Part III - Local Fields

Lectured by Rong Zhou

Artur Avameri

Michaelmas 2023

Contents

0 Introduction

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

1 Absolute values

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

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

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

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

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

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

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

  We will ignore this in this course.

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

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

  We can check the axioms:

  (1) The first axiom is clear.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a contradiction. The other inequality is analogous.

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

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

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

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

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

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

Example 1.1.

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

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

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

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

Convergence is easier in non–archimedean fields:

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

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

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

so (x_n) is Cauchy. □

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

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

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

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

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

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

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

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

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

Let $(K, |\cdot|)$ be a non–archimedean valued field. For $x \in K$ and $r \in \mathbb{R}_{>0}$, we define $B(x, r) = \{y \in K \mid |y - x| < r\}$ and $\overline{B} = \{y \in K \mid |y - x| \leq r\}$ to be the open and closed balls of radius r. 10 Oct 2022, Lecture 2

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

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

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

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

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

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

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

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

□

2 Valuation rings

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

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

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

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

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

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

Example 2.1.

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

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

Definition 2.3. Let $(K, |\cdot|)$ be a non–archimedean valued field. The **valuation ring** of K is defined to be
$$\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}.$$
(i.e. the closed unit ball, $\mathcal{O}_K = \overline{B}(0,1)$, or $\mathcal{O}_K = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$).

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

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

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

Proof. (i) We find:

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

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

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

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

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

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

□

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

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

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

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

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

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

Example 2.3.

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

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

Lemma 2.3. Let v be a valuation on K. Then the following are equivalent:

(i) v is discrete;

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

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

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

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

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

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

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

12 Oct 2022, Lecture 3

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

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

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

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

Proof. (i) $\mathcal{O}_K$ is a PID by the previous lemma, hence any nonzero prime ideal is maximal. Since $\mathcal{O}_K$ is a local ring, it is a DVR.

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

□

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

3 p–adic numbers

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

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

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

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

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

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

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

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

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

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

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

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

The inverse limit satisfies the following universal property:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(ii) Left as exercise on example sheet 1.

□

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

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

14 Oct 2022, Lecture 4

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

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

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

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

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

□

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

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

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

4 Complete valued fields

4.1 Hensel's lemma

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

Proof. Let $\pi \in \mathcal{O}_K$ be a uniformizer and let $r = v(f'(a))$ for v a normalized valuation, i.e. $v(\pi) = 1$. We inductively construct a sequence (x_n) in $\mathcal{O}_K$ such that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof. Left as an exercise on example sheet 1. $\square$

17 Oct 2022, Lecture 5

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

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

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

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

5 Teichmüller lifts

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

giving us the second property.

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

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

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

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

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

$\square$

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

More generally:

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

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

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

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

6 Extensions of complete valued fields

19 Oct 2022, Lecture 6

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

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

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

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

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

Facts:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(iii) For this, we need some preparation:

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

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

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

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

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

Proof. Exercise on example sheet 2. □

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

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

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

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

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

Assuming this, let $x, y \in L$ and WLOG assume $|x|_L \leq |y|_L$. Then we he $\left|\frac{x}{y}\right|_L \leq 1 \implies \frac{x}{y} \in \mathcal{O}_L$. Since $\mathcal{O}_L$ is a ring, $1 \in \mathcal{O}_L$, so $1 + \frac{x}{y} \in \mathcal{O}_L$ and hence $\left|1 + \frac{x}{y}\right|_L \leq 1$, so $|x + y|_L \leq |y|_L = \max(|x|_L, |y|_L)$, giving the ultrametric inequality property. 21 Oct 2022, Lecture 7

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

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

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

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

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

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

Corollary 6.6. Let $(K, |\cdot|)$ be a complete, nonarchimedean discretely valued field and L/K a finite extension. Then

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

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

Proof. (i) Fix v, the valuation on K responding to our absolute value, and let v_L be the valuation on L extending v. Let $n = [L : K]$. For $y \in L^\times$, $|y|_L = |N_{L/K}(y)|^{1/n}$, so $v_L(y) = \frac{1}{n} v(N_{L/K}(y))$, so $v_L(L^\times) \subset \frac{1}{n} v(K^\times)$. Since $v(K^\times)$ is discrete, so is v_L.

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7 Local fields

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

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

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

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

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

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

24 Oct 2022, Lecture 8

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For the profinite topology, $\mathcal{O}_K \to \mathcal{O}_K/\pi^n\mathcal{O}_K$ is continuous if and only if $a + \pi^n\mathcal{O}_K$ is open $\forall a \in \mathcal{O}_K$. □

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

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

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

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

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

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

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

for some $n \geq 1$.

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

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

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

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

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

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

26 Oct 2022, Lecture 9

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 Global fields

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

(i) an algebraic number field.

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

Lemma 8.1. Let $(K, |\cdot|)$ be a complete discretely valued field and L/K a finite Galois extension with absolute value $|\cdot|_L$ extending $|\cdot|_K$. Then for $x \in L$ and $\sigma \in \mathrm{Gal}(L/K)$, we have $|\sigma(x)|_L = |x|_L$.

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

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

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

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

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

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

Informally, "nearby" polynomials define the same extension.

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

29 Oct 2022, Lecture 10

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

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

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

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

9 Dedekind domains

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

(i) R is a Noetherian integral domain.

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

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

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

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

We start with two lemmas.

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

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

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

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

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

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

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

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

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

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

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

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

Example 9.2.

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

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

Fact. There exists a bijection between

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

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

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

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

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

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

31 Oct 2022, Lecture 11

Definition 9.3. If R is a Dedekind domain and $\mathfrak{p} \subset R$ is a nonzero prime ideal, we write $v_{\mathfrak{p}}$ for the normalized valuation on $\mathrm{Frac}(R) = \mathrm{Frac}(R_{(\mathfrak{p})})$ corresponding to the DVR $R_{(\mathfrak{p})}$.

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

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

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

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

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

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

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

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

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

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

10 Dedekind domains and extensions

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

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

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

The converse is also true and is left as an exercise on example sheet 3: A finite extension L/K is separable if and only if the trace form is nondegenerate.

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

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

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

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

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

We prove:

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

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

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

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

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

□

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

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

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

02 Nov 2022, Lecture 12

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

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

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

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

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

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

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

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

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

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

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

Corollary 10.6. Let K be a number field with ring of integers $\mathcal{O}_K$. Then any absolute value on K is equivalent to either

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

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

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

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

10.1 Completions

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

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

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

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

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

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

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

Proof. Exercise on example sheet 2. □

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

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

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

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

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

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

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

To prove these:

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

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

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

□

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

04 Nov 2022, Lecture 13

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

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

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

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

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

□

11 Decomposition groups

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

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

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

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

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

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

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

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

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

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

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

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

In particular, (2) and (3) imply that e_i, f_i don't change when we replace $\mathcal{O}_K$ and $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$. Thus we may assume that $\mathcal{O}_K$ is a DVR (and hence a PID). By CRT, we have

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The formula now follows from Theorem 11.1. □

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

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

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

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

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

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

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