Local Fields

Daniel Naylor

November 29, 2024

Contents

Lecture 1

Part I

Basic Theory

Example. $f(x_1, \ldots, x_r) \in \mathbb{Z}[c_1, \ldots, x_r]$, $f(x_1, \ldots, x_r) = 0$? This is hard to study. It is easier to study

$$f(x_1, \ldots, x_r) \equiv 0 \pmod{p}$$
$$f(x_1, \ldots, x_r) \equiv 0 \pmod{p^2}$$
$$\vdots$$
$$f(x_1, \ldots, x_r) \equiv 0 \pmod{p^n}$$

A local field packages all this information together.

1 Absolute values

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

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

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

(iii) $|x + y| \leq |x| + |y|$ $\forall x, y \in K$ (triangly inequality).

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

Example.

- $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with usual absolute value $|a + ib| = \sqrt{a^2 + b^2}$. Write $|\bullet|_\infty$ for this absolute value.
- K any field. The trivial absolute value is

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

  Although this is technically an absolute value, it is not useful or interesting, so should be ignored.

Definition 1.2 (p-adic absolute value)**.** Let $K = \mathbb{Q}$, and p be a prime. For $0 \neq x \in \mathbb{Q}$, write $x = p^n \frac{a}{b}$, where $(a, p) = 1$, $(b, p) = 1$. The *p-adic absolute value* is defined to be

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

Verification:

(i) Clear

(ii) Write $y = p^m \frac{c}{d}$. Then

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

(iii) Without loss of generality, $m \geq n$. Then

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

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

Definition 1.3 (Place)**.** Let $|\bullet|$, $|\bullet|'$ be absolute values on a field K. We say $|\bullet|$ and $|\bullet|'$ are *equivalent* if they induce the same topology. An equivalence class of absolute values is called a *place*.

Proposition 1.4. Assuming that:

- $|\bullet|$, $|\bullet|'$ are (non-trivial) absolute values on K.

Then the following are equivalent:

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

(ii) $|x| < 1 \iff |\bullet|' < 1$ for all $x \in K$.

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

Proof.

(i) $\implies$ (ii)

$$\begin{aligned} |x| < 1 &\iff x^n \to 0 \text{ w.r.t } |\bullet| \\ &\iff x^n \to 0 \text{ w.r.t } |\bullet|' \\ &\iff |x|' < 1 \end{aligned}$$

(ii) $\implies$ (iii) Note: $|x|^c = |x|' \iff c \log|x| = \log|x|'$. Let $a \in K^\times$ such that $|a| > 1$ (exists since $|\bullet|$ is non-trivial). We need that $\forall x \in K^\times$,

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

Assume that

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

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

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

Then we have

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

Hence $\left|\frac{x^n}{a^m}\right| < 1$ and $\left|\frac{x^n}{a^m}\right| > 1$, contradiction. Similarly for the case where

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

(iii) $\implies$ (i) Clear.

$\square$

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

$$|x+y|^\beta \le |x|^\beta + |y|^\beta$$

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

Definition 1.5 (Non-archimedean)**.** An absolute value $|\bullet|$ on K is said to be *non-archimedean* if it satisfies the ultrametric inequality:

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

If $|\bullet|$ is not non-archimedean, then it is archimedean.

Example.

- $|\bullet|_\infty$ on $\mathbb{R}$ is archimedean.
- $|\bullet|_p$ is a non-archimedean absolute value.

Lemma 1.6. Assuming that:

- $(K, |\bullet|)$ is non-archimedean
- $x, y \in K$
- $|x| < |y|$

Then $|x-y| = |y|$.

Proof.

$$|x-y| \le \max(|x|, |y|) = |y|$$

and

$$|y| \le \max(|x|, |x-y|) \le |x-y|.$$

$\square$

Proposition 1.7. Assuming that:

- $(K, |\bullet|)$ is non-archimedean

- $(x_n)_{n=1}^{\infty}$ a sequence in K
- $|x_n - x_{n+1}| \to 0$

Then $(x_n)_{n=1}^{\infty}$ is Cauchy. In particular, if K is in addition complete, then $(x_n)_{n=1}^{\infty}$ converges.

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

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

The "In particular" is clear. □

Example. $p = 5$, construct sequence $(x_n)_{n=1}^{\infty}$ in $\mathbb{Z}$ such that

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

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

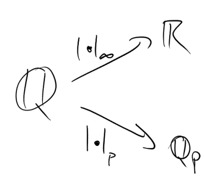
Take $x_1 = 2$. Suppose we have constructed x_n. Let $x_n^2 + 1 = a5^n$ and set $x_{n+1} = x_n + b5^n$. Then

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

We choose b such that $a + 2bx_n \equiv 0 \pmod 5$. Then we have $x_{n+1}^2 + 1 \equiv 0 \pmod{5^{n+1}}$. Now (ii) implies that $(x_n)_{n=1}^{\infty}$ is Cauchy. Suppose $x_n \to l \in \mathbb{Q}$. Then $x_n^2 \to l^2$. But (i) tells us that $x_n^2 \to -1$, so $l^2 = -1$, a contradiction. Thus $(\mathbb{Q}, |\bullet|_5)$ is not complete.

Definition 1.8. The p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\bullet|_p$.

Analogy with $\mathbb{R}$:



Lecture 2

Notation. As is usual when working with metric spaces, we will be using the notation:

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

Lemma 1.9. Assuming that:

- $(K, |\bullet|)$ is a non-archimedean valued field

Then

(i) If $z \in B(x, r)$, then $B(z, r) = B(x, r)$ – so open balls don't have a centre.

(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 $|x - y| < r$ hence

$$\begin{aligned} |z - y| &= |(z - x) + (x - y)| \\ &\leq \max(|z - x|, |x - y|) \\ &< r \end{aligned}$$

Thus $B(x, r) \subseteq B(z, r)$. $\supseteq$ follows by symmetry.

(ii) Same as (i).

(iii) Let $y \notin B(x, r)$. If $z \in B(x, r) \cap B(y, r)$ then $B(x, r) = B(z, r) = B(y, r)$ Hence $y \in B(x, r)$. Hence $B(x, r) \cap B(y, r) = \emptyset$.

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

2 Valuation Rings

Definition 2.1 (Valuation)**.** 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 determines a valuation $v(x) = \log_\alpha |x|$.

Remark.

- Ignore the trivial valuation $v(x) = 0$.
- Say v_1, v_2 are equivalent if there exists $c \in \mathbb{R} > 0$ such that $v_1(x) = cv_2(x)$ for all $x \in K^\times$.

Example.

- $K = \mathbb{Q}$, $v_p(x) = -\log_p |x|_p$ is known as the p-adic valuation.
- If k is a field, consider $K = k(t) = \mathrm{Frac}(k[t])$ the rational function field. Then define

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

for $f, g \in k[t]$ with $f(0), g(0) \neq 0$. We call this the t-adic valuation.

- $K = k((t)) = \mathrm{Frac}(k[[t]]) = \left\{\sum_{i=n}^{\infty} a_i t^i \mid a_i \in k, n \in \mathbb{Z}\right\}$, known as the field of formal Laurent series over k. Then we can define

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

is the t-adic valuation on K.

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

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

Proposition 2.3.

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

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

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

Proof.

(i) $|0| = 0$, $|1| = 1$ so $0, 1 \in \mathcal{O}_K$. If $x \in \mathcal{O}_K$, then $|-x| = |x|$ hence $-x \in \mathcal{O}_K$. If $x, y \in \mathcal{O}_K$, then

$$|x + y| \le \max(|x|, |y|) \le 1.$$

Hence $x + y \in \mathcal{O}_K$. If $x, y \in \mathcal{O}_K$, then $|xy| = |x| |y| \le 1$, hence $xy \in \mathcal{O}_K$. Thus $\mathcal{O}_K$ is a ring. Since $\mathcal{O}_K = \overline{B}(0,1)$, it is open.

(ii) Similar to (i).

(iii) Note that $|x| \left|x^{-1}\right| = \left|xx^{-1}\right| = 1$. Thus

$$\begin{aligned} |x| = 1 &\iff \left|x^{-1}\right| = 1 \\ &\iff x, x^{-1} \in \mathcal{O}_K \\ &\iff x \in \mathcal{O}_K^\times \end{aligned}$$

□

Notation.

- $m := \{x \in \mathcal{O}_K \mid |x| < 1\}$ is a max ideal of $\mathcal{O}_K$.
- $k := \mathcal{O}_K / m$ is the *residue field*.

Corollary 2.4. $\mathcal{O}_K$ is a local ring with unique maximal ideal m (a local ring is a ring with a unique maximal ideal).

Proof. Let m' be a maximal ideal. Suppose $m' \ne m$. Then there exists $x \in m' \setminus m$. Using part (iii) of Proposition 2.3, we get that x is a unit, hence $m' = \mathcal{O}_K$, a contradiction. □

Example. $K = \mathbb{Q}$ with $|\bullet|_p$. Then

$$\mathcal{O}_K = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \middle| p \nmid b \right\},$$

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

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

Example.
- $K = \mathbb{Q}$ with p-adic valuation is a discrete valuation ring.
- $K = k(t)$ with t-adic valuation is a discrete valuation ring.
- $K = k(t)(t^{1/2}, t^{1/4}, t1/8, \dots)$. Here, the t-adic valuation is not discrete.

Remark. If v is a discrete valuation, can replace with equivalent one such that $v(K^\times) = \mathbb{Z}>$ Call such a v *normalised valuations* (then $v(\pi) = 1$ if and only if π is a unit).

Lemma 2.6. Assuming that:

- v is 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) m is principal

Proof.

(i) $\implies$ (ii) $\mathcal{O}_K$ is an integral domain since it is a subset of K, which is an integral domain. Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Let $x \in I$ such that $v(x) = \min\{v(a) \mid a \in I\}$, which exists since v is discrete. Then we claim

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

is equal to I.

$\subseteq$ (I is an ideal)

$\supseteq$ Let $y \in I$. Then $v(x^{-1}y) \geq 0$. Hence $y = x(x^{-1}y) \in x\mathcal{O}_K$.

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

(iii) $\implies$ (iv) Write $m = x_1\mathcal{O}_K + \cdots + x_n\mathcal{O}_K$. Without loss of generality,

$$v(x_1) \leq v(x_2) \leq \cdots \leq v(x_n).$$

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

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

Lecture 3

Suppose v is a discrete valuation on K, $\pi \in \mathcal{O}_K$ a uniformiser. For $x \in K^\times$, let $n \in \mathbb{Z}$ such that $v(x) = nv(\pi)$. Then $u = \pi^{-n}x \in \mathcal{O}_K^\times$ 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 2.7 (Discrete valuation ring)**.** A ring R is called a *discrete valuation ring* (DVR) if it is a PID with exactly one non-zero prime ideal (necessarily maximal).

Lemma 2.8.

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

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

Proof.

(i) $\mathcal{O}_K$ is a PID by Lemma 2.6. Hence any non-zero prime ideal is maximal and hence $\mathcal{O}_K$ is a discrete valuation ring since it is a local ring.

(ii) Let R be a discrete valuation ring, with maximal ideal m. Then $m = (\pi)$ for some $\pi \in R$. Since PIDs are UFDs, we may write any $x \in R \setminus \{0\}$ uniquely as $\pi^n u$ with $n \geq 0$, $u \in R^\times$. Then any $y \in K^\times$ can be written uniquely as $\pi^m u$ with $u \in R^\times$, $m \in \mathbb{Z}$. Define $v(\pi^m u) = m$; check v is a valuation and $\mathcal{O}_K = R$. □

Example. $\mathbb{Z}_{(p)}$, $k[[t]]$ (k a field) are discrete valuation rings.

3 The p-adic numbers

Recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\bullet|_p$. On Example Sheet 1, we will show that $\mathbb{Q}_p$ is a field. We also show that $|\bullet|_p$ extends to $\mathbb{Q}_p$ and the associated valuation is discrete.

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

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

Facts: $\mathbb{Z}_p$ is a discrete valuation ring, with maximal ideal $p\mathbb{Z}_p$, and non-zero ideals are given by $p^n\mathbb{Z}_p$.

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

Proof. Need to show $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Note $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Since $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is open, we have that $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$. Now:

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

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

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

In particular, $\mathbb{Z}_p$ is complete and $\mathbb{Z} \subseteq \mathbb{Z}_p$ is dense. □

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

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

Define the group / ring operation componentwise.

Notation. 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 (Universal property of inverse limits)**.** Assuming that:

- B is a set / group / ring
- ψ_n are homomorphisms $\psi_n : B \to A_n$ such that

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

  commutes for all n

Then there exists a unique homomorphism $\psi : B \to \varprojlim_{n} A_n$ such that $\theta_n \circ \psi = \psi_n$.

Proof. Define

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

Then $\psi_n = \varphi_n \circ \psi_{n+1}$ implies that $\psi(b) \in \varprojlim_{n} A_n$. The map is clearly unique (determined by $\psi_n = \theta_n \circ \psi$) and is a homomorphism of sets / groups / rings. □

Definition 3.3 (I-adic completion)**.** Let $I \subseteq R$ be an ideal (R a ring). The I-adic completion of R is the

$$\hat{R} := \varprojlim_{R} / I^n$$

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 of inverse limits (there exist maps $R \to R/I^n$). We say R is *I-adically complete* if it is an isomorphism.

