Local Fields

Lectured by Dr Rong Zhou
Typed by David Kurniadi Angdinata

Michaelmas 2020

Syllabus

Contents

1 Basic theory

Lecture 1 Friday 09/10/20

How can we find solutions to Diophantine equations? Let $f(X_1, \dots, X_r) \in \mathbb{Z}[X_1, \dots, X_r]$ be a polynomial with integer coefficients. What are integer or rational solutions to $f(X_1, \dots, X_r) = 0$? Finding solutions to Diophantine equations in general is a very difficult problem. Consider a related but much simpler problem of solving the congruences

$$f(X_1, \dots, X_r) \equiv 0 \mod p, \qquad \dots, \qquad f(X_1, \dots, X_r) \equiv 0 \mod p^n, \qquad \dots.$$

Now this is just a finite computation, since modulo primes there are only finitely many choices for solutions, so this is a much easier problem. Local fields give a way to package all this information together.

1.1 Absolute values

Definition 1.1.1. Let K be a field. An **absolute value** on K is a function $|\cdot| : K \to \mathbb{R}_{\ge 0}$ such that

1. $|x| = 0$ if and only if $x = 0$,
2. $|xy| = |x||y|$ for all $x, y \in K$, and
3. the triangle inequality $|x + y| \le |x| + |y|$ for all $x, y \in K$.

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

Example.

- Let $K = \mathbb{R}$ or $K = \mathbb{C}$ with the usual absolute value. Write $|\cdot|_\infty$ for this absolute value.
- Let K be any field. The **trivial absolute value** on K is defined by

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

  Ignore this case in this course.
- Let $K = \mathbb{Q}$ and p a prime. For $0 \ne x \in \mathbb{Q}$, write $x = p^n(a/b)$, where $a, b \in \mathbb{Z}$ such that $(a, p) = 1$ and $(b, p) = 1$. The **p-adic absolute value** is defined to be

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

  Axiom 1 is clear. Write $y = p^m(c/d)$. Axiom 2 is

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

  Without loss of generality $m \ge n$. Axiom 3 is

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

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

Exercise. $+$ and $\cdot$ are continuous.

Definition 1.1.2. Let $|\cdot|$ and $|\cdot|'$ be absolute values on a field K. We say $|\cdot|$ and $|\cdot|'$ are **equivalent** if they induce the same topology. An equivalence class of absolute values is called a **place**.

Proposition 1.1.3. *Let $|\cdot|$ and $|\cdot|'$ be non-trivial absolute values on K. The following are equivalent.*

1. *$|\cdot|$ and $|\cdot|'$ are equivalent.*
2. *$|x| < 1$ if and only if $|x|' < 1$ for all $x \in K$.*
3. *There exists $c \in \mathbb{R}_{>0}$ such that $|x|^c = |x|'$ for all $x \in K$.*

Proof.

$1 \implies 2$. $|x| < 1$ if and only if $x^n \to 0$ with respect to $|\cdot|$, if and only if $x^n \to 0$ with respect to $|\cdot|'$, if and only if $|x|' < 1$.

$2 \implies 3$. Let $a \in K^\times$ such that $|a| < 1$, which exists since $|\cdot|$ is non-trivial. We need to show that

$$\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}, \qquad x \in K^\times.$$

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

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

Then we have $n \log|x| < m \log|a|$ and $n \log|x|' > m \log|a|'$, so $|x^n/a^m| < 1$ and $|x^n/a^m|' > 1$, a contradiction. Similarly for $\log|x| / \log|a| > \log|x|' / \log|a|'$.

$3 \implies 1$. Clear.

□

This course is mainly interested in the following types of absolute values.

Definition 1.1.4. 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, then it is **archimedean**.

Example.

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

Lemma 1.1.5 (All triangles are isosceles)**.** *Let $(K, |\cdot|)$ be a non-archimedean valued field and $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$.*

Fact.

- $|1| = |-1| = 1$.
- $|-y| = |y|$.

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

Convergence is easier for non-archimedean $|\cdot|$.

Proposition 1.1.6. *Let $(K, |\cdot|)$ be non-archimedean and $(x_n)_{n=1}^\infty$ a sequence in K. If $|x_n - x_{n+1}| \to 0$, 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 $\epsilon > 0$, choose N such that $|x_n - x_{n+1}| < \epsilon$ for all $n > N$. Then for $N < n < m$,

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

so $(x_n)_{n=1}^\infty$ is Cauchy. □

Example. Let $p = 5$. Construct a sequence $(x_n)_{n=1}^{\infty}$ such that

1. $x_n^2 + 1 \equiv 0 \mod 5^n$, and
2. $x_n \equiv x_{n+1} \mod 5^n$,

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

$$x_{n+1}^2 + 1 = x_n^2 + 2bx_n5^n + b^2 5^{2n} + 1 = a5^n + 2x_n b5^n + b^2 5^{2n} \equiv (a + 2x_n b) 5^n \mod 5^{n+1}.$$

We choose b such that $a + 2x_n b \equiv 0 \mod 5$. Then we have $x_{n+1}^2 + 1 \equiv 0 \mod 5^{n+1}$ as desired. By 2, $(x_n)_{n=1}^{\infty}$ is Cauchy. Suppose $x_n \to L \in \mathbb{Q}$. Then $x_n^2 \to L^2$. But by 1, $x_n^2 \to -1$, so $L^2 = -1$, a contradiction. Thus $(\mathbb{Q}, |\cdot|_5)$ is not complete.

