $\mathrm{Gal}(F/K)$. For this last result, consider the following commutative diagram with exact rows:

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

We show (a) and (c) are surjective, which will imply that (b) is surjective through a diagram chase.

- For (a), if K_0/K is the maximal unramified extension contained in L, then $K_0 \cap F$ is the maximal unramified extension contained in F. This is because $I_{L/K} = \mathrm{Gal}(L/K_0) \twoheadrightarrow \mathrm{Gal}(FK_0/K_0) \cong \mathrm{Gal}(F/K_0 \cap F)$, but $\mathrm{Gal}(L/K_0)$ also surjects onto $\mathrm{Gal}(F/K_0 \cap F)$, so $\mathrm{Gal}(F/K_0 \cap F) = I_{F/K}$.
- For (c), $\mathrm{Gal}(k_F/k)$ is generated by $\mathrm{Fr}_{k_F/k}$, which implies (c) is surjective.

(ii) Let F/K be a finite subextension and consider the surjective maps

$$\begin{tikzcd}
\mathrm{Gal}(L/K) \arrow[r, two heads] & \mathrm{Gal}(k_L/k) \arrow[r, phantom, "\supset"] & \langle \mathrm{Fr}_{k_L/k} \rangle \\
\mathrm{Gal}(L/F) \arrow[u, hook] \arrow[r, two heads] & \mathrm{Gal}(k_L/k_F) \arrow[u, hook] \arrow[r, phantom, "\supset"] & \langle \mathrm{Fr}_{k_L/k_F} \rangle \arrow[u, hook]
\end{tikzcd} .$$

For $\sigma \in \mathrm{Gal}(L/F)$, $\sigma \in W(L/F) \iff \sigma|_{k_L} \in \langle \mathrm{Fr}_{k_L/k_F} \rangle \overset{(\star)}{\iff} \sigma|_{k_L} \in \langle \mathrm{Fr}_{k_L/k} \rangle \iff \sigma \in W(L/K)$, where the second equivalence $(\star)$ follows as $\mathrm{Gal}(k_L/k_F) \cap \langle \mathrm{Fr}_{k_L/k} \rangle = \langle \mathrm{Fr}_{k_L/k_F} \rangle$.

(iii) As quotients,

$$\frac{W(L/F)}{W(L/K)} \overset{\text{(ii)}}{\cong} \frac{W(L/K)}{W(L/K) \cap \mathrm{Gal}(L/F)} = \frac{W(L/K)\mathrm{Gal}(L/F)}{\mathrm{Gal(L/F)}} \overset{\text{(i)}}{\cong} \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)} \cong \mathrm{Gal}(F/K).$$

□

20 Nov 2022,
Lecture 20

Let K be a local field.

Definition 17.3. Let K be a local field. An extension L/K is **abelian** if it is Galois and $\mathrm{Gal}(L/K)$ is an abelian group.

Facts. Let L_1/K and L_2/K be abelian. Then:

(i) L_1L_2/K is abelian.

(ii) If $L_1 \cap L_2 = K$, then there exists a canonical isomorphism $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Note that (i) implies that there exists a maximal abelian extension K^{ab} of K.

Example 17.1. Let K^{ur} denote the maximal unramified extension of K inside K^{sep} (the separable closure of K). Then $K^{\mathrm{ur}} = \bigcup_{m=1}^{\infty} K(\zeta_{q^m-1})$ (for $q = |k|$). Also note that $k_{K^{\mathrm{ur}}} = \overline{\mathbb{F}_q}$.