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

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

Proposition 3.4. Assuming that:

- K is complete with respect to $| \bullet |$

Then

(i) Then $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ ($\mathcal{O}_K$ is π-adically complete)

(ii) Every $x \in \mathcal{O}_K$ can be written uniquely as $x = \sum_{i=0}^{n} a_i\pi^i$, $a_i \in A$, where $A \subseteq \mathcal{O}_K$ is a set of coset representatives for $\mathcal{O}_K/\pi\mathcal{O}_K$.

Proof.

(i) K is complete and $\mathcal{O}_K$ is closed, so $\mathcal{O}_K$ is complete.
$x \in \bigcap_{n=1}^{\infty} \pi^n\mathcal{O}_K$ impies $v(x) \geq nv(\pi)$ for all n, and hence $x = 0$. Hence $\mathcal{O}_K \to \varprojlim_{\mathcal{O}} K/\pi^n\mathcal{O}_K$ is injective.
Let $(x_n)_{n=1}^{\infty} \in \varprojlim_{\mathcal{O}} K/\pi^n\mathcal{O}_K$ and for each n, let $y_n \in \mathcal{O}_K$ be a lifting of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$. Then $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$ so that $v(y_n - y_{n+1}) \geq nv(\pi)$.
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 the $\varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$. Thus $\mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ is surjective.

(ii) Exercise on Example Sheet 1. □

Corollary 3.5.

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

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

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

with $n \in \mathbb{Z}$, $a_i \in \{0, 1, \ldots, -1\}$.

Lecture 4

Proof.

(i) It suffices by Proposition 3.4 to show that

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

Let $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map

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

hence $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is injective.

Let $\tau \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ and let $c \in \mathbb{Z}_p$ be a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there exists $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$ is open in $\mathbb{Z}_p$. Then $f_n(x) = \tau$, hence $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective.

(ii) It follows from Proposition 3.4(ii) to $p^{-n}x \in \mathbb{Z}_p$ for some $n \in \mathbb{Z}$ □

Example.

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \cdots$$

Part II

Complete Valued Fields

4 Hensel's Lemma

Theorem 4.1 (Hensel's Lemma version 1)**.** Assuming that:

- $(K, |\bullet|)$ is a complete discretely valued field
- $f(X) \in \mathcal{O}_K[X]$
- assume $\exists a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$

Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $|x - a| < |f'(a)|$.

Proof. Let $\pi \in \mathcal{O}_K$ be a uniformiser and let $r = v(f'(a))$, with v the normalised valuation ($v(\pi) = 1$). We construct a sequence $(x_n)_{n=1}^{\infty}$ 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 $x_1 = a$: then $f(x_1) \equiv 0 \pmod{\pi 1 + 2r}$.

Now we suppose we have constructed $x_1, \dots, x_n$ satisfying (i) and (ii). Define

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

Since $x_n \equiv x_1 \pmod{\pi^{r+1}}$, we have

$$v(f'(x_n)) = v(f'(x_i)) = r,$$

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 letting X, Y be indeterminates, we have

$$f(X + Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \cdots,$$

where $f_i(X) \in \mathcal{O}_K[X]$ and $f_0(X) = f(X)$, $f_1(X) = f'(X)$. Thus

$$f(x_{n+1}) = f(x_n) + cf'(x_n) + c^2 f_2(x_N) + \underbrace{c^2 f_2(x_n) + \cdots}_{\in \pi^{n+2r+1}}$$

where $c = -\frac{f(x_n)}{f'(x_n)}$.

Since $c \equiv 0 \pmod{\pi^{n+r}}$ and $v(f_i(x_n)) \geq 0$ we have

$$f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \pmod{\pi^{n+2r+1}},$$

so (i) holds.

Property (ii) implies that $(x_n)_{n=1}^{\infty}$ is Cauchy, so let $x \in \mathcal{O}_K$ such that $x_n \to x$. Then $f(x) = \lim_{n\to\infty} f(x_n) = 0$ by (i).

Moreover, (ii) impies that

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

This proves existence.

Uniqueness: suppose x' also satisfies $f'(x) = 0$, $|x'-a| < |f'(a)|$. Set $\delta = x' - x \neq 0$. Then

$$|x'-a| < |f'(a)| \qquad |x-a'| < |f'(a)|,$$

and the ultrametric inequality implies

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

But

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

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

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

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

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

Corollary 4.3.

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

Proof. **Case** $p > 2$**:** Let $b \in {\mathbb{Z}_p}^\times$. Applying to $f(X) = X^2 - b$, we find that $b \in ({\mathbb{Z}_p}^\times)^2$ if and only if $b \in (\mathbb{F}_p^\times)^2$. Thus ${\mathbb{Z}_p}^\times/({\mathbb{Z}_p}^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$ ($\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$).

We have an isomorphism

$$ {\mathbb{Z}_p}^\times \times (\mathbb{Z}, +) \cong {\mathbb{Q}_p}^\times $$

given by $(u, n) \mapsto up^n$. Thus

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

Case $p = 2$**:** Let $b \in \mathbb{Z}_2^\times$. Consider $f(X) = X^2 - b$. Note $f'(X) = 2X \equiv 0 \pmod 2$. Let $b \equiv 1 \pmod 8$. Then

$$ |f(1)| = 2^{-3} < 2^{-2} = |f'(1)|^2. $$

Hensel's Lemma version 1 gives

$$ b \in (\mathbb{Z}_2^\times)^2 \iff b \equiv 1 \pmod 8. $$

Then

$$ \mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times \equiv (\mathbb{Z}/2\mathbb{Z})^j. $$

Again using $\mathbb{Q}_2^\times \equiv \mathbb{Z}_2^\times \times \mathbb{Z}$, we find that $\mathbb{Q}_2^\times \cong (\mathbb{Z}/2\mathbb{Z})^3$. □

Remark. Proof uses the iteration

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

which is the non-archimedean analogue of the unewton Raphson method.

Theorem 4.4 (Hensel's Lemma version 2)**.** Assuming that:

- $(K, |\bullet|)$ is a complete discretely valued field
- $f(X) \in \mathcal{O}_K[X]$

- $\overline{f}(X) := f(X) \pmod{m} \in k[X]$ factorises as $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$ in $k[X]$
- $\overline{g}(X)$ and $\overline{h}(X)$ coprime.

Then there is a factorisation

$$f(X) = g(X)h(X)$$

in $\mathcal{O}_K[X]$, with $\overline{g}(X) \equiv g(X) \pmod{m}$, $\overline{h}(X) \equiv h(X) \pmod{m}$ and $\deg \overline{g} = \deg g$.

Proof. Example Sheet 1. □

Lecture 5

Corollary 4.5. Let $(K, |\bullet|)$ be a complete discretely valued field. Let

$$f(X) = a_n X^n + \cdots + a_n \in K[X]$$

with $a_0, a_n \neq 0$. If $f(X)$ is irreducible, then $|a_i| \leq \max(|a_0|, |a_n|)$ for all i.

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

$$\overline{f}(X) = X^r(a_r + \cdots + a_n X^{n-r}) \pmod{m}.$$

Then Theorem 4.4 implies $f(X) = g(X)h(X)$ with $0 < \deg < n$. □

5 Teichmüller lifts

Definition 5.1 (Perfect)**.** A ring R of characteristic $p > 0$ (prime) is a *perfect ring* if the Frobenius $x \mapsto x^p$ is a bijection. A field of characteristic p is a perfect field if it is perfect as a ring.

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

Example.

(i) $\mathbb{F}_{p^n}$ and $\overline{\mathbb{F}_p}$ are perfect fields.

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

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

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

Theorem 5.2. Assuming that:

- $(K, |\bullet|)$ is a complete discretely valued field
- such that $k := \mathcal{O}_K/m$ is a perfect field of characterist p

Then there exists a unique map $[\bullet] : k \to \mathcal{O}_K$ such that

(i) $a \equiv [a] \bmod m$ for all $a \in k$

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

Moreover if characteristic $\mathcal{O}_K = p$, then $[\bullet]$ is a ring homomorphism.

Definition 5.3. The element $[a] \in \mathcal{O}_K$ constructed in Theorem 5.2 is the *Teichmüller lift* of a.

Lemma 5.4. Assuming that:

- $(K, |\bullet|)$ is a complete discretely valued field
- such that $k := \mathcal{O}_K/m$ is a perfect field of characterist p
- $\pi \in \mathcal{O}_K$ a fixed uniformiser
- $x, y \in \mathcal{O}_K$ such that $x \equiv y \bmod \pi^k$ $(k \geq 1)$

Then $x^p \equiv y^p \bmod \pi^{k+1}$.

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

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

Since $\mathcal{O}_K/\pi\mathcal{O}_K$ has characteristic p, we have $p \in \pi\mathcal{O}_K$. Thus

$$\binom{p}{i}(u\pi^k)^i y^{p-i} \in \pi^{k+1}\mathcal{O}_K \qquad \forall i \geq 1,$$

hence $x^p \equiv y^p \bmod \pi^{k+1}$. □

Proof of Theorem 5.2. Let $a \in k$. For each $i \geq 0$ we choose a lift $y_i \in \mathcal{O}_K$ of $a^{\frac{1}{p^i}}$, and we define

$$x_i := y_i^{p_i}.$$

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

By construction, $y_i \equiv y_{i+1}^p \bmod \pi$. By Lemma 5.4 and induction on k, we have $y_i^{p^k} \equiv y_{i+1}^{p^{k+1}}$ and hence $x_i \equiv x_{i+1} \bmod \pi^{i+1}$ (take $i = p$). Hence $(x_i)_{i=1}^{\infty}$ is Cauchy, so $x_i \to x \in \mathcal{O}_K$.

Suppose $(x_i')_{i=1}^{\infty}$ arises from another choice of y_i' lifting $a_i^{\frac{1}{p^i}}$. Then $(x_i')_{i=1}^{\infty}$ is Cauchy, and $x_i' \to x' \in \mathcal{O}_K$. Let

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

Then x_i'' arises from lifting

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

Then x_i'' is Cauchy and $x_i'' \to x$, $x_i'' \to x'$. So $x = x'$ and hence x is independet of the choice of y_i. So we may define $[a] = x$.

Then $x_i = y_i^{p^i} \equiv (a^{\frac{1}{p^i}})^{p^i} \equiv a \bmod \pi$. Hence $x \equiv a \bmod \pi$. So (i) is satisfied.

We let $b \in k$ and we choose $u_i \in \mathcal{O}_K$ a lift of $b^{\frac{1}{p^i}}$, and let $z_i := u_i^{p^i} t$. Then $\lim_{i\to\infty} z_i = [b]$.

Now $u_i y_i$ is a lift of $(ab)^{\frac{1}{p^i}}$, hence

$$[ab] = \lim_{i\to\infty} x_i z_i = (\lim_{i\to\infty} x_i)(\lim_{i\to\infty} z_i) = [a][b].$$

So (ii) is satisfied.

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

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

Easy to check that $[0] = 0$, $[1] = 1$, and hence $[\bullet]$ is a ring homomorphism.

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

$$\begin{aligned} [a] &= \lim_{i\to\infty} \phi(a^{\frac{1}{p^i}})^{p^i} \\ &= \lim_{i\to\infty} \phi(a) \\ &= \phi(a) \end{aligned}$$

□

Example. $K = \mathbb{Q}_p$, $[\bullet] : \mathbb{F}_p \to \mathbb{Z}_p$, $a \in \mathbb{F}_p^\times$, $[a]^{p-1} = [a^{p-1}] = [1] = 1$. So $[a]$ is a $(p-1)$-th root of unity.

Lemma 5.5. Assuming that:

- $(K, |\bullet|)$ complete discretely valued field
- $k = \mathcal{O}_K/m \subseteq \overline{\mathbb{F}_p}$
- $a \in k^\times$

Then $[a]$ is a root of unity.

Proof.

$$\begin{aligned} a \in k^\times &\implies a \in \mathbb{F}_{p^n}^\times \text{ for some } n \\ &\implies [a]^{p^n-1} = [a^{p^n-1}] = [1] = 1 \end{aligned}$$

□

Theorem 5.6. Assuming that:

- $(K, |\bullet|)$ complete discretely valued field
- $\text{characteristic}(K) = p > 0$

- k is perfect

Then $K = k((t))$ ($k = \mathcal{O}_K/m$).

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

$$\varphi : k[[t]] \to \mathcal{O}_K$$
$$\varphi\left(\sum_{i=0}^{\infty} a_i t^i\right) = \sum_{i=0}^{\infty} [a_i]\pi^i$$

Then φ is a ring homomorphism since $[\bullet]$ is, and it is a bijection by Proposition 3.4(ii). $\square$

Lecture 6

6 Extensions of complete valued fields

Theorem 6.1. Assuming that:

- $(K, |\bullet|)$ is a complete discretely valued field
- L/K a finite extension of degree n

Then

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

$$|y|_L = \left|N_{L/L}(y)\right|^{\frac{1}{n}} \qquad \forall y \in L.$$

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

Recall: If L/K is finite, $N_{L/K} : L \to K$ is defined by $N_{L/K}(y) = \det_K(\text{mult}(y)$ where $\text{mult}(y) : L \to L$ is the K-linear map induced by multiplication by y.

Facts:

- $N_{L/K}$ is multiplicative.
- Let $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ be the minimal polynomial of $y \in L$. Then $N_{L/K}(y) = \pm a_0^m$ for some $m \geq 1$ (in fact, m is the degree of $L/K[y]$).
- $N_{L/K}(y) = 0 \iff y = 0$.