Definition 1.1.7. The ***p*-adic numbers** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Remark. By analogy, $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$.

Let K be a non-archimedean valued field. For $x \in K$ and $r \in \mathbb{R}_{>0}$, define Lecture 2 Monday 12/10/20

$$\mathrm{B}(x, r) = \{y \in K \mid |x - y| < r\}, \qquad \overline{\mathrm{B}}(x, r) = \{y \in K \mid |x - y| \le r\}.$$

Lemma 1.1.8. *Let $(K, |\cdot|)$ be non-archimedean.*

1. *If $z \in \mathrm{B}(x, r)$, then $\mathrm{B}(z, r) = \mathrm{B}(x, r)$, so open balls do not have centres.*
2. *If $z \in \overline{\mathrm{B}}(x, r)$, then $\overline{\mathrm{B}}(z, r) = \overline{\mathrm{B}}(x, r)$.*
3. *$\mathrm{B}(x, r)$ is closed.*
4. *$\overline{\mathrm{B}}(x, r)$ is open.*

Proof.

1. Let $y \in \mathrm{B}(x, r)$. Then $|x - y| < r$, so $|z - y| = |(z - x) + (x - y)| \le \max(|z - x|, |x - y|) < r$. Thus $\mathrm{B}(x, r) \subseteq \mathrm{B}(z, r)$. The reverse inclusion follows by symmetry.
2. Same as 1.
3. Let $y \notin \mathrm{B}(x, r)$. If $z \in \mathrm{B}(x, r) \cap \mathrm{B}(y, r)$, then $\mathrm{B}(x, r) = \mathrm{B}(z, r) = \mathrm{B}(y, r)$, so $y \in \mathrm{B}(x, r)$, a contradiction. Thus $\mathrm{B}(x, r) \cap \mathrm{B}(y, r) = \emptyset$.
4. If $z \in \overline{\mathrm{B}}(x, r)$, then $\mathrm{B}(z, r) \subseteq \overline{\mathrm{B}}(z, r) = \overline{\mathrm{B}}(x, r)$, by 2.

□

1.2 Valuation rings

Definition 1.2.1. Let K be a field. A **valuation** on K is a function $v : K^\times \to \mathbb{R}$ such that

- $v(xy) = v(x) + v(y)$, and
- $v(x + y) \ge \min(v(x), v(y))$.

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

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

determines a non-archimedean absolute value. Conversely, a non-archimedean absolute value determines a valuation $v(x) = \log_a |x|$.

Remark.

- We ignore the trivial valuation $v(x) = 0$ for all $x \in K^\times$ corresponding to the trivial absolute value.
- Say v_1 and 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.

- If $K = \mathbb{Q}$, then $\mathrm{v}_p(x) = -\log_p |x|_p$ is the **p-adic valuation**.
- If k is a field and $K = k(t) = \operatorname{Frac} k[t]$ is the **rational function field**, then
$$\mathrm{v}\left(t^n \frac{f(t)}{g(t)}\right) = n, \qquad f, g \in k[t], \qquad f(0), g(0) \neq 0$$
is the **t-adic valuation**.
- If $K = k((t)) = \operatorname{Frac} k[[t]] = \left\{\sum_{i=n}^{\infty} a_i t^i \mid a_i \in k,\ n \in \mathbb{Z}\right\}$ is the **field of formal Laurent series** over k, then
$$\mathrm{v}\left(\sum_i a_i t^i\right) = \min\{i \mid a_i \neq 0\}$$
is the t-adic valuation on K.

Definition 1.2.2. Let $(K, |\cdot|)$ be a non-archimedean valued field. The **valuation ring** of K is defined to be
$$\mathcal{O}_K = \overline{\mathrm{B}}(0,1) = \{x \in K \mid |x| \leq 1\} = \left\{x \in K^\times \mid v(x) \geq 0\right\} \cup \{0\}.$$

Proposition 1.2.3.

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

Proof.

1. By last lecture, $|1| = 1$, so $1 \in \mathcal{O}_K$. Since $|0| = 0$, $0 \in \mathcal{O}_K$. Since $|-1| = 1$, $|-x| = |x|$. Thus if $x \in \mathcal{O}_K$, then $-x \in \mathcal{O}_K$. 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 ring. Since $\mathcal{O}_K = \overline{\mathrm{B}}(0,1)$ it is open.
2. Similar to 1.
3. Note that $|x|\left|x^{-1}\right| = \left|xx^{-1}\right| = 1$. Thus $|x| = 1$ if and only if $\left|x^{-1}\right| = 1$, if and only if $x, x^{-1} \in \mathcal{O}_K$, if and only if $x \in \mathcal{O}_K^\times$.

$\square$

Notation.

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

A ring is **local** if it has a unique maximal ideal.

Exercise. R is local if and only if $R \setminus R^\times$ is an ideal.

Corollary 1.2.4. *$\mathcal{O}_K$ is a local ring with unique maximal ideal $\mathfrak{m}$.*

Example.

- If $K = k((t))$, then $\mathcal{O}_K = k[[t]]$, $\mathfrak{m} = \langle t \rangle$, and $\kappa = k$.
- If $K = \mathbb{Q}$ with $|\cdot|_p$, then $\mathcal{O}_K = \mathbb{Z}_{(\langle p \rangle)}$, $\mathfrak{m} = p\mathbb{Z}_{(\langle p \rangle)}$, and $\kappa = \mathbb{F}_p$.