We know that for unramified extensions, $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$, so this extension is abelian. Also note that $\mathrm{Fr}_{\overline{\mathbb{F}_q}/\mathbb{F}_q} \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, which corresponds to $\mathrm{Fr}_{K^{\mathrm{ur}}/K}$. Hence K^{ur} is abelian and $K^{\mathrm{ur}} \subset K^{\mathrm{ab}}$. This gives us an exact sequence

$$0 \to I_{K^{\mathrm{ab}}/K} \to W(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathbb{Z} = \langle \mathrm{Fr}_{K^{\mathrm{ab}}/K} \rangle \to 0.$$

Theorem 17.3. (i) (Local Artin reciprocity). For K a local field, there exists a unique topological isomorphism (i.e. a group isomorphism and a homomorphism) $\mathrm{Art}_K : K^\times \to W(K^{\mathrm{ab}}/K)$ satisfying:

- $\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Fr}_{K^{\mathrm{ur}}/K}$ for any uniformizer π of K.
- For each finite subextension L/K inside K^{ab}/K, $\mathrm{Art}_K(N_{L/K}(L^\times))|_L = \{1\}$.

Art_K is called the **Artin map** or the **Artin reciprocity map**.

(ii) Let L/K be a finite abelian extension. Then Art_K induces an isomorphism $K^\times/N_{L/K}(L^\times) \cong \frac{W(K^{\mathrm{ab}}/K)}{W(K^{\mathrm{ab}}/L)} \cong \mathrm{Gal}(L/K)$ (as quotients).

Properties of the Artin map:

- (Existence theorem). For $H \subset K^\times$ an open finite index subgroup, there exists a finite abelian extension L/K such that $N_{L/K}(L^\times) = H$. In particular, Art_K induces an (inclusing reversing) isomorphism of posets $\{\text{open finite index subgroups of } K^\times\} \leftrightarrow \{\text{finite abelian extensions } L/K\}$, given by $H \mapsto (K^{\mathrm{ab}})^{\mathrm{Art}_K(H)}$ (the fixed field) and $N_{L/K}(L^\times) \leftarrow\!\shortmid L/K$.
- (Norm functoriality). Let L/K be a finite separable extension. Then we have the commutative diagram

$$\begin{tikzcd} L^\times \arrow[r, "\mathrm{Art}_L"] \arrow[d, "N_{L/K}"] & W(L^{\mathrm{ab}}/L) \arrow[d, "\mathrm{res}"] \\ K^\times \arrow[r, "\mathrm{Art}_K"] & W(K^{\mathrm{ab}}/K) \end{tikzcd}.$$

The rest of the course is now focused the construction of the Artin map.

Proposition 17.4. If L/K is finite abelian extension of degree n, then $e_{L/K} = [\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$.

Proof. Given $x \in L^\times$, we have $v_K(N_{L/K}(x)) = f_{L/K}v_L(x)$. This implies that we have a surjection $K^\times/N_{L/K}(L^\times) \overset{v_K}{\to} \mathbb{Z}/f_{L/K}\mathbb{Z}$ with kernel $\frac{\mathcal{O}_K^\times N_{L/K}(L^\times)}{N_{L/K}(L^\times)} \cong \frac{\mathcal{O}_K^\times}{\mathcal{O}_K^\times \cap N_{L/K}(L^\times)} \cong \frac{\mathcal{O}_K^\times}{N_{L/K}(\mathcal{O}_L^\times)}$. By Theorem 17.3 (ii), $n = [K^\times : N_{L/K}(L^\times)] = f_{L/K}[\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$. To finish, use the fact that $n = e_{L/K}f_{L/K}$. □

Corollary 17.5. Let L/K be finite abelian. Then L/K is unramified $\iff$ $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$.

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

Recall that $\mathbb{Q}_p^{\mathrm{ur}} = \bigcup_{m=1}^\infty \mathbb{Q}_p(\zeta_{p^m-1}) = \bigcup_{p\nmid m} \mathbb{Q}_p(\zeta_m)$. On the other hand, $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$ with $\theta_n : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \overset{\sim}{\to} (\mathbb{Z}/p^n\mathbb{Z})^\times$.

For $n \geq m \geq 1$, there exists a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \arrow[r, two heads] \arrow[d, "\theta_n"] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) \arrow[d, "\theta_m"] \\
(\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r, "\text{canonical}\\ \text{projection}"] & (\mathbb{Z}/p^m\mathbb{Z})^\times
\end{tikzcd}$$

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

$$\theta : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \overset{(\star)}{\cong} \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$$

with $(\star)$ following from example sheet 4.