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

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

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

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

Example. If V is finite dimensional and $e_1, \ldots, e_n$ is a basis of V. The supremum $\|\bullet\|_{\sup}$ on V is defined by

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

where $x = \sum_{i=1}^n x_i e_i$.
Exercise: $\|\bullet\|_{\sup}$ is a norm.

Definition 6.3 (Equivalent norms)**.** Two norms $\| \bullet \|_1$ and $\| \bullet \|_2$ on V are equivalent if there exists $C, D \in \mathbb{R}_{>0}$ such that

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

Fact: A norm defines a topology on V, and equivalent norms induce the same topology.

Proposition 6.4. Assuming that:

- $(K, |\bullet|)$ is a complete non-archimedean valued field
- V a finite dimensional vector space over K

Then V is complete with respect to $\| \bullet \|_{\sup}$.

Proof. Let $(v_i)_{i=1}^{\infty}$ 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 $v_i \to v := \sum_{j=1}^{n} x_j e_j$. □

Theorem 6.5. Assuming that:

- $(K, |\bullet|)$ is a complete non-archimedean valued field
- V a finite dimensional vector space over K

Then any two norms on K are equivalent. In particular, V is complete with respect to any norm (using Proposition 6.4).

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

Let $e_1, \dots, e_n$ be a basis for V, and set $D := \max_i \|e_i\| > 0$. Then for $x = \sum_{i=1}^{n} x_i e_i$, we have

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

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

For $n = 1$: $\|x\| = \|x_1 e_1\| = |x_1| \, \|e_1\|$, so take $C = \|e_1\|$.

For $n > 1$: set $V_i = \operatorname{span}\langle e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n \rangle$. By induction, V_i is complete with respect to $\| \bullet \|$, hence closed.

Then $e_i + V_i$ is closed for all i, and hence

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

is a closed subset not containing 0. Thus there exists $c > 0$ such that $B(0, C) \cap S = \emptyset$ where $B(0, C) = \{x \in V \mid \|x\| < C\}$.

Let $0 \neq x = \sum_{i=1}^{n} x_i e_i$ and suppose $|x_j| = \max_i |x_i|$. Then $\|x\|_{\sup} = |x_j|$, and $\frac{1}{x_j} \in S$. Thus $\left\|\frac{x_i}{x_j}\right\| \geq C$, and hence

$$\|x\| \geq C\,|x_j| = C\|x\|_{\sup}.$$

V is complete since it is complete with respect to $\| \bullet \|_{\sup}$ (see Proposition 6.4). □

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

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

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

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

Proof. Example Sheet 2. □

Lemma 6.8. Assuming that:

- $(K, |\bullet|)$ is non-archimedean valued field

Then $\mathcal{O}_K$ is integrally closed in K.

Proof. Let $x \in K$ be integral over $\mathcal{O}_K$. Without loss of generality, $x \neq 0$. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ such that $f(x) = 0$. Then

$$x = -a_{n-1}\frac{1}{x} - \cdots - a_0\frac{1}{x_{n-1}}.$$

If $|x| > 1$, we have $\left|-a_{n-1}\frac{1}{x} - \cdots - a_0\frac{1}{x_{n-1}}\right| < 1$. Thus $|x| \leq 1 \implies x \in \mathcal{O}_K$. □

Lemma 6.9. $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ inside L.

Proof. Let $0 \neq y \in L$ and let

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$$

be the minimal (monic) polynomial of y.

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

$\Rightarrow$ Clear.

$\Leftarrow$ Let $g(X) \in \mathcal{O}_K[X]$ monic such that $g(y) = 0$. Then $f \mid g$ (in $K[X]$), and hence every root of f is a root of g. So every root of f in $\overline{K}$ is integral over $\mathcal{O}_K$, so a_i are integral over $\mathcal{O}_K$ for $i = 0, \ldots, d-1$.

Hence $a_i \in \mathcal{O}_k$ (by Lemma 6.8). By Corollary 4.5, $|a_i| \leq \max(|a_0|, 1)$ for $i = 0, \ldots, d-1$. By property of $N_{L/K}$, we have $N_{L/K}(y) = \pm a_0^m$ for $m \geq 1$.

Hence

$$\begin{aligned} y \in \mathcal{O}_L &\iff |N_{L/K}(y)| \leq 1 \\ &\iff |a_0| \leq 1 \\ &\overset{Corollary\ 4.5}{\iff} |a_i| \leq 1 \qquad \forall i, \text{i.e. } a_i \in \mathcal{O}_K \end{aligned}$$

Thus ${\mathcal{O}_K}^{\text{int}(L)} = \mathcal{O}_L$ and proves the Lemma. □

Proof of Theorem 6.1. We first show $|\bullet|_L = \left|N_{L/K}(\bullet)\right|^{\frac{1}{n}}$ satisfies the three axioms in the definition of absolute value.

(i)

$$\begin{aligned} |y|_L = 0 &\iff \left|N_{L/K}(y)\right|^{\frac{1}{n}} = 0 \\ &\iff N_{L/K}(y) = 0 \\ &\iff y = 0 \end{aligned}$$

(ii)

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

(iii) Set $\mathcal{O}_L = \{y \in L \mid |y|_L \leq 1\}$.

Claim: $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ inside L.

Assuming this, we prove (iii). Let $x, y \in L$, and without loss of generality assume $|x|_L \leq |y|_L$. Then $\left|\frac{x}{y}\right|_L$ hence $\frac{x}{y} \in \mathcal{O}_L$. Since $1 \in \mathcal{O}_L$ and $\mathcal{O}_L$is a ring, we have $1 + \frac{x}{y} \in \mathcal{O}_L$ and hence $\left|1 + \frac{x}{y}\right|_L \leq 1$. Hence $|x + y|_L \leq |y|_L = \max(|x|_L, |y|_L)$ thus (iii) is satisfied.

Lecture 7

So we have proved that $|\bullet|_L$ is an absolute value on L.

Since $N_{L/K}(x) = x^n$ for $x \in K$, $|x|_L$ extends $|\bullet|$ on K.

If $|\bullet|'_L$ is another absolute value on L extending $|\bullet|$, then $|\bullet|_L, |\bullet|'_L$ are norms on L.

Theorem 6.5 tells us that $|\bullet|'_L, |\bullet|_L$ induce the same topology on L. Hence $|\bullet|'_L = |\bullet|^c_L$ for some $c > 0$ (by Proposition 1.4) since $|\bullet|'_L$ extends $|\bullet|$, we have $c = 1$.

Now we show that L is complete with respect to $|\bullet|_L$: this is immediate by Theorem 6.5. □

Let $(K, |\bullet|)$ be a complete discretely valued field.

Corollary 6.10. Let L/K be a finite extension. Then

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

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

Proof.

(i) v a valuation on K, v_L valuation on L such that v_L extends v. Let $n = [L : K]$, and let $y \in L^\times$. Then $|y|_L = |N_{L/K}(y)|^{\frac{1}{n}}$ hence $v_L(y) = \frac{1}{n}v(N_{L/K}(y))$, hence $v_L(L^\times) \le \frac{1}{n}v(K^\times)$, so v_L is discrete.

(ii) Lemma 6.9.

□

Corollary 6.11. Let $\overline{K}/K$ be an algebraic closure of K. Then $|\bullet|$ extends to a unique absolute value $|\bullet|_{\overline{K}}$ on $\overline{K}$.

Proof. Let $x \in \overline{K}$, then $x \in L$ for some L/K finite. Define $|x|_{\overline{K}} = |x|_L$. Well-defined, i.e. independent of L by the uniqueness in Theorem 6.1.

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

Uniqueness: clear. □

Remark. $|\bullet|_{\overline{K}}$ on $\overline{K}$ is never discrete. For example $K = \mathbb{Q}_p$, $\sqrt[n]{p} \in \overline{\mathbb{Q}_p}$ for all $n \in \mathbb{Z}_{>0}$. Then

$$v_p(\sqrt[n]{p}) = \frac{1}{n} v(p) = \frac{1}{n}.$$

$\overline{\mathbb{Q}_p}$ is not complete with respect to $|\bullet|_{\overline{\mathbb{Q}_p}}$.
Example Sheet 2: $\mathbb{C}_p :=$ completion of $\overline{\mathbb{Q}_p}$ with respect to $|\bullet|_{\overline{\mathbb{Q}_p}}$, then $\mathbb{C}_p$ is algebraically closed.

Proposition 6.12. Assuming that:

- L/K finite extension of complete discretely valued fields.
- (i): $\mathcal{O}_K$ is compact.
- (ii): The extension of residue fields k_L/k is finite and separable.

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

Later we'll prove that the (i) implies (ii).

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

- there exists $\beta \in \mathcal{O}_L[\alpha]$ a uniformiser for $\mathcal{O}_L$
- $\mathcal{O}_K[\alpha] \to k_L$ surjective

k_L/k separable tells us that there exists $\overline{\alpha} \in k_L$ such that $k_L = k(\overline{\alpha})$.

Let $\alpha \in \mathcal{O}_L$ a lift of $\overline{\alpha}$, and $g(X) \in \mathcal{O}_K[X]$ a monic lift of the minimal polynomial of $\overline{\alpha}$.

Fix $\pi_L \in \mathcal{O}_L$ a uniformiser. Then $\overline{g}(X) \in k[X]$ irreducible and separable, hence $g(\alpha) \equiv 0 \bmod \pi_L$ and $g'(\alpha) \not\equiv 0 \bmod \pi_L$.

If $g(\alpha) \equiv 0 \bmod \pi_L^2$, then

$$g(\alpha + \pi_L) \equiv g(\alpha) + \pi_L g'(\alpha) \bmod \pi_L^2.$$

Thus

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

(v_L normalised valuation on L).

Thus either $v_L(g(\alpha)) = 1$ or $v_L(g(\alpha + \pi_L)) = 1$. Upon possibly replacing α by $\alpha + \pi_L$, we may assume $v_L(g(\alpha)) = 1$.

Set $\beta = g(\alpha) \in \mathcal{O}_K[\alpha]$ a uniformiser. Then $\mathcal{O}_K[\alpha] \subseteq L$ is the image of a continuous map:

$$\mathcal{O}_K^n \to L$$
$$(x_0, \ldots, x_{n-1}) \mapsto \sum_{i=0}^{n} x_i a^i$$

where $n = [K(\alpha) : K]$. Since $\mathcal{O}_K$ is compact, $\mathcal{O}_K[\alpha] \subseteq L$ is compact, hence closed. Since $k_L = k(\overline{\alpha})$, $\mathcal{O}_K[\alpha]$ contians a set of coset representatives for $k_L = \mathcal{O}_L/\beta\mathcal{O}_L$.

Let $y \in \mathcal{O}_L$. Then Proposition 3.4 gives us

$$y = \sum_{i=0}^{\infty} \lambda_i \beta^i, \qquad \lambda_i \in \mathcal{O}_K[\alpha]$$

Then $y_m = \sum_{i=0}^{m} \lambda_i \beta^i \in \mathcal{O}_K[\alpha]$. Hence $y \in \mathcal{O}_K[\alpha]$, since $\mathcal{O}_k[\alpha]$ is closed. □

Part III

Local Fields

7 Local Fields

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

Reminder: locally compact means for all $x \in K$, there exists U open and V compact such that $x \in U \subseteq V$.

Example. $\mathbb{R}$ and $\mathbb{C}$ are compact.

Proposition 7.2. Assuming that:

- $(K, |\bullet|)$ is a non-archimedean complete valued field

Then the following are equivalent:

(i) K is locally compact

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

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

Lecture 8

Proof.

(i) $\implies$ (ii) Let $U \ni 0$ be a compact neighbourhood of 0 ($0 \in U \subseteq Z$ with U open, Z compact). Then there exists $x \in \mathcal{O}_K$ such that $x\mathcal{O}_K \subseteq U$. Since $x\mathcal{O}_K$ is closed, $x\mathcal{O}_K$ is compact. Hence $\mathcal{O}_K$ is compact ($x\mathcal{O}_K \overset{\cdot x^{-1}}{\to} \mathcal{O}_K$ is a homeomorphism).

(ii) $\implies$ (i) $\mathcal{O}_K$ compact implies $a + \mathcal{O}_K$ is compact for all $a \in K$. So K is locally compact.

(ii) $\implies$ (iii) Let $x \in m$, and $A_x \subseteq \mathcal{O}_K$ be a set of coset representatives for $\mathcal{O}_K/x\mathcal{O}_K$. Then $\mathcal{O}_K = \bigcup_{y \in A} y + x\mathcal{O}_K$ is a disjoint open cover. So A_x is finite by compactness of $\mathcal{O}_K$. So $\mathcal{O}_K/x\mathcal{O}_K$ is finite, hence $\mathcal{O}_K/m\mathcal{O}_K$ is finite.o

Suppose v is not discrete. Then let $x_1, x_2, \dots$ such that

$$v(x_1) > v(x_2) > \cdots > 0.$$

Then $x\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq x_3\mathcal{O}_K \subsetneq \cdots \subsetneq \mathcal{O}_K$. But $\mathcal{O}_K/x\mathcal{O}_K$ is finite so can only have finitely many subgroups, contradiction.

(iii) $\implies$ (ii) Since $\mathcal{O}_K$ is a metric space, it suffices to prove $\mathcal{O}_K$ is sequentially compact.