Definition 1.2.5. Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \cong \mathbb{Z}$, we say v is a **discrete valuation**, and K is said to be a **discretely valued field**. An element $\pi \in \mathcal{O}_K$ is a **uniformiser** if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$.

Example.

- $K = \mathbb{Q}$ with the p-adic valuation.
- $K = k(t)$ with the t-adic valuation.

Remark. If v is a discrete valuation, we can replace it with an equivalent one such that $v(K^\times) = \mathbb{Z} \subseteq \mathbb{R}$. Such v are called **normalised valuations**. Then $v(\pi) = 1$ for π a uniformiser.

Lemma 1.2.6. *Let v be a valuation on K. The following are equivalent.*

1. *v is discrete.*
2. *$\mathcal{O}_K$ is a PID.*
3. *$\mathcal{O}_K$ is Noetherian.*
4. *$\mathfrak{m}$ is principal.*

Proof.

$1 \implies 2$. 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 $x\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq v(x)\} \subseteq I$, and hence $x\mathcal{O}_K = I$ by definition of x.

$2 \implies 3$. Clear.

$3 \implies 4$. Write $\mathfrak{m} = \mathcal{O}_K x_1 + \dots + \mathcal{O}_K x_n$. Without loss of generality $v(x_1) \leq \dots \leq v(x_n)$. Then $\mathfrak{m} = \mathcal{O}_K x_1$.

$4 \implies 1$. Let $\mathfrak{m} = \mathcal{O}_K \pi$ for some $\pi \in \mathcal{O}_K$ and let $c = v(\pi)$. Then if $v(x) > 0$, then $x \in \mathfrak{m}$ and hence $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \emptyset$. Since $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, we have $v(K^\times) = c\mathbb{Z}$.

□

Lemma 1.2.7. *Let v be a discrete valuation on K and $\pi \in \mathcal{O}_K$ a uniformiser. For all $x \in K^\times$, there exist $n \in \mathbb{Z}$ and $u \in \mathcal{O}_K^\times$ such that $x = \pi^n u$. In particular $K = \mathcal{O}_K[1/x]$ for any $x \in \mathfrak{m}$ and hence $K = \operatorname{Frac} \mathcal{O}_K$.*

Proof. For $x \in K^\times$, let n such that $v(x) = nv(\pi) = v(\pi^n)$, then $v(x\pi^{-n}) = 0$, so $u = x\pi^{-n} \in \mathcal{O}_K^\times$. □

Definition 1.2.8. 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 1.2.9.

1. *Let v be a discrete valuation on K. Then $\mathcal{O}_K$ is a DVR.*
2. *Let R be a DVR. Then there exists a valuation v on $K = \operatorname{Frac} R$ such that $R = \mathcal{O}_K$.*

Proof.

1. $\mathcal{O}_K$ is a PID by Lemma 1.2.6. Let $0 \neq I \subseteq \mathcal{O}_K$ be an ideal, then $I = \langle x \rangle$. If $x = \pi^n u$ for π a uniformiser, then $\langle x \rangle$ is prime if and only if $n = 1$ and $I = \langle \pi \rangle = \mathfrak{m}$.
2. Let R be a DVR with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = \langle \pi \rangle$ for some $\pi \in R$. By unique factorisation of PIDs, we may write any $x \in R \setminus \{0\}$ uniquely as $\pi^n u$ for $n \geq 0$ and $u \in R^\times$. Then any $y \in K \setminus \{0\}$ can be written uniquely as $\pi^m u$ for $u \in R^\times$ and $m \in \mathbb{Z}$. Define $v(\pi^m u) = m$. It is easy to check v is a valuation and $\mathcal{O}_K = R$.

□

Example.

- $\mathbb{Z}_{(\langle p \rangle)}$ is a DVR, the valuation ring of $|\cdot|_p$ on $\mathbb{Q}$.
- The ring of formal power series $k[[t]] = \left\{\sum_{n \geq 0} a_n t^n \;\middle|\; a_n \in k\right\}$ is a DVR, the valuation ring for the t-adic absolute value on $k((t))$.
- Non-example. If $K = k(t)$ is the rational function field and $K' = K\left(t^{1/2}, t^{1/4}, \dots\right)$, then the t-adic valuation extends to K', and $\mathrm{v}\left(t^{1/2^n}\right) = 1/2^n$ is not discrete.

1.3 The p-adic numbers

Lecture 3 Wednesday 14/10/20

Recall that $\mathbb{Q}_p$ is defined to be the completion of $\mathbb{Q}$ with respect to the metric induced by $|\cdot|_p$. By example sheet 1, $\mathbb{Q}_p$ is a field, $|\cdot|_p$ extends to $\mathbb{Q}_p$, and the associated valuation is discrete, so $\mathbb{Q}_p$ is a discretely valued field.

Definition 1.3.1. The ring of **p-adic integers** $\mathbb{Z}_p$ is the valuation ring

$$\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \;\middle|\; |x|_p \le 1\right\}.$$

Fact.

- $\mathbb{Z}_p$ is a DVR with maximal ideal $p\mathbb{Z}_p$.
- The non-zero ideals in $\mathbb{Z}_p$ are $p^n\mathbb{Z}_p$ for $n \in \mathbb{N}$.