We have $\mathbb{Q}_p(\zeta_{p^\infty}) \cap \mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p$, since the first extension is totally ramified and the second is unramified. Hence there exists an isomorphism $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$.

Theorem 17.6 (Local Kronecker–Weber)**.** $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{ur}}\mathbb{Q}_p(\zeta_{p^\infty})$.

Proof. Omitted in this course. □

Assuming this theorem, we can construct the Artin map as follows: We have $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$ by $(n, u) \mapsto p^n u$. Then let

$$\mathrm{Art}_{\mathbb{Q}_p}(p^n u) = (\mathrm{Fr}^n_{K^{\mathrm{ur}}/K}, \theta^{-1}(u^{-1}))$$

with the first element lying inside $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p$ and we can check that the image of this map lies inside $W(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$.

17.2 Construction of Art_K

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

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

(ii) For $n \geq m \geq 1$, there exists a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(K_{\pi,n}/K) \arrow[r, two heads] \arrow[d, "\Psi_n"] & \mathrm{Gal}(K_{\pi,m}/K) \arrow[d, "\Psi_m"] \\
\mathcal{O}_K^\times/U_k^{(n)} \arrow[r, two heads] & \mathcal{O}_K^\times/U_k^{(m)}
\end{tikzcd}$$

with the vertical arrows being isomorphisms.

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

Once we have this, we can define the Artin map: (ii) implies that there exists an isomorphism $\Psi : \text{Gal}(K_{\pi,\infty}/K) \overset{\sim}{\to} \mathcal{O}_K^\times$, and now define Art_K by

$$\begin{aligned} &K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times \to \text{Gal}(K^{\text{ur}}/K) \times \text{Gal}(K_{\pi,\infty}/K) \cong \text{Gal}(K^{\text{ab}}/K). \\ &p^n u \leftarrow\!\shortmid (n, u) \mapsto (\text{Fr}^n_{K^{\text{ur}}/K}, \Psi^{-1}(u^{-1})). \end{aligned}$$

Our goal now is to construct these $K_{\pi,n}$. 23 Nov 2022, Lecture 21

Remark. There is no maximal totally ramified extension of K. Hence Art_K depends on the choice $K_{\pi,\infty}$, and the isomorphism $K^\times \cong \mathbb{Z}\times\mathcal{O}_K^\times$. These choices are both dependent on the choice of π – they "cancel out" and Art_K is canonical.

18 Lubin–Tate theory

18.1 Formal group laws

Let R be a ring. We denote by $R[[X_1, \dots, X_n]] = \{\sum_{k_1,\dots,k_n \geq 0} a_{k_1\dots,k_n} X^{k_1} \dots X^{k_n} \mid a_{k_1\dots k_n} \in R\}$ the ring of formal power series in variables over R.

Definition 18.1. A (1–dimensional) **formal group law** over R is a power series $F[[X, Y]] \in R[[X, Y]]$ satisfying

1. $F(X, Y) \equiv X + Y \pmod{\deg 2}$ (i.e. modulo X^2, XY, Y^2).
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$ – the associativity axiom.
3. $F(X, Y) = F(Y, X)$.

Example 18.1.

- $\hat{\mathcal{G}}_a = X + Y$. This is called the formal additive group.
- $\hat{\mathcal{G}}_m = X + Y + XY$. This is the formal multiplicative group.

Lemma 18.1. For F a formal group law over R,

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

(ii) There exists a unique power series $i(X) \in XR[[X]]$ with $F(X, i(X)) = 0$.

Proof. Exercise on example sheet 4. □

If K is a non–archimedean valued field and F is a formal group law over $\mathcal{O}_K$, then $F(x, y)$ converges $\forall x, y \in \mathfrak{m}_K$ to an element in $\mathfrak{m}_K$. This allows us to define $x \cdot_F y = F(x, y)$, which turns $(\mathfrak{m}_K, \cdot_F)$ into a commutative group.