Let $(x_n)_{n=1}^\infty$ be a sequence in $\mathcal{O}_K$, and fix $\pi \in \mathcal{O}_K$ a uniformiser. Since $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong k$, $\mathcal{O}_K/\pi^i\mathcal{O}_K$ is finite for all i ($\mathcal{O}_K \supseteq \pi\mathcal{O}_K \supseteq \cdots \supseteq \pi^i\mathcal{O}_K$). Since $\mathcal{O}_K/\pi\mathcal{O}_K$ is finite, there exists $a_1 \in \mathcal{O}_K/\pi\mathcal{O}_K$ and a subsequence $(x_n)_{n=1}^\infty$ such that $x_{1n} \equiv a \bmod \pi$ for all n.

Since $\mathcal{O}_K/\pi^2\mathcal{O}_K$ is finite, there exists $a_2 \in \mathcal{O}_K/\pi^2\mathcal{O}_K$ and a subsequence $(x_{2n})_{n=1}^\infty$ of $(x_{1n})_{n=1}^\infty$ such that $x_{2n} \equiv a_2 \pmod{\pi}^2\mathcal{O}_K$. Continuing, this, we obtain sequences $(x_{in})_{n=1}^\infty$ for $i = 1, 2, \dots$ such that

(1) $(x_{(i+1)n})_{n=1}^\infty$ is a subsequence of $(x_{in})_{n=1}^\infty$

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

Then necessarily $a_i \equiv a_{i+1} \bmod \pi^i$ for all i.

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

Example.

(i) $\mathbb{Q}_p$ is a local field.

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

More on inverse limits.

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

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

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

Proposition 7.4. Assuming that:

- K is a non-archimedean local field

Then under the isomorphism $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ ($\pi \in \mathcal{O}_K$ a uniformiser), the topology on $\mathcal{O}_K$ coincides with the profinite topology.

Proof. One checks that the sets

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

is a basis of open sets in both topologies.

For $|\bullet|$: clear.

For profinite topology: $\mathcal{O}_K/\mathcal{O}_K/\pi^n\mathcal{O}_K$ is continuous if and only if $a+\pi^n\mathcal{O}_K$ is open for all $a \in \mathcal{O}_K$. □

Goal: Classify all local fields.

Lemma 7.5. Assuming that:

- K is a non-archimedean local field
- L/K a finite extension

Then L is a local field.

Proof. Theorem 6.1 implies that L is complete and discretely valued. Suffices to show $k_L := \mathcal{O}_L/m_L$ is finite. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L as a K vector space.

$\| \bullet \|_{\text{sup}}$ (sup norm) equivalent to $| \bullet |_L$ implies that there exists $r > 0$ such that

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

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

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

Then $\mathcal{O}_L$ is finitely generated as a module over $\mathcal{O}_K$, hence k_L is finitely generated over k. □

Definition 7.6 (Equal characteristic)**.** A non-archimedean valued field $(K, |\bullet|)$ has *equal characteristic* if characteristic(K) = characteristic(k). Otherwise it has *mixed characteristic*.

Example. $\mathbb{Q}_p$ has mixed characteristic.

Theorem 7.7. Assuming that:

- K is a non-archimedean local field of equal characteristic $p > 0$

Then $K \cong \mathbb{F}_{p^n}((t))$ for some $n \ge 1$.

Proof. K complete discretely valued, characteristic $K > 0$. Moreover, $k \cong \mathbb{F}_{p^n}$ is finite, hence perfect.

By Theorem 5.6, $K \cong \mathbb{F}_{p^n}((t))$. □

Lemma 7.8. Assuming that:

- K a field

Then an absolute value $|\bullet|$ is non-archimedean if and only if $|n|$ is bounded for all $n \in \mathbb{Z}$.

Proof.

⇒ Since $|-1| = 1$, $|-n| = |n|$, it suffices to show that $|n|$ bounded for $n \geq 1$. Then note that

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

⇐ Suppose $|n| \leq B$ for all $n \in \mathbb{Z}$. Let $x, y \in K$ with $|x| \leq |y|$. Then we have

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

Taking m-th roots gives

$$|x+y| \leq |y| [B(m+1)]^{\frac{1}{m}}.$$

The right hand side tends to $|y|$ as $m \to \infty$, hence

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

□.

Lecture 9

Theorem 7.9 (Ostrowski's Theorem)**.** Assuming that:

- $|\bullet|$ is a non-trivial absolute value on $\mathbb{Q}$

Then $|\bullet|$ is equivalent to either the usual absolute value $|\bullet|_\infty$ or the p-adic absolute value $|\bullet|_p$ for some prime p.

Proof. **Case:** $|\bullet|$ is archimedean. We fix $b > 1$ an integer such that $|b| > 1$ (exists by Lemma 7.8). Let $a > 1$ be an integer and write b^n in base a:

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

with $0 \leq c_i < a$, $c_m \neq 0$. Let $B = \max_{0 \leq c < a-1}(|c|)$, and then we have

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

Then $|a| > 1$ and

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

Switching roles of a and b, we also obtain

$$|a| \leq |b|^{\log_b a}. \tag{$**$}$$

Then $(*)$ and $(**)$ gives (using $\log_a b = \frac{\log b}{\log a}$):

$$\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} = \lambda \in \mathbb{R}_{>0}.$$

Hence $|a| = a^\lambda$ for all $a \in \mathbb{Z}_{>1}$, hence $|x| = |x|_\infty^\lambda$ for all $x \in \mathbb{Q}$.

Case 2: $|\bullet|$ is non-archimedean. As in Lemma 7.8, we have $|n| \leq 1$ for all $n \in \mathbb{Z}$. Since $|\bullet|$ is non-trivial, there exists $n \in \mathbb{Z}_{>1}$ such that $|n| < 1$. Write $n = p_1^{e_1} \cdots p_r^{e_r}$ decomposition into prime factors. Then $|p| < 1$, for some $p \in \{p_1, \ldots, p_r\}$. Suppose $|q| < 1$ for some prime q, $q \neq p$. Write $1 = rp + sq$ with $r, s \in \mathbb{Z}$. Then

$$\begin{aligned} 1 &= |rp + sq| \\ &\leq \max(|rp|, |sq|) \\ &< 1 \end{aligned}$$

contradiction. Thus $|p| = \alpha < 1$ and $|q| = 1$ for all primes $q \neq p$. Hence $|\bullet|$ is equivalent to $|\bullet|_p$. $\square$

Theorem 7.10. Assuming that:

- $(K, |\bullet|)$ is a non-archimedean local field of mixed characteristic

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

Proof. K mixed characteristic implies that characteristic $K = 0$, hence $\mathbb{Q} \subseteq K$. K non-archimedean implies that $|\bullet|\,|_{\mathbb{Q}} = |\bullet|_p$ for some prime p. Since K is complete, $\mathbb{Q}_p \subseteq K$. Suffices to show that $\mathcal{O}_K$ is finite as a $\mathbb{Z}_p$-module.

Let $\pi \in \mathcal{O}_K$ be a uniformiser, v a normalised valuation and set $v(p) = e$. Then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\pi^e\mathcal{O}_K$ is finite since $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong \mathcal{O}_K/\pi\mathcal{O}_K$ is finite. Since $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K$ we have $\mathcal{O}_K/p\mathcal{O}_K$ a finite dimensional vector space over $\mathbb{F}_p$.

Let $x_1, \ldots, x_n \in \mathcal{O}_K$ be coset representatives for $\mathbb{F}_p$-basis of $\mathcal{O}_K/p\mathcal{O}_K$. Then

$$\left\{ \sum_{i=1}^n a_i x_i \,\middle|\, a_i \in \{0, \ldots, r-1\} \right\}$$

is a set of coset representatives for $\mathcal{O}_K/p\mathcal{O}_K$. Let $y \in \mathcal{O}_K$. Proposition 3.4(ii) tells us that

$$\begin{aligned} y &= \sum_{i=0}^{\infty} \left(\sum_{j=1}^{n} a_{ij} x_j \right) p^i && (a_{ij} \in \{0, \dots, p-1\}) \\ &= \sum_{j=1}^{n} \left(\sum_{i=0}^{\infty} a_{ij} p^i \right) x_j \\ &\in \mathbb{Z}_p \end{aligned}$$

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

On Example Sheet 2 we will show that if K is complete and archimedean, then $K \simeq \mathbb{R}$ or $\mathbb{C}$. In summary:

If K a local field, then either:

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

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

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

8 Global Fields

Definition 8.1 (Global field)**.** 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 8.2. Assuming that:

- $(K, |\bullet|)$ is a complete discretely valued field
- L/K a finite Galois extension with absolute value $|\bullet|_L$ extending $|\bullet|$.

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 another absolute value on L extending $|\bullet|$ on K, the result follows from uniqueness of $|\bullet|_L$. □

Lemma 8.3 (Kummer's Lemma)**.** Assuming that:

- $(K, |\bullet|)$ a complete discretely valued field
- $f(X) \in K[X]$ a separable irreducible polynomial with roots $\alpha_1, \dots, \alpha_n \in K^{\mathrm{sep}}$ (K^{sep} is the separable closure of K)
- $\beta \in K^{\mathrm{sep}}$ with
$$|\beta - \alpha_1| < |\beta - \alpha_i|$$
for $i = 2, \dots, n$.

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

Proof. Let $L = K(\beta)$, $L' = L(\alpha_1, \dots, \alpha_n)$. Then L'/L is a Galois extension. Let $\sigma \in \mathrm{Gal}(L'/L)$. We have

$$\begin{aligned} |\beta - \sigma(\alpha_1)| &= |\sigma(\beta - \alpha_1)| \\ &= |\beta - \alpha_1| \end{aligned}$$

using Lemma 8.2. Hence $\sigma(\alpha_1) = \alpha_1$, so $\alpha_1 \in K(\beta)$. □

Proposition 8.4. Assuming that:

- $(F, |\bullet|)$ is a complete discretely valued field

- $f(X) = \sum_{i=0}^n a_i X^i \in \mathcal{O}_K[X]$ a separable irreducible monic polynomial
- $\alpha \in K^{\text{sep}}$ a root of f

Then there exists $\varepsilon > 0$ such that for any $g(X) = \sum_{i=0}^n b_i X^i \in \mathcal{O}_K[X]$ monic with $|a_i - b_i| < \varepsilon$ for all i, there exists a root β of $g(X)$ such that $K(\alpha) = K(\beta)$.

"Nearby polynomials define the same extensions".

Proof. Let $\alpha_1, \dots, \alpha_n \in K^{\text{sep}}$ be the roots of f which are necessarily distinct. Then $f'(\alpha_1) \neq 0$. We choose ε sufficiently small such that $|g(\alpha_1)| < |f'(\alpha_1)|^2$ and $|f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha_1)|$. Then we have $|g'(\alpha_1)| < |f'(\alpha_1)|^2 = |g'(\alpha_1)|^2$ (the equality is by Lemma 1.6).

By Hensel's Lemma version 1 applied to the field $K(\alpha_1)$ there exists $\beta \in K(\alpha_1)$ such that $g(\beta) = 0$ and $|\bullet - \alpha_1| < |g'(\alpha_1)|$. Then

$$\begin{aligned} |g'(\alpha_1)| &= |f'(\alpha_1)| \\ &= \prod_{j=1}^n |\alpha_1 - \alpha_j| \\ &\le |\alpha_1 - \alpha_i| \end{aligned}$$

for $i = 2, \dots, n$. (Use $|\alpha_1 - \alpha_i| \le 1$ since α_i integral). Since $|\beta - \alpha_1| < |\alpha_1 - \alpha_i| = |\beta - \alpha_i|$ using Lemma 1.6, we have that Kummer's Lemma gives that $\alpha_1 \in K(\beta)$ and hence $K(\alpha_1) = K(\beta)$. □

Lecture 10

Theorem 8.5. Assuming that:

- K is a local field

Then K is the completion of a global field.

Proof. **Case 1:** $|\bullet|$ is archimedean. Then $\mathbb{R}$ is the completion of $\mathbb{Q}$, and $\mathbb{C}$ is the completion of $\mathbb{Q}(i)$ (with respect to $|\bullet|_\infty$).

Case 2: $|\bullet|$ non-archimedean, equal characteristic. Then $K \cong \mathbb{F}_q((t))$ is the completion of $\mathbb{F}_q(t)$ with respect to the t-adic valuation.

Case 3: $|\bullet|$ non-archimedean mixed characteristic. Then $K = \mathbb{Q}_p(\alpha)$, with α a root of a monic irreducible polynomial $f(X) \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we choose $g(X) \in \mathbb{Z}[X]$ as in Proposition 8.4. Then $K = \mathbb{Q}(\beta)$ with β a root of $g(X)$. Since $\mathbb{Q}(\beta)$ dense in $\mathbb{Q}_p(\beta) = K$, and K is complete, we must have that K is the completion of $\mathbb{Q}(\beta)$. □

Part IV

Dedekind domains

9 Dedekind domains

Definition 9.1 (Dedekind domain)**.** 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 non-zero prime ideal is maximal.

Example.

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

Theorem 9.2. A ring R is a discrete valuation ring if and only if R is a Dedekind domain with exactly one non-zero prime.

Lemma 9.3. Assuming that:

- R is a Noetherian ring
- $I \subseteq R$ a non-zero ideal

Then there exists non-zero prime ideals $p_1, \dots, p_r$ such that $p_1, \dots, p_r \subseteq I$.