Proposition 1.3.2. *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. In particular $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$.*

Proof. Need to show $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ and $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is open, $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$. Then

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

the localisation at $\langle p\rangle$. Thus it suffices to show $\mathbb{Z}$ is dense in $\mathbb{Z}_{(\langle p\rangle)}$. Let $a/b \in \mathbb{Z}_{(\langle p\rangle)}$ for $a, b \in \mathbb{Z}$ and $p \nmid b$. For $n \in \mathbb{N}$, choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \mod p^n$. Then $y_n \to a/b$ as $n \to \infty$. In particular, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, which is complete. ☐

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

$$\varprojlim_n A_n = \left\{(a_n)_{n=1}^\infty \in \prod_{n=1}^\infty A_n \;\middle|\; \phi_n(a_{n+1}) = a_n\right\},$$

so

$$\begin{array}{ccccc} A_{n+1} & \xrightarrow{\phi_n} & A_n & \xrightarrow{\phi_{n-1}} & A_{n-1} \\ a_{n+1} & \longmapsto & a_n & \longmapsto & a_{n-1} \end{array}.$$

Fact. If A_n is a group or ring, then $\varprojlim_n A_n$ is a group or ring.

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

Proposition 1.3.3. *Let $((A_n)_{n=1}^\infty, (\phi_n)_{n=1}^\infty)$ as above. Then for any set or group or ring B together with homomorphisms $\psi_n : B \to A_n$ such that*

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

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

Proof. Define

$$\begin{array}{cccc} \psi & : & B & \longrightarrow & \prod_{n=1}^\infty A_n \\ & & b & \longmapsto & \prod_{n=1}^\infty \psi_n(b) \end{array}.$$

Then $\psi_n = \phi_n \circ \psi_{n+1}$ implies that $\psi(b) \in \varprojlim_n A_n$. The map is clearly unique, determined by $\psi_n = \phi_n \circ \psi_{n+1}$, and is a homomorphism of rings. ☐

Definition 1.3.4. Let R be a ring and $I \subseteq R$ an ideal. The ***I*-adic completion** of R is the ring

$$\widehat{R} = \varprojlim_n R/I^n,$$

where $\phi_n : R/I^{n+1} \to R/I^n$ is the natural projection. Note there is a natural map $\iota : R \to \widehat{R}$ by the universal property. We say that R is ***I*-adically complete** if ι is an isomorphism.

Fact. $\ker\left(\iota : R \to \widehat{R}\right) = \bigcap_{n=1}^{\infty} I^n$.

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

Proposition 1.3.5. *Assume K is complete.*

1. *Then $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$, so $\mathcal{O}_K$ is π-adically complete.*
2. *If in addition K is discretely valued and π is a uniformiser, then every $x \in \mathcal{O}_K$ can be written uniquely as $x = \sum_{i=0}^{\infty} a_i\pi^i$ for $a_i \in A$, where A is a set of coset representatives for $\kappa = \mathcal{O}_K/\pi\mathcal{O}_K$. Moreover, any series $\sum_{i=0}^{\infty} a_i\pi^i$ converges to an element in $\mathcal{O}_K$.*

Proof.

1. Let $\iota : \mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$. Since $\bigcap_{n=1}^{\infty} \pi^n\mathcal{O}_K = \{0\}$, ι is injective. Let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ and for each n, choose $y_n \in \mathcal{O}_K$ a lift of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$. Let v be the valuation on K normalised such that $v(\pi) = 1$, then $v(y_n - y_{n+1}) \geq n$, since $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$, so $(y_n)_{n=1}^{\infty}$ is a Cauchy sequence in $\mathcal{O}_K$. But $\mathcal{O}_K$ is complete, since $\mathcal{O}_K \subseteq K$ is closed, so $y_n \to y$, and y maps to $(x_n)_{n=1}^{\infty}$. Thus ι is surjective.
2. Let $x \in \mathcal{O}_K$. Choose a_i inductively. Choose $a_0 \in A$ such that $a_0 \equiv x \mod \pi$. Suppose have chosen $a_0, \dots, a_k$ such that $\sum_{i=0}^{k} a_i\pi^i \equiv x \mod \pi^{k+1}$. Then $\sum_{i=0}^{k} a_i\pi^i - x = c\pi^{k+1}$ for $c \in \mathcal{O}_K$. Choose $a_{k+1} \equiv -c \mod \pi$. Then $\sum_{i=0}^{k+1} a_i\pi^i \equiv x \mod \pi^{k+2}$, so $\sum_{i=0}^{\infty} a_i\pi^i = x$. For uniqueness, assume $\sum_{i=0}^{\infty} a_i\pi^i = \sum_{i=0}^{\infty} b_i\pi^i \in \mathcal{O}_K$. Then let n be minimal such that $a_n \neq b_n$. Then $\sum_{i=0}^{\infty} a_i\pi^i \not\equiv \sum_{i=0}^{\infty} b_i\pi^i \mod \pi^{n+1}$, a contradiction.

□

A warning is if $(K,|\cdot|)$ is not discretely valued, $\mathcal{O}_K$ is not necessarily $\mathfrak{m}$-adically complete.

Corollary 1.3.6. *If K is as in Proposition 1.3.5.2, then every $x \in K$ can be written uniquely as $\sum_{i=n}^{\infty} a_i\pi^i$ for $a_i \in A$. Conversely any such expression defines an element of K.*

Proof. Use $K = \mathcal{O}_K\left[\frac{1}{\pi}\right]$. □

Corollary 1.3.7.