Example 18.2. $\hat{\mathcal{G}}_m/\mathbb{Z}_p$, so $x \cdot_{\hat{\mathcal{G}}_m} y = x + y + xy$. Then $(p\mathbb{Z}_p, \hat{\mathcal{G}}_m) \cong (1 + p\mathbb{Z}_p, \times)$ by $x \mapsto 1 + x$.

Definition 18.2. Let F, G be formal group laws over a ring R. A **homomorphism** $f : F \to G$ is an element $f(X) \in XR[[X]]$ such that $f(F(X,Y)) = G(f(X), f(Y))$.

A homomorphism $f : F \to G$ is an **isomorphism** if there exists a homomorphism $g : G \to F$ such that $f(g(X)) = g(f(X)) = X$.

Definition 18.3. We define $\mathrm{End}_R(F)$ to be the set of homomorphisms $f : F \to F$.

Proposition 18.2. Let R be a $\mathbb{Q}$–algebra. Then there is an isomorphism of formal group laws $\exp : \hat{\mathcal{G}}_a \to \hat{\mathcal{G}}_m$ given by $\exp(X) = \sum_{n=1}^{\infty} \frac{X^n}{n!}$ (notice that the constant term is missing).

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

Note that we need R to be a $\mathbb{Q}$–algebra for $\frac{1}{n!}$ to make sense. An exercise on example sheet 4 shows that if we replace R with a field of positive characteristic then there are no nontrivial homomorphisms between the additive group and the multiplicative group.

Lemma 18.3. $\mathrm{End}_R(F)$ is a ring with addition $(f +_F g) = F(f(X), g(X))$ and multiplication given by composition.

Proof. For $f, g \in \mathrm{End}_R(F)$, we have

$$\begin{aligned}
&(f +_F g) \circ F(X,Y) = F(f(F(X,Y)), g(F(X,Y))) \\
&= F(F(f(X), f(Y)), F(g(X), g(Y))) \\
&\overset{(\star)}{=} F(F(f(X), g(X)), F(f(Y), g(Y))) \\
&= F(f +_F g(X), f +_F g(Y)) \\
\implies &f +_F g \in \mathrm{End}_R(F),
\end{aligned}$$

where $(\star)$ follows by associativity and commutativity axioms.

Also $f \circ g \circ F = f \circ F \circ g = F \circ f \circ g$, so $f \circ g \in \mathrm{End}_R(F)$. The ring axioms are left as an exercise. □

18.2 Lubin–Tate formal groups

Let K be a non–archimedean local field with residue field k of size q.

Definition 18.4. 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 $[\ ]_F : \mathcal{O}_K \to$

$\mathrm{End}_{\mathcal{O}_K}(F)$ such that $\forall a \in \mathcal{O}_K, [a]_F(X) \equiv aX \pmod{X^2}$ (i.e. modulo degree 2 terms).

A **homomorphism/isomorphism** of $f : F \to G$ of formal $\mathcal{O}_K$–modules s a homomorphism/isomorphism of formal group laws such that $f \circ [a]_F = [a]_G \circ f$ $\forall a \in \mathcal{O}_K$.

Definition 18.5. 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) $f(X) \equiv \pi X \pmod{X^2}$.

(ii) $f(X) \equiv X^q \pmod{\pi}$.

Example 18.3. $\pi X + X^q$ is a Lubin–Tate series.

Theorem 18.4. Let $f(X)$ be a Lubin–Tate series for π. Then

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

(ii) There exists a ring homomorphism $[\ ]_{F_f} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F_f)$ satisfying $[\pi]_{F_f}(X) = f(X)$ 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 called the **Lubin–Tate formal group law for** π (which by (iii) only depends on π up to isomorphism).