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

Let $I_1 + (x)$, $I_2 = I + (y)$. Then by maximality of I, there exist $p_1, \dots, p_r$ and $q_1, \dots, q_s$ such that $p_1 \cdots p_r \subseteq I_1$ and $q_1 \cdots q_s \subseteq I_2$. Then $p_1 \cdots p_r q_1 \cdots q_s \subseteq I_1 I_2 \subset I$. □

Lemma 9.4. Assuming that:

- R is an integral domain
- R is integrally closed in $K = \mathrm{Frac}(R)$
- $0 \neq I \subseteq R$ a finitely generated ideal
- $x \in K$

Then if $xI \subseteq I$, we have $x \in R$.

Proof. Let $I = (c_1, \dots, c_n)$. We write

$$xc_i = \sum_{j=1}^{n} a_{ij} c_j$$

for some $a_{ij} \in R$. Let A be the matrix $A = (a_{ij})_{1 \le i,j \le n}$ and set $B = x \operatorname{id}_n - A \in M_{n \times n}(K)$.

Then in K^n

$$B \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \mathbf{0}.$$

Multiply by $\operatorname{adj}(B)$, the adjugate matrix for B. We have

$$\det(B) \operatorname{id}_n \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0.$$

Hence $\det(B) = 0$. But $\det B$ is a monic polynomial with coefficients in R. Then x is integral over R, hence $x \in R$. □

Proof of Theorem 9.2.

⇒ Clear.

⇐ We need to show R is a PID. The assumption implies that R is a local ring with unique maximal ideal m.

Step 1: m is principal.

Let $0 \ne x \in m$. By Lemma 9.3, $(x) \supseteq m^n$ for some $n \ge 1$. Let n minimal such that $(x) \supset m^n$, then we may choose $y \in m^{n-1} \setminus (x)$.

Set $\pi = \frac{x}{y}$. Then we have $ym \subseteq m^n \subseteq (x)$ and hence $\pi^{-1} m \subseteq R$. If $\pi^{-1} m \subseteq m$, then $\pi^{-1} \in R$ by Lemma 9.4 and $y \in (x)$, contradiction. Hence $\pi^{-1} m = R$, so $m = \pi R$ is principal.

Step 2: R is a PID.

Let $I \subseteq R$ be a non-zero ideal. Consider a sequence of fractional ideals $I \subseteq \pi^{-1} I \subseteq \pi^{-2} I \subseteq \cdots$ in K. Then since $\pi^{-1} \notin R$, we have $\pi^{-k} I \ne \pi^{-(k+1)} I$ for all k by Lemma 9.4. Therefore since R is Noetherian, we may choose n maximal such that $\pi^{-n} I \subseteq R$. If $\pi^{-n} I \subseteq m = (\pi)$, then $\pi^{-(n+1)} \subseteq R$. So we must have $\pi^{-n} I = R$, and hence $I = (\pi^n)$. □

Let R be an integral domain and $S \subseteq R$ a multiplicatively closed subset ($x, y \in S$ implies $xy \in S$, and also have $1 \in S$). The localisation $S^{-1} R$ of R with respect to S is the ring

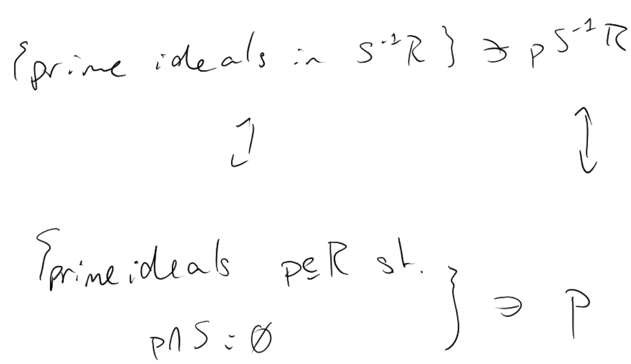
$$S^{-1} R = \left\{ \frac{r}{s} \,\middle|\, r \in R, s \in S \right\} \subseteq \operatorname{Frac}(R).$$

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

Example.

- $p = (0)$, then $R_{(p)} = \mathrm{Frac}(R)$.
- $R = \mathbb{Z}$, $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \middle| a \in \mathbb{Z}, (b, p) = 1 \right\}$, where p is a rational prime.

Facts: (not proved in this course, but can be found in a typical course / textbook on commutative algebra)

- R Noetherian implies $S^{-1}R$ is Noetherian.
- 

Corollary 9.5. Let R be a Dedekind domain and $p \subseteq R$ a non-zero prime ideal. Then $R_{(p)}$ is a discrete valuation ring.

Proof. By properties of localisation, $R_{(p)}$ is a Noetherian integral domain with a unique non-zero prime ideal $pR_{(p)}$.

It suffices to show $R_{(p)}$ is integrally closed in $\mathrm{Frac}(R_{(p)}) = \mathrm{Frac}(R)$ (since then $R_{(p)}$ is a Dedekind domain hence by Theorem 9.2, $R_{(p)}$ is a discrete valuation ring).

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

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

with $a_i \in R$, $s \in S = R \setminus p$. Multiply by s^{n-1}. Then xs is integral over R, so $xs \in R$. Hence $x \in R_{(p)}$. $\square$

Lecture 11

Definition 9.6 (Valuation on a Dedekind domain)**.** If R is a Dedekind domain, and $p \subseteq R$ a non-zero prime ideal, we write v_p for the normalised valuation on $\mathrm{Frac}(R) = \mathrm{Frac}(R_{(p)})$ corresponding to the discrete valuation ring $R_{(p)}$.

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

Theorem 9.7. Assuming that:

- R is a Dedekind domain
- $I \subseteq R$ a non-zero ideal

Then Ican be written uniquely as aproduct of prime ideals:

$$I = p_1^{e_1} \cdots p_r^{e_r}$$

(with p_i distinct).

Remark. Clear for PIDs (PID implies UFD).

Proof (Sketch). We quote the following properties of localisation:

(i) $I = J \iff IR_{(p)} = JR_{(p)}$ for all prime ideals p.

(ii) If R a Dedekind domain, p_1, p_2 non-zero ideals, then

$$p_1 R_{(p_2)} = \begin{cases} p_2 R_{(p_2)} & p_1 = p_2 \\ R_{(p_2)} & p_1 \neq p_2 \end{cases}$$

Let $I \subseteq R$ be a non-zero ideal. By Lemma 9.3, there are distinct prime ideals $p_1, \dots, p_r$ such that $p_1^{\beta_1} \cdots p_r^{\beta_r} \subseteq I$, where $\beta_i > 0$.

Let $0 \neq p$ be a prime ideal, $p \notin \{p_1, \dots, p_r\}$. Then property (ii) gives that $p_i R_{(p)} = R_{(p)}$, and hence $IR_{(p)} = R_{(p)}$.

Corollary 9.5 gives $IR_{(p_i)} = (p_i R_{(p_i)})^{\alpha_i} = p_i^{\alpha_i} R_{(p_i)}$ for some $0 \leq \alpha_i \leq \beta_i$. Thus $I = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ by property (i).

For uniqueness, if $I = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ then $p_i^{\alpha_i} R_{(p_i)} = p_i^{\gamma_i} R_{(p_i)}$ hence $a_i = \gamma_i$ by unique factorisation in discrete valuation rings. □

10 Dedekind domains and extensions

Let L/K be a finite extension. For $x \in L$, we write $\mathrm{Tr}_{L/K}(x) \in K$ for the trace of the K-linear map $L \to L$, $y \mapsto xy$.

If L/K is separable of degree n and $\sigma_1, \dots, \sigma_n : L \to \overline{K}$denotes the set of embeddings of L into an algebraic closure $\overline{K}$, then $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x) \in K$.

Lemma 10.1. Assuming that:

- L/K a finite separable extension of fields

Then the symmetric bilinear pairing

$$\begin{aligned}(\bullet, \bullet) &\to K \\ (x, y) &\mapsto \mathrm{Tr}_{L/K}(xy)\end{aligned}$$

is non-degenerate.

Proof. L/K separable tells us that $L = K(\alpha)$ for some $\alpha \in L$. Consider the matrix A for $(\bullet, \bullet)$ in the K-basis for L given by $1, \alpha, \dots \alpha^{n-1}$.

Then $A_{ij} = \mathrm{Tr}_{L/K}(\alpha^{i+j}) = [BB^\top]_{ij}$ where

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

So

$$\det A = \det(B)^2 = \left[\prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha)) \right]^2$$

(Vandermonde determinant), which is non-zero since $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$ by separability. □

Exercise: On Example Sheet 3 we will show that a finite extension L/K is separable if and only if the trace form is non-degenerate.

Theorem 10.2. Assuming that:

- $\mathcal{O}_K$ a Dedekind domain
- 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. $\mathcal{O}_L$ a subring of L, hence $\mathcal{O}_L$ is an integral domain.

Need to show:

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

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

(iii) Every $\neq 0$ prime ideal P in $\mathcal{O}_L$ is maximal.

Proofs:

(i) Let $e_1, \dots, e_n \in L$ be a K-basis for L. Upon scaling by K, we may assume $e_i \in \mathcal{O}_L$ for all i.

Let $f_i \in L$ be the dual basis with respect to the trace form $(\bullet, \bullet)$. Let $x \in \mathcal{O}_L$, and write $x = \sum_{i=1}^n \lambda_i f_i, \lambda_i \in K$. Then $\lambda_i = \mathrm{Tr}_{L/K}(xe_i) \in \mathcal{O}_K$.

(For any $z \in \mathcal{O}_L$, $\mathrm{Tr}_{L/K}(z)$ is a sum of elements in $\overline{K}$ which are integral over $\mathcal{O}_K$. Hence $\mathrm{Tr}_{L/K}(z) \in K$ is integral over $\mathcal{O}_K$, hence $\mathrm{Tr}_{L/K}(z) \in \mathcal{O}_K$.)

Thus $\mathcal{O}_L \subseteq \mathcal{O}_K f_1 + \cdots + \mathcal{O}_K f_n \subseteq L$. 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) Example Sheet 2.

(iii) Let P be a non-zero prime ideal of $\mathcal{O}_L$, and $p := P \cap \mathcal{O}_K$ be a prime ideal of $\mathcal{O}_K$. Let $0 \neq x \in P$. Then x satisfies an equation

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

with $a_0 \neq 0$. Then $a_0 \in P \cap \mathcal{O}_K$ is a non-zero element of p, hence p is non-zero, hence p is maximal.

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

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

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

Convention: $\mathcal{O}_K$ is the ring of integers of a number field – $p \leq \mathcal{O}_K$ a non-zero prime ideal. We normalise $| \bullet |_p$ (absolute value associated to v_p, as defined in Definition 9.6) by $|x|_p = (Np)^{-v_p(x)}$,
Lecture 12 where $N_p = |\mathcal{O}_K/p|$.

In the following theorems and lemmas we will have:

- $\mathcal{O}_K$ a Dedekind domain

- $K = \mathrm{Frac}(\mathcal{O}_K)$
- L/K finite separable
- $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L (which is a Dedekind domain by Theorem 10.2).

Lemma 10.4. Assuming that:

- $0 \neq x \in \mathcal{O})K$

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

Proof. $x\mathcal{O}_{K,_{(p)}} = (p\mathcal{O}_{K,(p)})^{v_p(x)}$ by definition of $v_p(x)$.

Lemma follows from property of localisation
$$I = J \iff I\mathcal{O}_{K,(p)} = J\mathcal{O}_{K,(p)}$$
for all prime ideals p. □

Notation. $P \le \mathcal{O}_L$, $p \le \mathcal{O}_K$ non-zero prime ideals. We write $P \mid p$ if $p\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$ and $P \in \{P_1, \dots, P_r\}$ ($e_i > 0$, P distinct).

Theorem 10.5. Assuming that:

- $\mathcal{O}_K$, $\mathcal{O}_L$, K, L as usual
- for p a non-zero prime ideal of $\mathcal{O}_K$, we write $p\mathcal{O}_L P_1^{e_1} \cdots P_r^{e_r}$

Then the absolute values on L extending $|\bullet|_p$ (up to equivalence) are precisely $|\bullet|_{P_1}, \dots, |\bullet|_{P_L}$.

Proof. By Lemma 10.4 for any $0 \neq x \in \mathcal{O}_K$ and $i = 1, \dots, r$ we have $v_{P_i}(x) = e_i v_p(x)$. Hence, up to equivalence, $|\bullet|_{P_i}$ extends $|\bullet|_p$.

Now suppose $|\bullet|$ is an absolute value on L extending $|\bullet|_p$. Then $|\bullet|$ is bounded on $\mathbb{Z}$, hence is non-archimedean. Let $R = \{x \in L \mid |x| \le 1\} \le L$ be the valuation ring for L with respect to $|\bullet|$. Then $\mathcal{O}_K \subseteq R$, and since R is integrally closed in L (Lemma 6.8), we have $\mathcal{O}_L \subseteq R$. Set
$$\begin{aligned} P &:= \{x \in \mathcal{O}_L \mid |x| < 1\} \\ &= m_R \cap \mathcal{O}_L \end{aligned}$$
(where m_R is the maximal ideal of R).

Hence P a prime ideal in $\mathcal{O}_L$. It is non-zero since $p \subseteq P$. Then $\mathcal{O}_{L,(p)} \subseteq R$, since $s \in \mathcal{O}_L \setminus P \implies |s| = 1$.