1. *$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.*
2. *Every element of $\mathbb{Q}_p$ can be written uniquely as $\sum_{i=n}^{\infty} a_ip^i$ for $a_i \in \{0, \dots, p-1\}$.*

Proof.

1. By Proposition 1.3.5, it suffices 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. We have $\ker f_n = \left\{x \in \mathbb{Z} \,\middle|\, |x|_p \leq p^{-n}\right\} = p^n\mathbb{Z}$, so $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is injective. Let $\overline{c} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, and $c \in \mathbb{Z}_p$ a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, can choose $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$, which is open in $\mathbb{Z}_p$, so $f_n(x) = \overline{c}$. Thus $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective.
2. Follows from Corollary 1.3.6 noting that $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

□

Example.

- $1/(1-p) = 1 + p + \dots \in \mathbb{Q}_p$.
- Let $K = k((t))$ with the t-adic valuation. Then $\mathcal{O}_K = k[[t]] = \varprojlim_n k[[t]]/\langle t^n\rangle$. Moreover $\mathcal{O}_K$ is the t-adic completion of $k[t]$.

2 Complete valued fields

2.1 Hensel's lemma

Lecture 4 Friday 16/10/20

For complete valued fields, there is a nice way to produce solutions in $\mathcal{O}_K$ to certain equations from solutions modulo $\mathfrak{m}$.

Theorem 2.1.1 (Hensel's lemma version 1)**.** *Let $(K,|\cdot|)$ be a complete discretely valued field. Let $f(X) \in \mathcal{O}_K[X]$ and assume there exists $a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$, where $f'(a)$ is the formal derivative such that if $f(X) = X^n$ then $f'(X) = nX^{n-1}$. 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 $r = v(f'(a))$ for v a normalised valuation, so $v(\pi) = 1$.

- We construct a sequence $(x_n)_{n=1}^{\infty}$ in $\mathcal{O}_K$ such that

  1. $f(x_n) \equiv 0 \mod \pi^{n+2r}$, and
  2. $x_{n+1} \equiv x_n \mod \pi^{n+r}$.

  Take $x_1 = a$, then $f(x_1) \equiv 0 \mod \pi^{1+2r}$. Suppose have constructed $x_1, \dots, x_n$ satisfying 1 and 2. Define
  $$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

  2. Since $x_n \equiv x_1 \mod \pi^{1+r}$, $v(f'(x_n)) = r$ and hence $f(x_n)/f'(x_n) \equiv 0 \mod \pi^{n+r}$ by 1. It follows that $x_{n+1} \equiv x_n \mod \pi^{n+r}$ so 2 holds.
  1. Note that for X and Y indeterminates,
  $$f(X+Y) = f^{(0)}(X) + f^{(1)}(X)Y + \dots, \qquad f^{(i)}(X) \in \mathcal{O}_K[X].$$
  Thus
  $$f(x_{n+1}) = f(x_n) + f'(x_n)c + \dots, \qquad c = -\frac{f(x_n)}{f'(x_n)}.$$
  Since $c \equiv 0 \mod \pi^{n+r}$ and $v\left(f^{(i)}(x_n)\right) \geq 0$, we have $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \mod \pi^{n+2r+1}$, so 1 holds.

  This gives the construction of $(x_n)_{n=1}^{\infty}$. By property 2, $(x_n)_{n=1}^{\infty}$ 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 1.
  - Moreover 2 implies $a = x_1 \equiv x_n \mod \pi^{1+r}$ for all n, so $a \equiv x \mod \pi^{1+r}$, so $|x-a| < |f'(a)|$.

  This proves existence.

- For uniqueness, suppose x' also satisfies $f(x') = 0$ and $|x'-a| < |f'(a)|$. Set $\delta = x' - x \neq 0$. Then $|x'-a| < |f'(a)|$, $|x-a| < |f'(a)|$, and the ultrametric inequality implies $|\delta| = |x-x'| < |f'(a)| = |f'(x)|$. But
  $$0 = f(x') = f(x+\delta) = f(x) + f'(x)\delta + \underbrace{\dots}_{|\cdot| \leq |\delta|^2},$$
  where $f(x) = 0$. Hence $|f'(x)\delta| \leq |\delta|^2$, so $|f'(x)| \leq |\delta|$, a contradiction.

$\square$

Corollary 2.1.2. *Let $(K,|\cdot|)$ be a complete discretely valued field. Let $f(X) \in \mathcal{O}_K[X]$ and $\overline{c} \in \kappa = \mathcal{O}_K/\mathfrak{m}$ a simple root of $\overline{f}(X) = f(X) \mod \mathfrak{m} \in \kappa[X]$. Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $x \equiv \overline{c} \mod \mathfrak{m}$.*

Proof. Apply Theorem 2.1.1 to a lift $c \in \mathcal{O}_K$ of $\overline{c}$. Then $|f(c)| < |f'(c)|^2 = 1$ since $\overline{c}$ is a simple root. $\square$

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

Corollary 2.1.3.

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

Proof.

$p > 2$. Let $b \in \mathbb{Z}_p^\times$. Applying Corollary 2.1.2 to $f(X) = X^2 - b$, we find that $b \in \left(\mathbb{Z}_p^\times\right)^2$ if and only if $b \in \left(\mathbb{F}_p^\times\right)^2$. Thus $\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2 \cong \mathbb{F}_p^\times / \left(\mathbb{F}_p^\times\right)^2 \cong \mathbb{Z}/2\mathbb{Z}$ since $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. We have an isomorphism $\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$ given by $(u, n) \mapsto up^n$. Thus $\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$.