26 Nov 2022, Lecture 22

Example 18.4. If $K = \mathbb{Q}_p$, then $f(X) = (X+1)^p - 1$ is a Lubin–Tate series for (the uniformizer) p. The Lubin–Tate formal group law in this case is $\hat{\mathcal{G}}_m$. For this, it suffices to show that $f \circ \hat{\mathcal{G}}_m = \hat{\mathcal{G}}_m \circ f$, but we compute

$$f \circ \hat{\mathcal{G}}_m(X,Y) = (1+X)^p(1+Y)^p - 1 = \hat{\mathcal{G}}_m(f(X), f(Y))$$

using $\hat{\mathcal{G}}_m(X,Y) = (1+X)(1+Y) - 1$.

The key to the proof of Theorem 18.4 is the following lemma:

Lemma 18.5. Let $f(X), g(X)$ be Lubin–Tate series for π and $L(X_1, \dots, X_n) = \sum_{i=1}^n a_i X_i$ with $a_i \in \mathcal{O}_K$. Then there exists a unique power series $F(X_1, \dots, X_n) \in \mathcal{O}_K[[X_1, \dots, X_n]]$ such that

(i) $F(X_1, \dots, X_n) \equiv L(X_1, \dots, X_n)$ (mod deg 2)

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

Proof. We show by induction that there exist unique polynomials $F_m \in \mathcal{O}_K[X_1, \dots, X_m]$ of total degree $\leq m$ satisfying:

(a) $f(F_m(X_1, \dots, X_n)) \equiv F_m(g(X_1), \dots, g(X_n)) \pmod{\deg m+1}$.

(b) $F_m(X_1, \dots, X_n) \equiv L(X_1, \dots, X_n) \pmod{\deg 2}$.

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

For $m = 1$, take $F_1 = L$. It satisfies property (b), and (a) follows from the fact that $f(F(X_1, \dots, X_n)) \overset{(\star)}{\equiv} \pi L(X_1, \dots, X_n) \equiv F(g(X_1), \dots, g(X_n))$ (mod deg 2), where ($\star$) follows as $f(X) \equiv \pi X \pmod{X^2}$.

Now suppose we've constructed F_m for some $m \geq 1$. We set $F_{m+1} = F_m + h$ for $h \in \mathcal{O}_K[X_1, \dots, X_n]$ homogeneous of degree $m + 1$. Since $f(X + Y) = f(X) + f'(X)Y + Y^2(\dots)$ and $f'(X) \equiv \pi \pmod{X}$, we have

$$f \circ (F_m + h) = f \circ F_m + \pi h \pmod{\deg m+2}.$$

Similarly $(F_m+h) \circ g \overset{(\star)}{\equiv} F_m \circ g + h(\pi X_1, \dots, \pi X_n) \equiv F_m \circ g + \pi^{m+1} h(X_1, \dots, X_n)$ (mod deg $m + 2$) where ($\star$) follows from $g(X) \equiv \pi X \pmod{X^2}$. Thus (a), (b), (c) will be satisfied if and only if

$$f \circ F_m - F_m \circ g \equiv (\pi - \pi^{m+1})h \pmod{\deg m+2}.$$

But using the fact that $f(X) \equiv g(X) \equiv X^q \pmod{\pi}$, we find

$$f \circ F_m - F_m \circ g \equiv F_m(X_1, \dots, X_n)^q - F_m(X_1^q, \dots, X_n^q) \equiv 0 \pmod{\pi}.$$

Let $r(X_1, \dots, X_n)$ be the degree $m + 1$ terms in $f \circ F_m - F_m \circ g$. Then set $h = \frac{1}{\pi(1-\pi^m)} r \in \mathcal{O}_K[X_1, \dots, X_n]$, so our computations show F_{m+1} satifies (a), (b), (c). This is unique, since h is determined by (a).

Set $F = \lim_{m\to\infty} F_m$, so $F(X_1, \dots, X_n) \in \mathcal{O}_K[[X_1, \dots, X_n]]$ and F satisfies properties (i) and (ii). The uniqueness of F follows from the uniqueness of the F_m, as truncating the power series F needs to give F_m. □

Proof of Theorem 18.4. (i) By Lemma 18.5, there exists a unique $F_f(X, Y) \in \mathcal{O}_K[[X, Y]]$ such that

- $F(X, Y) \equiv X + Y \pmod{\deg 2}$.
- $f(F_f(X, Y)) = F_f(f(X), f(Y))$.