But $\mathcal{O}_{L,(p)}$ is a discrete valuation ring, hence a maximal subring of L, so $\mathcal{O}_{L,(p)} = R$. Hence $|\bullet|$ is equivalent to $|\bullet|_p$. Since $|\bullet|$ extends $|\bullet|_p$, $P \cap \mathcal{O}_K = p$ so $P_1^{e_1} \cdots P_r^{e_r} \subseteq P$, so $P = P_i$ for some i. □

Let K be a number field. If $\sigma : K \to \mathbb{R}, \mathbb{C}$ is a real or complex embedding, then $x \mapsto |\sigma(x)|_\infty$ defines an absolute value on K (Example Sheet 2) denoted $|\bullet|_\sigma$.

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) $|\bullet|_p$ for some non-zero prime ideal of $\mathcal{O}_K$.

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

Proof. **Case 1:** $|\bullet|$ non-archimedean. Then $|\bullet|\big|_{\mathbb{Q}}$ is equivalent to $|\bullet|_p$ for some prime p by Ostrowski's Theorem. Theorem 10.5 gives that $|\bullet|$ is equivalent to $|\bullet|_p$ for some $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal with $\mathfrak{p} \mid p$.

Case 2: $|\bullet|$ archimedean. See Example Sheet 2. □

10.1 Completions

$\mathcal{O}_K$ a Dedekind domain, L/K a finite separable extension.

Let $\mathfrak{p} \subseteq \mathcal{O}_K$, $P \subseteq \mathcal{O}_L$ be non-zero prime ideals with $P \mid \mathfrak{p}$.

We write $K_\mathfrak{p}$ and L_P for the completions of K and L with respect to the absolute values $|\bullet|_\mathfrak{p}$ and $|\bullet|_P$ respectively.

Lemma 10.7.

(i) The natural $\pi_P : L \otimes_K K_\mathfrak{p} \to L_P$ is surjective.

(ii) $[L_P : K_P] \leq [L : K]$.

Proof. Let $M = LK_\mathfrak{p} = \mathrm{Im}(\pi_P) \subseteq L_P$.

Write $L = K(\alpha)$ then $M = K_\mathfrak{p}(\alpha)$. Hence M is a finite extension of $K_\mathfrak{p}$ and $[M : K_\mathfrak{p}] \leq [L : K]$. Moreover M is complete (Theorem 6.1) and since $L \subseteq M \subseteq L_P$, we have $M = L_P$. □

Lemma 10.8 (Chinese remainder theorem)**.** Assuming that:

- R a ring
- $I_1, \dots, I_n \subseteq R$ ideals
- $I_i + I_j = R$ for all $i \neq j$

Then

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

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

Proof. Example Sheet 2. □

Theorem 10.9. The natural map

$$L \otimes_K K_{\mathfrak{p}} \to \prod_{P|\mathfrak{p}} L_P$$

is an isomorphism.

Proof. Write $L = K(\alpha)$ and let $f(X) \in K[X]$ be the minimal polynomial of α. Then we have

$$f(X) = f_1(X) \cdots f_r(X) \in K_{\mathfrak{p}}[X]$$

where $f_i(X) \in K_{\mathfrak{p}}[X]$ are distinct irreducible (separable). Since $L \cong K[X]/f(X)$,

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

Set $L_i = K_{\mathfrak{p}}[X]/f_i(X)$ a finite extension of $K_{\mathfrak{p}}$. Then L_i contains both $K_{\mathfrak{p}}$ and L (use $K[X]/f(x) \to K_{\mathfrak{p}}[X]/f_i(X)$ injective since morphism of fields). Moreover L is dense inside L_i (approximate coefficients of $K_{\mathfrak{p}}[X]/f_i(X)$ with an element of $K[X]/f_i(X)$).

The theorem follows from the following three claims:

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

(2) Each P appears at most once.

(3) Each P appears at least once.

Proof of claims:

(1) Since $[L_i : K_{\mathfrak{p}}] < \infty$, there is a unique absolute value on L_i extending $|\bullet|_{\mathfrak{p}}$. Theorem 10.5 gives us that $|\bullet|\big|_L$ is equivalent to $|\bullet|_P$ for some $P \mid \mathfrak{p}$. Since L is dense in L and L_i is complete, we have $L_i \cong L_P$.

(2) Suppose $\varphi : L_i \to L_j$ is an isomorphism preserving L and $K_{\mathfrak{p}}$; then

$$\varphi : K_{\mathfrak{p}}[X]/f_i(X) \to K_{\mathfrak{p}}[X]/f_i(X)$$

takes x to x and hence $f_i = f_i$.

(3) By Lemma 10.7, the natural map $\pi_P : L \otimes_K K_{\mathfrak{p}} \to L_P$ is surjective for any prime $P \mid \mathfrak{p}$.

Since L_P is a field, π_P factors through L_i for some i, and hence $L_i \cong L_P$ by surjectivity of π_P. □

Lecture 13

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $f(X) = X^2 + 1$. Hensel's Lemma version 1 gives us that $\sqrt{-1} \in \mathbb{Q}_5$. Hence (5) splies in $\mathbb{Q}(i)$, i.e. $5\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$.

Corollary 10.10. Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal. For $x \in L$ we have

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

Proof. Let $B_1, \dots, B_r$ be bases for $L_{P_1}, \dots, L_{P_r}$ as $K_{\mathfrak{p}}$-vector spaces. Then $B = \bigcup_i B_i$ is a basis for $L \otimes_K K_{\mathfrak{p}}$ over $K_{\mathfrak{p}}$. Let $[\text{mult}(x)]_B$ (respectively $[\text{mult}(x)]_{B_i}$) denote the matrix for $\text{mult}(x) : L \otimes_K K_{\mathfrak{p}} \to L \otimes_K K_{\mathfrak{p}}$ (respectively $L_{P_i} \to L_{P_i}$) with respect to the basis B (respectively B_i). Then

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

hence

$$\begin{aligned} N_{L/K}(x) &= \det([\text{mult}(x)]_B) \\ &= \prod_{i=1}^r \det[\text{mult}(x)]_{B_i} \\ &= \prod_{i=1}^r N_{L_{P_i}/K_{\mathfrak{p}}}(x) \end{aligned}$$

□

11 Decomposition groups

Definition 11.1 (Ramification)**.** Let $0 \neq \mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and

$$\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$$

with P_i distinct prime ideals in $\mathcal{O}_L$, and $e_i > 0$.

(i) e_i is the *ramification index* of P_i over $\mathfrak{p}$.

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

Example. $\mathcal{O}_K = \mathbb{C}[t]$, $\mathcal{O}_L = \mathbb{C}[T]$. $\mathcal{O}_K \to \mathcal{O}_L$ sends $t \mapsto T^n$. Then $t\mathcal{O}_L = T^n\mathcal{O}_L$, so the ramification index of (T) over (t) is n.
Corresponds geometrically to the degree n of covering of Riemann surfaces $\mathbb{C} \to \mathbb{C}$, $x \mapsto x^n$.

Definition 11.2 (Residue class degree)**.** $f_i := [\mathcal{O}_L/P_i : \mathcal{O}_K/\mathfrak{p}]$ is the *residue class degree* of P_i over $\mathfrak{p}$.

Theorem 11.3. $\sum_{i=1}^r e_i f_i = [L : K]$.

Proof. Let $S = \mathcal{O}_K \setminus (\mathfrak{p})$. Exercise (properties of localisation):

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

(2) $S^{-1}\mathfrak{p}S^{-1}\mathcal{O}_L \cong S^{-1}P_1^{e_1} \cdots S^{-1}P_r^{e_r}$.

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

In particular, (2) and (3) imply e_i and f_i don't change when we replace $\mathcal{O}_K$ and $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$.

Thus we may assume that $\mathcal{O}_K$ is a discrete valuation ring (hence a PID). By Chinese remainder theorem, we have

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

We count dimension as $k := \mathcal{O}_K/\mathfrak{p}$ vector spaces.

RHS: for each i, there exists a decreasing sequence of k-suibspaces

$$0 \subseteq P_i^{e_i-1}/P_i^{e_i} \subseteq \cdots \subseteq P_i/P_i^{e_i} \subseteq \mathcal{O}_L/P_i^{e_i}.$$

Thus $\dim_k \mathcal{O}_L/P_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_k(P_i^j/P_i^{j+1})$. Note that P_i^j/P_i^{j+1} is an $\mathcal{O}_L/P_i$-module and $x \in P_i^j \setminus P_i^{j+1}$ is a generator (for example can prove this after localisation at P_i).

Then $\dim_k P_i^j/P_i^{j+1} = f_i$ and we have

$$\dim_k \mathcal{O}_L/P_i^{e_i} = e_i f_i,$$

and hence

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

LHS: Structure theorem for finitely generated modules over PIDs tells us that $\mathcal{O}_L$ is a free module over $\mathcal{O}_K$ of rank n.

Thus $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_K/\mathfrak{p})^n$ as k-vector spaces, hence $\dim_k \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$. □

Geometric analogue:

$f : X \to Y$ a degree n cover of compact Riemann surfaces. For $y \in Y$:

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

where e_x is the ramification index of x. Now assume L/K is Galois. Then for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(P_i) \cap \mathcal{O}_K = \mathfrak{p}$ and hence $\sigma(P_i) \in \{P_1, \dots, P_r\}$.

Proposition 11.4. The action of $\mathrm{Gal}(L/K)$ on $\{P_1, \dots, P_r\}$ is transitive.

Proof. Suppose not, so that there exists $i \neq j$ such that $\sigma(P_i) \neq P_j$ for all $\sigma \in \mathrm{Gal}(L/K)$.

By Chinese remainder theorem, we may choose $x \in \mathcal{O}_L$ such that $x \equiv 0 \mod P_i$, $x \equiv 1 \mod \sigma(P_i)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Then

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathcal{O}_K \cap P_i = \mathfrak{p} \subseteq P_j.$$

Since P_j prime, there exists $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(x) \in P_j$. Hence $x \in \tau^{-1}(P_j)$, i.e. $x \equiv 0 \mod \tau^{-1}(P_j)$, contradiction. □

Corollary 11.5. Suppose L/K is Galois. Then $e_1 = \cdots = e_r = e$, $f_1 = \cdots = f_r = f$, and we have $n = efr$.

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

(i) $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p})\mathcal{O}_L = \sigma(P_1)^{e_1} \cdots \sigma(P_r)^{e_r}$, hence $e_1 = \cdots = e_r$.

(ii) $\mathcal{O}_L/P_i \cong \mathcal{O}_L/\sigma(P_i)$ via σ. Hence $f_1 = \cdots = f_r$. □

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

Corollary 11.6. Let L/K be a finite separable extension. Then $[L : K] = ef$.

$\mathcal{O}_K$ a Dedekind domain:

Definition 11.7 (Decomposition)**.** Let L/K be a finite Galois extension. The decomposition at a prime P of $\mathcal{O}_L$ is the subgroup of $\mathrm{Gal}(L/K)$ defined by

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

Lecture 14

Proposition 11.8. Assuming that:

- $\mathcal{O}_K$ a Dedekind domain
- L/K a finite Galois extension
- $0 \neq P \subseteq \mathcal{O}_L$ a prime ideal
- $P \mid \mathfrak{p} \subseteq \mathcal{O}_K$

Then

(i) $L_P/K_{\mathfrak{p}}$ is Galois.

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

Proof.

(i) L/K Galois implies that L is a splitting field of a separable polynomial $f(X) \in K[X]$. Hence L_P is the splitting field of $f(X) \in K_[X]$, hence $L_P/K_{\mathfrak{p}}$ is Galois.

(ii) Let $\sigma \in \mathrm{Gal}(L_P/K_{\mathfrak{p}})$, then $\sigma(L) = L$ since L/K is normal, hence we have a map $\mathrm{res} : \mathrm{Gal}(L_P/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$, $\sigma \mapsto \sigma|_L$. Since L is dense in L_P, res is injective. By Lemma 8.2, we have
$$|\sigma(x)|_P = |x|_P$$

for all $\sigma \in \mathrm{Gal}(L_P/K_\mathfrak{p})$ and $x \in L_P$. Hence $\sigma(P) = P$ for all $\sigma \in \mathrm{Gal}(L_P/K_\mathfrak{p})$ and hence $\mathrm{res}(\sigma) \in G_P$ for all $\sigma \in \mathrm{Gal}(L_P/K_\mathfrak{p})$.

To show surjectivity, it suffices to show that

$$|G_P| = ef = [L_P : K_\mathfrak{p}].$$

Write $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$, $f = [\mathcal{O}_L/P : \mathcal{O}_K/\mathfrak{p}]$. Then

- $|G_P| = \frac{|\mathrm{Gal}(L/K)|}{r} = \frac{efr}{r} = ef$ (using Corollary 11.5).
- $[L_P : K_\mathfrak{p}] = ef$. Apply Corollary 11.6 to $L_P/K_\mathfrak{p}$, noting that e, f don't change when we take completions. □

Part V

Ramification Theory

$p = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Z}[i]$ if and only if $p = x^2 + y^2$.

We will consider L/K extension of algebraic number fields with $[L : K] = n$.

12 Different and discriminant

Notation. Let $x_1, \dots, x_n \in L$. Set

$$\begin{aligned}\Delta(x_1, \dots, x_n) &= \det(\mathrm{Tr}_{L/K}(x_i x_j)) \in K \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)\right) \\ &= \det(BB^\top)\end{aligned}$$

where $\sigma_k : L \to \overline{K}$ are distinct embeddings and $B = (\sigma_i(x_j))$.