$p = 2$. Let $b \in \mathbb{Z}_2^\times$. Consider $f(X) = X^2 - b$. Then $f'(X) = 2X \equiv 0 \mod 2$. Let $b \equiv 1 \mod 8$. Then $|f(1)|_2 \le 2^{-3} < |f'(1)|_2^2 = 2^{-2}$. By Hensel's lemma, $f(X)$ has a root in $\mathbb{Z}_2$, so $b \in \left(\mathbb{Z}_2^\times\right)^2$ if and only if $b \equiv 1 \mod 8$. Thus $\mathbb{Z}_2^\times / \left(\mathbb{Z}_2^\times\right)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$. Again using $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$, we find that $\mathbb{Q}_2^\times / \left(\mathbb{Q}_2^\times\right)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$.

$\square$

Remark. The proof of Hensel's lemma uses the iteration $x_{n+1} = x_n - f(x_n)/f'(x_n)$, the non-archimedean analogue of the Newton-Raphson method.

For later applications, we need the following version of Hensel's lemma.

Theorem 2.1.4 (Hensel's lemma version 2)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(X) \in \mathcal{O}_K[X]$. Suppose $\overline{f}(X) = f(X) \mod \mathfrak{m} \in \kappa[X]$ factorises as $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$ in $\kappa[X]$, with $\overline{g}(X)$ and $\overline{h}(X)$ coprime. Then there is a factorisation $f(X) = g(X)h(X)$ in $\mathcal{O}_K[X]$, with $\overline{g}(X) = g(X) \mod \mathfrak{m}$, $\overline{h}(X) = h(X) \mod \mathfrak{m}$, and $\deg \overline{g} = \deg g$.*

Proof. Example sheet 1. $\square$

Corollary 2.1.5. *Let $f(X) = a_n X^n + \dots + a_0 \in K[X]$ with $a_0, a_n \neq 0$. If $f(X)$ is irreducible, then $|a_i| \le \max(|a_0|, |a_n|)$ 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 be minimal such that $|a_r| = 1$, then $0 < r < n$. Thus we have $\overline{f}(X) = X^r\left(a_r + \dots + a_n X^{n-r}\right) \mod \mathfrak{m}$. Then Theorem 2.1.4 implies $f(X) = g(X)h(X)$, with $0 < \deg g = r < n$. $\square$

2.2 Teichmüller lifts

Lecture 5 Monday 19/10/20

Recall that in lecture 3 every element of $x \in \mathbb{Q}_p$ can be written as $x = \sum_{i=n}^\infty a_i p^i$ for $a_i \in A = \{0, \dots, p-1\}$, but $\mathbb{F}_p \to A \subseteq \mathbb{Z}_p$ does not respect any algebraic structure. It turns out there is a natural choice of coset representatives in many cases which does respect some algebraic structure.

Definition 2.2.1. A ring R of characteristic p is a **perfect ring** if the Frobenius $x \mapsto x^p$ is an automorphism of R. A field of characteristic p is a **perfect field** if it is perfect as a ring.

Remark. Since $\operatorname{ch} R = p$, $(x+y)^p = x^p + y^p$, so Frobenius is a ring homomorphism.

Example.

- $\mathbb{F}_{p^n}$ and $\overline{\mathbb{F}_p}$ are perfect fields.
- $\mathbb{F}_p[t]$ is not perfect, since $t \notin \operatorname{im} \mathrm{Fr}$.
- $\mathbb{F}_p\left(t^{1/p^\infty}\right) = \mathbb{F}_p\left(t, t^{1/p}, \dots\right)$ is a perfect field, the **perfection** of $\mathbb{F}_p(t)$. The t-adic absolute value extends to $\mathbb{F}_p\left(t^{1/p^\infty}\right)$, and the completion of $\mathbb{F}_p\left(t^{1/p^\infty}\right)$ is a **perfectoid field**.

Fact. A field K is perfect if and only if any finite extension of K is separable.

Theorem 2.2.2. *Let $(K,|\cdot|)$ be a complete discretely valued field such that $\kappa = \mathcal{O}_K/\mathfrak{m}$ is a perfect field of characteristic p. Then there exists a unique map $[\cdot] : \kappa \to \mathcal{O}_K$ such that*

1. *$a \equiv [a] \mod \mathfrak{m}$ for all $a \in \kappa$, and*
2. *$[ab] = [a][b]$ for all $a, b \in \kappa$.*

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

Definition 2.2.3. The element $[a] \in \mathcal{O}_K$ constructed in Theorem 2.2.2 is called the **Teichmüller lift** of a.

The following is the idea of the proof. Let $\alpha \in \mathcal{O}_K$ be any lift of $a \in \kappa$. Then α is well-defined up to $\pi\mathcal{O}_K$. Let $\beta \in \mathcal{O}_K$ be a lift of $a^{1/p}$. We claim that β is a better lift. Why? Let $\beta' \in \mathcal{O}_K$ be another lift of $a^{1/p}$, then $\beta = \beta' + \pi u$ for $u \in \mathcal{O}_K$, so

$$\beta^p = (\beta' + \pi u)^p = \beta'^p + \underbrace{\sum_{i=1}^{p} \binom{p}{i} \beta'^{p-i} (\pi u)^i}_{\in \pi^2 \mathcal{O}_K},$$

using $p \in \langle \pi \rangle$, so β^p is well-defined up to $\pi^2\mathcal{O}_K$. Repeat this process to get better and better lifts.