We need to check that F_f is a formal group law.

- Associativity: $F_f(X, F_f(Y, Z)) \equiv X + Y + Z \equiv F_f(F_f(X, Y), Z)$ (mod deg 2) and $f \circ F_f(X, F_f(Y, Z)) = F_f(f(X), f(F_f(Y, Z))) = F_f(f(X), F_f(f(Y), F(Z)))$. Similarly we find $f \circ F_f(F_f(X, Y), Z) = F_f(F_f(f(X), f(Y)), f(Z))$. By uniqueness in Lemma 18.5, we have $F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$.

- Commutativity: analogously check that the two power series are equal, have the same linear terms and are both compatible with the Lubin–Tate series.

(ii) By Lemma 18.5, for $a \in \mathcal{O}_K$ there exists a unique $[a]_{F_f} \in \mathcal{O}_K[[X]]$ such that $[a]_{F_f} \equiv aX \pmod{X^2}$ and $f \circ [a]_{F_f} = [a]_{F_f} \circ f$. Then $[a]_{F_f} \circ F_f = F_f \circ [a]_{F_f}$ by uniqueness, i.e. $[a]_{F_f} \in \mathrm{End}_{\mathcal{O}_K}(F_f)$. The map $[\ ]_{F_f} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F_f)$ is a ring homomorphism (again by uniqueness). This implies that F_f is a formal $\mathcal{O}_K-$-module over $\mathcal{O}_K$. The fact that $[\pi]_{F_f} = f$ follows by uniqueness again.

(iii) If $g(X)$ is another Lubin–Tate series for π, then let $\theta(X) \in \mathcal{O}_K[[X]]$ such that

- $\theta(X) \equiv X \pmod{X^2}$
- $\theta \circ f(X) = g \circ \theta(X)$.

Then $\theta \circ F_f = F_g \circ \theta$ (by uniqueness again), so $\theta \in \mathrm{Hom}(F_f, F_g)$. Reversing the roles of f and g we obtain $\theta^{-1} \in \mathcal{O}_K[[X]]$ such that $\theta^{-1} \in \mathrm{Hom}(F_g, F_f)$. Then $\theta \circ \theta^{-1}(X) = X = \theta^{-1} \circ \theta(X)$ (by uniqueness in Lemma 18.5). Finally, uniqueness implies that $\theta \circ [a]_{F_f} = [a]_{F_g} \circ \theta \ \forall a \in \mathcal{O}_K$, so θ is an isomorphism of $\mathcal{O}_K$–modules.

□

18.3 Lubin–Tate extensions

Let $\overline{K}$ be a separable closure of K and $\overline{\mathfrak{m}} \subset \mathcal{O}_{\overline{K}}$ the maximal ideal.

Lemma 18.6. Let F be a formal $\mathcal{O}_K$–module over $\mathcal{O}_K$. Then $\overline{\mathfrak{m}}$ becomes a (genuine) $\mathcal{O}_K$–module with operations $x +_F y = F(x, y)$ for $x, y \in \overline{\mathfrak{m}}$ and $a \cdot_F x = [a]_F(x)$ for $a \in \mathcal{O}_K, x \in \overline{\mathfrak{m}}$.

Proof. We can't apply the argument directly to $\overline{K}$, as it is not complete. Instead, $x \in \overline{\mathfrak{m}} \implies x \in \mathfrak{m}_L$ for some L/K finite. Then $[a]_F \in \mathcal{O}_K[[X]] \implies [a]_F(x)$ converges in L and since $\mathfrak{m}_L$ is closed, $[a]_F(x) \in \mathfrak{m}_L \subset \overline{\mathfrak{m}}$.

Similarly $x +_F y \in \overline{\mathfrak{m}}$.

The module structure follows from definitions. □