Note:

- If $y_i = \sum_{j=1}^n a_{ij} x_j$, $a_{ij} \in K$, then
$$\Delta(y_1, \dots, y_n) = \det(A)^2 \Delta(x_1, \dots, x_n)$$
where $A = (a_{ij})$.
- If $x_1, \dots, x_n \in \mathcal{O}_L$, then $\Delta(x_1, \dots, x_n) \in \mathcal{O}_K$.

Lemma 12.1. Assuming that:

- k a perfect field
- R a k-algebra which is finite dimensional as a k-vector space

Then the Trace form

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

is non-degenerate if and only if $R = k_1 \times \cdots \times k_r$ where k_i/k is a finite separable extension of k.

Proof. Example Sheet 3. □

Theorem 12.2. Assuming that:

- $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal

Then

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

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

Proof.

(i) Let $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$, $0 \neq P_i \subseteq \mathcal{O}_L$ distinct prime ideals, $e_i > 0$. Define

$$R := \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \overset{\text{CRT}}{=} \prod_{i=1}^{r} \mathcal{O}_L/P_i^{e_i}.$$

If $\mathfrak{p}$ ramifies, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ has nilpotents. Hence

$$\Delta(\overline{x}_1, \ldots, \overline{x}_n) = 0 \qquad \forall \overline{x}_i \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L.$$

Then using the fact that

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & R = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \\ \big\downarrow \scriptstyle{\mathrm{Tr}_{L/K}} & & \big\downarrow \scriptstyle{\mathrm{Tr}_{R/k}} \\ \mathcal{O}_K & \longrightarrow & k = \mathcal{O}_K/\mathfrak{p} \end{array}$$

commutes, we get that

$$\Delta(x_1, \ldots, x_n) \equiv 0 \bmod \mathfrak{p} \qquad \forall x_i \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L.$$

(ii) $\mathfrak{p}$ unramified implies $R = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a product of finite extensions of k. By Lemma 12.1, we get that the Trace form is non-degenerate, hence for $\overline{x}_1, \ldots, \overline{x}_n$ a basis of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ as a k vector space, we have $\Delta(\overline{x}_1, \ldots, \overline{x}_n) \neq 0$. So thee exist $x_1, \ldots, x_n \in \mathcal{O}_L$ such that

$$\Delta(x_1, \ldots, x_n) \not\equiv 0 \bmod \mathfrak{p}.$$

□

Definition 12.3 (Discriminant)**.** The *discriminant* is the ideal $d_{L/K} \subseteq \mathcal{O}_K$ generated by $\Delta(x_1, \ldots, x_n)$ for all choices of $x_1, \ldots, x_n \in \mathcal{O}_L$.

Corollary 12.4. $\mathfrak{p}$ ramifies L if and only if $\mathfrak{p} \mid d_{L/K}$. In particular, only finitely many primes ramify in L.

Definition 12.5 (Inverse different)**.** The *inverse different* is

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

an $\mathcal{O}_L$ submodule of L.

Lemma 12.6. $D_{L/K}^{-1}$ is a fractional ideal in L.

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

$$d := \Delta(x_1, \dots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)),$$

which is non-zero since separable.

For $x \in D_{L/K}^{-1}$ write $x = \sum_{j=1}^{r} \lambda_j x_j$ with $\lambda_j \in K$. We show $\lambda_j \in \frac{1}{d}\mathcal{O}_K$. We have

$$\mathrm{Tr}_{L/K}(x x_i) = \sum_{j=1}^{n} \lambda_j \, \mathrm{Tr}_{L/K}(x_i x_j) \in \mathcal{O}_K.$$

Set $A_{ij} = \mathrm{Tr}_{L/K}(x_i x_j)$. Multiplying by $\mathrm{Adj}(A) \in M_n(\mathcal{O}_K)$, we get

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

Since $\lambda_i \in \frac{1}{d}\mathcal{O}_K$, we have $x \in \frac{1}{d}\mathcal{O}_L$. Thus $D_{L/K}^{-1} \le \frac{1}{d\mathcal{O}_K}$, so $D_{L/K}^{-1}$ is a fractional ideal. □

Lecture 15 The inverse $D_{L/K}$ of $D_{L/K}^{-1}$ is the different ideal.

Remark. $D_{L/K} \le \mathcal{O}_L$ since $\mathcal{O}_L \subseteq D_{L/K}^{-1}$.

Let I_L, I_K be the groups of fractional ideals.

Theorem 9.7 gives that

$$I_L \cong \bigotimes_{\substack{0 \ne P \\ \text{prime ideals in } \mathcal{O}_L}} \mathbb{Z}, \qquad I_K \cong \bigotimes_{\substack{0 \ne P \\ \text{prime ideals in } \mathcal{O}_K}} .$$

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

Fact:

$$\begin{array}{ccc} L^\times & \longrightarrow & I_L \\ \downarrow N_{L/K} & & \downarrow N_{L/K} \\ K^\times & \longrightarrow & I_K \end{array}$$

(Use Corollary 10.10 and $v_\mathfrak{p}(N_{L_P/K_\mathfrak{p}}(x)) = f_{P/\mathfrak{p}} v_(x)$ for $x \in L_P{}^\times$ where $v_\mathfrak{p}$ and v_P are the normalised valuations for L_P, $K_\mathfrak{p}$).

Theorem 12.7. $N_{L/K}(D_{L/K}) = d_{L/K}$.

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

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

But

$$\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2.$$

Thus

$$\Delta(x_1, \dots, x_n)\Delta(y_1, \dots, y_n) = 1.$$

Write $D_{L/K}^{-1} = \beta\mathcal{O}_L$ since $\beta \in L$. Then

$$\begin{aligned} d_{L/K}^{-1} &= (\Delta(x_1, \dots, x_n)^{-1}) \\ &= (\Delta(y_1, \dots, y_n)) \\ &= (\Delta(\beta x_1, \dots, \beta x_n)) && \text{change of basis matrix is invertible in } \mathcal{O}_K \\ &= N_{L/K}(\beta^2)\Delta(x_1, \dots, x_n) && \text{change of basis matrix is } [\mathrm{mult}(\beta)] \end{aligned}$$

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, localise at $S = \mathcal{O}_K \setminus \mathfrak{p}$ and use $S^{-1}D_{L/K} = D_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$. Then $S^{-1}d_{L/K} = d_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$. Details omitted. □

Theorem 12.8. Assuming that:

- $\mathcal{O}_L = \mathcal{O}_K[\alpha]$
- α has monic minimal polynomial $g(X) \in \mathcal{O}_K[X]$

Then $D_{L/K} = (g'(\alpha))$.

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

$$\frac{g(X)}{X - \alpha} = \beta_{n-1}X^{n-1} + \cdots + \beta_1 X + \beta_0$$

with $\beta_i \in \mathcal{O}_L$ and $\beta_{n-1} = 1$. We claim

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

for $0 \le r \le n-1$.

Indeed the difference is a palynomial of degree $< n$, which vanishes for $X = \alpha_1, \ldots, \alpha_n$. Equate coefficients of X^s, which gives

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

Since $1, \alpha, \ldots, \alpha^{n-1}$ is an $\mathcal{O}_K$ basis for $\mathcal{O}_L$, $D_{L/K}^{-1}$ has an $\mathcal{O}_K$ basis

$$\frac{\beta_0}{g'(\alpha)}, \frac{\beta_1}{g'(\alpha)}, \ldots, \underbrace{\frac{\beta_{n-1}}{g'(\alpha)}}_{\frac{1}{g'(\alpha)}}.$$

Note all of these are $\mathcal{O}_L$ multiples of the last term, since the β_i are in $\mathcal{O}_L$. So $D_{L/K}^{-1} = \frac{1}{(g'(\alpha))}$, hence $D_{L/K} = (g'(\alpha))$. □

P a prime ideal of $\mathcal{O}_L$, $\mathfrak{p} = \mathcal{O}_K \cap P$. $D_{L_P/K_\mathfrak{p}}$ using $\mathcal{O}_{K_\mathfrak{p}}$, $\mathcal{O}_{L_P}$. We identify $D_{L_P/K_\mathfrak{p}}$ with a power $\mathcal{P}$.

Theorem 12.9. $D_{L/K} = \prod_{\mathcal{P}} D_{L_P/K_\mathfrak{p}}$ (finite product, see later).

Proof. Let $x \in L$, $\mathfrak{p} \subseteq \mathcal{O}_K$. Then

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

(of Corollary 10.10).

Let $r(\mathcal{P}) = v_{\mathcal{P}}(D_{L/K})$, $s(\mathcal{P}) = v_{\mathcal{P}}(D_{L_P/K_\mathfrak{p}})$.

$\subseteq$ (i.e. $r(\mathcal{P}) \ge s(\mathcal{P})$). Let $x \in L$ with $v_{\mathcal{P}}(x) \ge -s(\mathcal{P})$ for all $\mathcal{P}$. Then $\mathrm{Tr}_{L_P/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$, for all $y \in L$ and for all $\mathcal{P}$. Using $(*)$ we get

$$\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_{K_\mathfrak{p}} \qquad \forall y \in \mathcal{O}_L, \forall \mathcal{P}.$$

Thus

$$\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K \qquad \forall y \in \mathcal{O}_L$$

so $D_{L/K} \subseteq \prod_{\mathcal{P}} D_{L_{\mathcal{P}}/K_\mathfrak{p}}$.

$\supseteq$ (i.e. $r(\mathcal{P}) \leq s(\mathcal{P})$). Fix $\mathcal{P}$ and let $x \in P^{-r(P)} \setminus P^{-r(P)+1}$. Then $v_P(x) = -r(P)$, $v_{P'}(x) \geq 0$ for all $P' \neq P$. By $(*)$, we have

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

hence

$$\mathrm{Tr}_{L_P/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}} \qquad \forall y \in \mathcal{O}_{L_P}.$$

Hence $x \in D_{L_P/K_\mathfrak{p}}^{-1}$, i.e. $-v_P(x) = r(P) \leq s(P)$. So $D_{L/K} \supseteq \prod_P D_{L_P/K_\mathfrak{p}}$. □

Corollary 12.10. $d_{L/K} = \prod_{P|\mathfrak{p}} d_{L_P/K_\mathfrak{p}}$.

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

13 Unramified and totally ramified extensions of local fields

Let L/K be a finite separable extension of non-archimedean local fields. Corollary 11.6 implies

$$[L : K] = e_{L/K} f_{L/K}. \qquad (*)$$

Lemma 13.1. Assuming that:

- $M/L/K$ finite separable extensions of local fields

Then

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

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

Proof.

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

(ii) (i) and $(*)$. ☐

Definition 13.2 (Unramified / ramified / totally ramified)**.** The extension L/K is said to be:

- *unramified* if $e_{L/K} = 1$ (equivalently $f_{L/K} = [L : K]$).
- *ramified* if $e_{L/K} > 1$ (equivalently $f_{L/K} < [L : K]$).
- *totally ramified* if $e_{L/K} = [L : K]$ (equivalently $f_{L/K} = 1$).

Lecture 16

From now on in this course: if unspecified L/K is a finite separable extension of (non-archimedean) local fields. Also, all local fields that we consider from now on will be non-archimedean.

Theorem 13.3. Assuming that:

- L/K a finite separable extension of non-archimedean local fields

Then there exists a field K_0, $K \subseteq K_0 \subseteq L$ and such that

(i) K_0 is unramified

(ii) L/K_0 is totally ramified

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

Proof. Let $k = \mathbb{F}_q$, so that $k_L = \mathbb{F}_{q^f}$, $f_{L/K} = f$. Set $m = q^f - 1$, $[\bullet] : \mathbb{F}_{q^f} \to L$ the Teichmüller map for L.

Let $\zeta_m := [\alpha]$ for α a generator of $\mathbb{F}_{q^f}^\times$. ζ_m a primitive m-th root of unity. Set $K_0 = K(\zeta_m) \subseteq L$, then K_0/K is Galois and has residue field $k_0 = \mathbb{F}_q(\alpha) = k_L$. Hence $f_{L/K_0} = 1$, i.e. L/K_0 is totally ramified.

Let $\text{res} : \text{Gal}(K_0/K) \to \text{Gal}(k_0/k)$ be the natural map. For $\sigma \in \text{Gal}(K_0/K)$. We have $\sigma(\zeta_m) = \zeta_m$ if $\sigma(\zeta_m) \equiv \zeta_m \bmod m$ (since $\mu_m(K_0) \cong \mu_m(k_0)$ by Hensel's Lemma version 1). Hence res is injective. Thus $|\text{Gal}(K_0/K)| \le |\text{Gal}(k_0/k)| = f_{K_0/K}$, so $[K_0 : K] = f_{K_0/K}$.

Hence res is an isomorphism, and K_0/K is unramified. □

Theorem 13.4. Assuming that:

- $k = \mathbb{F}_q$
- $n \ge 1$

Then there exists a unique unramified L/K of degree n. Moreover, L/K is Galois and the natural $\text{Gal}(L/K) \to \text{Gal}(k_L/k)$ is an isomorphism. In particular, $\text{Gal}(L/K) \cong \langle \text{Frob}_{L/K} \rangle$ is cyclic, where $\text{Frob}_{L/K}(x) = x^q \bmod m_L$ for all $x \in \mathcal{O}_L$.

Proof. For $n \ge 1$, take $L = K(\zeta_m)$ where $m = q^n - 1$.