Lemma 2.2.4. *Let $(K,|\cdot|)$ be as in Theorem 2.2.2, and fix $\pi \in \mathcal{O}_K$ a uniformiser. Let $x, y \in \mathcal{O}_K$ such that $x \equiv y \mod \pi^k$ for $k \geq 1$. Then $x^p \equiv y^p \mod \pi^{k+1}$.*

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

$$x^p = \sum_{i=0}^{p} \binom{p}{i} \left(u\pi^k\right)^i y^{p-i} = y^p + pu\pi^k y^{p-1} + \sum_{i=2}^{p} \binom{p}{i} y^{p-i} \left(u\pi^k\right)^i.$$

Since $\mathcal{O}_K/\pi\mathcal{O}_K$ has characteristic p, we have $p \in \langle \pi \rangle$. Thus $pu\pi^k y^{p-1} \in \pi^{k+1}\mathcal{O}_K$. For $i \geq 2$, $\left(u\pi^k\right)^i \in \pi^{k+1}\mathcal{O}_K$, so $x^p \equiv y^p \mod \pi^{k+1}$. ☐

Proof of Theorem 2.2.2. Let $a \in \kappa$.

- For each $i \geq 0$ we choose a lift $y_i \in \mathcal{O}_K$ of a^{1/p^i}, and we define

$$x_i = y_i^{p^i}.$$

  Then $x_i \equiv y_i^{p^i} \equiv \left(a^{1/p^i}\right)^{p^i} \equiv a \mod \pi$. We claim that $(x_i)_{i=1}^{\infty}$ is a Cauchy sequence, and its limit $x_i \to x$ is independent of the choice of y_i.

  - By construction $y_i \equiv y_{i+1}^p \mod \pi$. By Lemma 2.2.4 and induction on k, we have $y_i^{p^k} \equiv y_{i+1}^{p^{k+1}} \mod \pi^{k+1}$, and hence $x_i \equiv x_{i+1} \mod \pi^{i+1}$, by taking $k = i$, so $|x_i - x_{i+1}| \to 0$. Then $(x_i)_{i=1}^{\infty}$ 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^{1/p^i}. Then x_i' 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 $(x_i'')_{i=1}^{\infty}$ is Cauchy and $x_i'' \to x$ and $x_i'' \to x'$, so $x = x'$, hence x is independent of y_i.

  We define $[a] = x$.

  1. $x \equiv a \mod \pi$, so 1 is satisfied.

2. We let $b \in \kappa$ and we choose $u_i \in \mathcal{O}_K$ a lift of b^{1/p^i}, and let $z_i = u_i^{p^i}$. Then $\lim_{i\to\infty} z_i = [b]$. Now $u_i y_i$ is a lift of $(ab)^{1/p^i}$, 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 2 is satisfied. If $\operatorname{ch} \mathcal{O}_K = p$, then $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$. Then
$$[a+b] = \lim_{i\to\infty} (y_i + u_i)^{p^i} = \lim_{i\to\infty} \left(y_i^{p^i} + u_i^{p^i}\right) = \lim_{i\to\infty} (x_i + z_i) = [a] + [b]\,.$$
It is easy to check that $[0] = 0$ and $[1] = 1$, so $[\cdot]$ is a ring homomorphism.

- For uniqueness, let $\phi : \kappa \to \mathcal{O}_K$ be another such map. Then for $a \in \kappa$, $\phi\left(a^{1/p^i}\right)$ is a lift of a^{1/p^i}, it follows that
$$[a] = \lim_{i\to\infty} \phi\left(a^{1/p^i}\right)^{p^i} = \lim_{i\to\infty} \phi(a) = \phi(a)\,.$$

□

Example 2.2.5. Let $K = \mathbb{Q}_p$, and let $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$. If $a \in \mathbb{F}_p^\times$, then $[a]^{p-1} = \left[a^{p-1}\right] = [1] = 1$, so $[a]$ is a $(p-1)$-th root of unity.

More generally is the following.

Lemma 2.2.6. *Let $(K, |\cdot|)$ be a complete discretely valued field. If $\kappa = \mathcal{O}_K/\mathfrak{m} \subseteq \overline{\mathbb{F}_p}$, then $[a] \in \mathcal{O}_K^\times$ is a root of unity.*

Proof. If $a \in \kappa$, then $a \in \mathbb{F}_{p^n}$ for some n, so $[a]^{p^n-1} = \left[a^{p^n-1}\right] = [1] = 1$. □

Theorem 2.2.7. *Let $(K, |\cdot|)$ be a complete discretely valued field with $\operatorname{ch} K = p > 0$. Assume κ is perfect, then $K \cong \kappa((t))$.*

Proof. Since $K = \operatorname{Frac} \mathcal{O}_K$, it suffices to show $\mathcal{O}_K \cong \kappa[[t]]$. Fix $\pi \in \mathcal{O}_K$ a uniformiser, let $[\cdot] : \kappa \to \mathcal{O}_K$ be the Teichmüller map, and define
$$\begin{array}{cccc} \phi & : & \kappa[[t]] & \longrightarrow & \mathcal{O}_K \\ & & \sum_{i=0}^\infty a_i t^i & \longmapsto & \sum_{i=0}^\infty [a_i]\,\pi^i \end{array}.$$
Then ϕ is a ring homomorphism since $[\cdot]$ is a ring homomorphism and it is a bijection by Proposition 1.3.5.2. □