As in Theorem 13.3:
$$\text{Gal}(L/K) \xrightarrow{\sim} \text{Gal}(k_L/K) \cong \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q).$$
Hence $\text{Gal}(L/K)$ is cyclic, generated by a lift of $x \mapsto x^q$.

Uniqueness: L/K of degree n unramified. Then Teichmüller gives $\zeta_m \in L$, so $L = K(\zeta_m)$. □

Corollary 13.5. L/K a finite Galois extension. Then $\text{res} : \text{Gal}(L/K) \to \text{Gal}(k_L/k)$ is surjective.

Proof. res factorises as
$$\text{Gal}(L/K) \twoheadrightarrow \text{Gal}(K_0/K) \xrightarrow{\sim} \text{Gal}(k_L/k).$$
□

Definition 13.6 (Inertial subgroup)**.** The inertial subgroup is
$$I_{L/K} = \ker(\text{Gal}(L/K) \twoheadrightarrow \text{Gal}(k_L/k)).$$

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

- $I_{L/K} = \text{Gal}(L/K_0) - K_0$ as in Theorem 13.3.

Definition 13.7 (Eisenstein polynomial)**.** $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$ is *Eisenstein* if $v_K(a_i) \geq 1$ for all i, and $v_K(a_0) = 1$.

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

Theorem 13.8. (i) Let L/K finite totally ramified, $\pi_L \in \mathcal{O}_L$ a uniformiser. Then the minimal polynomial of π_L is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ (hence $L = K(\pi_L)$)

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

Proof.

(i) $[L : K] = e = e_{L/K}$. Let

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

the minimal polynomial for π_L. Then $m \leq e$. Since $v_L(K^\times) = e\mathbb{Z}$, we have $v_L(a_i\pi^i) \equiv e \bmod e$, for $i < m$. Hence these terms 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 $v_K(a_i) \geq 1$ for all i.

Hence $v_K(a_0) = 1$ and $m = e$. Thus $f(x)$ is Eisenstein and $L = K(\pi_L)$. For $y \in L$, we write $y = \sum_{i=0}^{e-1} \pi_L^i b_i$, $b_i \in K$. Then

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

Thus

$$\begin{aligned} y \in \mathcal{O}_L &\iff v_L(y) \geq 0 \\ &\iff v_K(b_i) \geq 0 \forall i \\ &\iff y \in \mathcal{O}_K[\pi_L] \end{aligned}$$

(ii) Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is Eisenstein and $e = e_{L/K}$. Thus $v_L(a_i) \geq e$ and $v_L(a_0) = e$. If $v_L(\alpha) \leq 0$, we have

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

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

$$v_L(\alpha^n) = v_L\left(-\sum_{i=0}^{n-1} a_i\alpha^i\right) = v_L(a_0) = e.$$

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

□

13.1 Structure of Units

Let $[K : \mathbb{Q}] < \infty$, $e := e_{K/\mathbb{Q}_p}$, π a uniformiser in K.

Proposition 13.9. Assuming that:

- $r > \frac{e}{p-1}$

Then $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ converges on $\pi^r\mathcal{O}_K$ and induces an isomorphism

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

Proof.

$$\begin{aligned} v_K(n!) &= ev_p(n!) \\ &= \frac{e(n - s_p(n))}{p-1} && \text{Example Sheet 1} \\ &\leq e\left(\frac{n-1}{p-1}\right) \end{aligned}$$

For $x \in \pi^r\mathcal{O}_K$ and $n \geq 1$,

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

Lecture 17 Hence $v_K\left(\frac{x^n}{n!}\right) \to \infty$ as $n \to \infty$. Thus $\exp(x)$ converges.

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

Consider log: $1 + \pi^r\mathcal{O}_K \to \pi^r\mathcal{O}_K$.

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

which converges as before.

Recall identities in $\mathbb{Q}[[X,Y]]$:

$$\begin{aligned}\exp(X+Y) &= \exp(X)\exp(Y)\\ \exp(\log(1+X)) &= 1+X\\ \log(\exp(X)) &= X\end{aligned}$$

Thus $\exp;(\pi^r\mathcal{O}_K,+) \xrightarrow{\sim} (1+\pi^r\mathcal{O}_K,\times)$ is an isomorphism. □

K *any* local field: $U_K := \mathcal{O}_K^\times$, $\pi \in \mathcal{O}_K$ uniformiser.

Definition 13.10 (s-th unit group)**.** For $s \in \mathbb{Z}$, the s-th unit group $U_K^{(s)}$ is defined by

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

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

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

Proposition 13.11.

(i) $U_K^{(0)}/U_K^{(i)} \cong (k^\times,\times)$ $(k \cong \mathcal{O}_K/\pi)$

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

Proof.

(i) Reduction modulo π. $\mathcal{O}_K^\times \to k^\times$ is surfective with kernel $1+\pi\mathcal{O}_K = U_K^{(1)}$.

(ii) $f; U_K^{(s)} \to k$, $1+\pi^s x \mapsto x \mod \pi$.

$$(1+\pi^s x)(1+\pi^s y) = 1+\pi^s(x+y+\pi^s xy).$$

$x+y+\pi^s xy \equiv x+y \bmod \pi$, hence f is a group homomorphism, surjective with kernel $U_K^{(s+1)}$.

□

Remark. Let $[K:\mathbb{Q}_p] < \infty$. Proposition 13.9, **??** implies that there exists finite index subgroup of $\mathcal{O}_K^\times$ isomorphism to $(\mathcal{O}_K,+)$.

Example. $\mathbb{Z}_p$, $p > 2$, $e = 1$, take $r = 1$. Then

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

$p = 2$, take $r = 2$.

$$\begin{aligned} \mathbb{Z}_2^\times &\xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + p^2\mathbb{Z}_p) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \\ x &\mapsto \left(x \bmod 4, \frac{x}{\varepsilon(x)} \right) \end{aligned}$$

where

$$\varepsilon(x) = \begin{cases} +1 & x \equiv 1 \pmod 4 \\ -1 & x \equiv -1 \pmod 4 \end{cases}$$

So:

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

14 Higher Ramification Groups

Let L/K be a finite Galois extension of local fields, and $\pi_L \in \mathcal{O}_L$ a uniformiser.

Definition 14.1 (s-th ramification group)**.** Let v_L be a normalised valuation in $\mathcal{O}_L$. For $s \in \mathbb{R}_{\geq -1}$, the s-th ramification group is

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

Remark. G_s only changes at integers.
G_s, $s \in \mathbb{R}_{\geq -1}$ used to define upper numbering.

Example.

$$\begin{aligned} G_{-1}(L/K) &= \mathrm{Gal}(L/K) \\ G_0(L/K) &= \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \bmod \pi_L \ \forall x \in \mathcal{O}_L\} \\ &= \ker(\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k)) \\ &= I_{L/K} \end{aligned}$$

Note. For $s \in \mathbb{Z}_{\geq 0}$,

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

hence $G_s(L/K)$ is normal in G_{-1}.

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

Theorem 14.2.

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

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

(iii) Let $s \in \mathbb{Z}_{\geq 0}$. Then there exists an injective group homomorphism
$$G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$$
induced by $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$. This map is independent of the choice of π_L.

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

(i) Theorem 13.8 implies $\mathcal{O}_L/\mathcal{O}_K[\pi_L]$. Suppose $v_L(\sigma(\pi_L)-\pi_L) \geq s+1$. Let $x \in \mathcal{O}_L$, then $x = f(\pi_L)$, $f(X) \in \mathcal{O}_K[X]$.

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

for some $g(X) \in \mathcal{O}_K[X]$, using the fact that $X^n - Y^n = (X-Y)(X^{n-1} + \cdots + Y^{n-1})$. Thus

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

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

(iii) Note: for $\sigma \in G_s$, $s \in \mathbb{Z}_{\geq 0}$,

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

hence

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

We claim

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

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

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

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

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

Hence φ is a group homomorphism. Moreover,

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

If $\pi_L' = a\pi_L$ is another uniformiser, $a \in \mathcal{O}_L^\times$. Then

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

Corollary 14.3. $\mathrm{Gal}(L/K)$ is solvable.

Lecture 18

Proof. By Proposition 13.11, Theorem 14.2 and Theorem 13.4, for $s \in \mathbb{Z}_{\geq -1}$,

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

Thus G_s/G_{s+1} is solvable for $s \geq -1$. Conclude using Theorem 14.2(ii). □

Let characteristic $k = p$. Then $p \nmid |G_0/G_1|$ and $|G_1| = p^n$. Thus G_1 is the unique (since normal) Sylow p-subgroup of $G_0 = I_{L/K}$.

Definition 14.4. G_1 is called the wild inertial group, and G_0/G_1 is called the tame quotient.

Suppose L/K is finite separable. Say L/K is tamely ramified if characteristic $k \nmid e_{L/K}$. Otherwise it is wildly ramified.

Theorem 14.5. Assuming that:

- $[K : \mathbb{Q}_p] < \infty$
- L/K finite
- $D_{L/K} = (\pi^{\delta(L/K)})$

Then $\delta(L/K) \geq e_{L/K} - 1$, with equality if and only if tamely ramified. In particular, L/K unramified if and only if $D_{L/K} = \mathcal{O}_L$.

Proof. Example Sheet 3 shows $D_{L/K} = D_{L/K_0} \cdot D_{K_0/K}$. Suffices to check 2 cases:

(i) L/K unramified. Then **??** gives that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, for some $\alpha \in \mathcal{O}_L$ with $k_L = k(\overline{\alpha})$.

Let $g(X) \in O_K[X]$ be the minimal polynomial of α. Since $[L : K] = [k_L : k]$, we have that $\overline{g}(X) \in k[X]$ is the minimal polynomial of $\overline{a}$. $\overline{g}(X)$ separable and hence $g'(\alpha) \not\equiv 0 \pmod{\pi}_L$. Theorem 12.8 implies $D_{L/K} = (g(\alpha)) = \mathcal{O}_L$.

(ii) L/K totally ramified. Say $[L : K] = e$, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, π_L a root of

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

is Eisenstein. Then

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

Thus $v_L(y'(\pi_L)) \geq e-1$. Equality if and only if $p \nmid e$. □

Corollary 14.6. Suppose L/K is an extension of number fields. Let $P \subseteq \mathcal{O}_L$, $P \cap \mathcal{O}_K = \mathfrak{p}$. Then $e(P/\mathfrak{p}) > 1$ if and only if $P \mid D_{L/K}$.

Proof. Theorem 12.9 implies $D_{L/K} = \prod_P D_{L_P/K_\mathfrak{p}}$. Then use $e(P/\mathfrak{p}) = e_{L_P/K_\mathfrak{p}}$ and Theorem 14.5. □

Example.

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

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

  See Example Sheet 3.

- $\Phi_{p^n}(X)$ irreducible (hence $\Phi_{p^n}(X)$ is the minimal polynomial of ζ_{p^n}).
- $L/\mathbb{Q}_p$ is Galois, totally ramified of degree $p^{n+1}(p-1)$.
- $\pi := \zeta_{p^n} - 1$ a uniformiser in $\mathcal{O}_L \rightsquigarrow \mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^n} - 1] = \mathbb{Z}_p[\zeta_{p^n}]$.
- $\mathrm{Gal}(L/\mathbb{Q}_p) \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times$ (abelian). $\sigma_m \leftrightarrow m$ where $\sigma_m(\zeta_{p^n}) = \zeta_{p^n}^m$.

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

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

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

  Theorem 14.2(i) implies that $\sigma_m \in G_i$ if and only if $p^k \geq i+1$. Thus

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

Part VI

Local Class Field Theory

15 Infinite Galois Theory

Definition 15.1 (Infinite Galois definitions)**.**

- L/K is separable if $\forall \alpha \in L$, the minimal polynomial $f_\alpha(X) \in K[X]$ for α is separable.
- L/K is normal if $f_\alpha(X)$ splits in L for all $\alpha \in L$.
- L/K is Galois if it is separable and normal. Write $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ in this case. If L/K is a finite Galois extension, then we have a Galois correspondence:

$$\{\text{subextensions } K \subseteq K' \subseteq L\} \leftrightarrow \{\text{subgroups of } \mathrm{Gal}(L/K)\}$$
$$K' \mapsto \mathrm{Gal}(K/K')$$

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

Example.

- Any total order (for example $(\mathbb{N}, \leq)$).
- $\mathbb{N}_{\geq 1}$ ordered by divisibility.

Definition 15.2. Let $(I, \leq)$ be a directed set and $(G_i)_{i \in I}$ a collection of groups together with maps $\varphi_{ij} : G_j \to G_i$, $i \leq j$ such that:

- $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ for any $i \leq j \leq k$
- $\varphi_{ii} = \mathrm{id}$

Say $((G_i)_{i=1}, \varphi_{ij})$ is an inverse system. The inverse limit of (G_i, φ_i) is

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

Remark.

- $(\mathbb{N}, \leq)$ recovers the previous set.
- There exist projection maps $\varphi_j : \varprojlim_{i \in I} G_i \to G_j$.
- $\varprojlim_{i \in I} G_i$ satisfies a universal property.
- Assume G_i finite. Then the profinite topology on $\varprojlim_{i \in I} G_i$ is the weakest topology such that φ_j are continuous for all $j \in I$.

Proposition 15.3. Assuming that:

- L/K Galois

Then

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

(ii) For $F, F' \in I$, $F \subseteq F'$ 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. Example Sheet 4. □

Index