2.3 Extensions of complete valued fields

Lecture 6
Wednesday
21/10/20

Theorem 2.3.1. *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field and L/K a finite extension of degree n.*

1. *$|\cdot|$ extends uniquely to an absolute value $|\cdot|_L$ on L defined by*
$$|y|_L = \left|\mathrm{N}_{L/K}(y)\right|^{\frac{1}{n}}, \qquad y \in L.$$
2. *L is complete with respect to $|\cdot|_L$.*

Recall that if L/K is finite,
$$\begin{array}{cccc} \mathrm{N}_{L/K} & : & L & \longrightarrow & K \\ & & y & \longmapsto & \det_K(\cdot y) \end{array},$$
where $\cdot y : L \to L$ is the K-linear map induced by multiplication by y.

Fact.

- $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\,\mathrm{N}_{L/K}(y)$.
- Let $X^n + a_{n-1}X^{n-1} + \dots + a_0 \in K[X]$ be the minimal polynomial of $y \in L$. Then $\mathrm{N}_{L/K}(y) = \pm a_0^m$ for $m \geq 1$.

Definition 2.3.2. Let $(K, |\cdot|)$ be a non-archimedean valued field and V a vector space over K. A **norm** on V is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ satisfying

- $\|x\| = 0$ if and only if $x = 0$,
- $\|\lambda x\| = |\lambda| \|x\|$ for all $\lambda \in K$ and $x \in V$, and
- $\|x + y\| \leq \max(\|x\|, \|y\|)$ for all $x, y \in V$.

Example. If V is finite-dimensional and $e_1, \dots, e_n$ is a basis of V, the **sup norm** on V is defined by

$$\|x\|_{\sup} = \max_i |x_i|, \qquad x = \sum_{i=1}^{n} x_i e_i.$$

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

Definition 2.3.3. Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on V are **equivalent** if there exist $C, D > 0$ such that

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

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

Proposition 2.3.4. *Let $(K, |\cdot|)$ be complete non-archimedean and V a finite-dimensional vector space over K. Then V is complete with respect to $\|\cdot\|_{\sup}$.*

Proof. Let $(v_i)_{i=1}^{\infty}$ be a Cauchy sequence in V and $e_1, \dots, e_n$ a basis for V. Write $v_i = \sum_{j=1}^{n} x_j^i e_j$. Then $\left(x_j^i\right)_{i=0}^{\infty}$ 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 2.3.5. *Let $(K, |\cdot|)$ be complete non-archimedean and V 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 any norm $\|\cdot\|$ is equivalent to $\|\cdot\|_{\sup}$. Let $e_1, \dots, e_n$ be a basis for V, and set $D = \max_i \|e_i\|$. 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 $C\|\cdot\|_{\sup} \leq \|\cdot\|$, we induct on $n = \dim V$.

$n = 1$. $\|x\| = \|x_1 e_1\| = |x_1| \|e_1\|$ so take $C = \|e_1\|$, since $|x_1| = \|x\|_{\sup}$.

$n > 1$. Set $V_i = \langle e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n \rangle$. By induction, V_i is complete with respect to $\|\cdot\|$, 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 zero. Thus there exists $C > 0$ such that $\mathrm{B}(0, C) \cap S = \emptyset$ where $\mathrm{B}(0, C) = \{x \in V \mid \|x\| < C\}$. Let $x = \sum_{i=1}^{n} x_i e_i$ and suppose $|x_j| = \max_i |x_i|$. Then $\|x\|_{\sup} = |x_j|$, and $(1/x_j) x \in S$. Thus $\|(1/x_j) x\| \geq C$, so $\|x\| \geq C|x_j| = C\|x\|_{\sup}$.

The completeness of V follows since V is complete with respect to $\|\cdot\|_{\sup}$. ☐

Definition 2.3.6. Let $R \subseteq S$ be rings.

- 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

$$R^{\mathrm{Int}\, S} = \{s \in S \mid s \text{ is integral over } R\}.$$

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

Proposition 2.3.7. *$R^{\mathrm{Int}\, S}$ is a subring of S. Moreover $R^{\mathrm{Int}\, S}$ is integrally closed in S.*

Proof. Example sheet 2. ☐

Lemma 2.3.8. *Let $(K, |\cdot|)$ be a non-archimedean valued field. Then $\mathcal{O}_K$ is integrally closed in K.*

Proof. Let $x \in K$ be integral over $\mathcal{O}_K$, and 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 $x = -a_{n-1} - \cdots - a_0/x^{n-1}$. If $|x| > 1$, we have $\left|-a_{n-1} - \cdots - a_0/x^{n-1}\right| \leq 1$, a contradiction. Thus $|x| \leq 1$, so $x \in \mathcal{O}_K$. ☐

Proof of Theorem 2.3.1.

1. We show $|\cdot|_L = |\mathrm{N}_{L/K}(\cdot)|^{1/n}$ satisfies the three axioms in the definition of absolute values.

    1. $|y|_L = 0$ if and only if $|\mathrm{N}_{L/K}(y)|^{1/n} = 0$, if and only if $\mathrm{N}_{L/K}(y) = 0$, if and only if $y = 0$, by property of $\mathrm{N}_{L/K}$.
    2. $|y_1 y_2|_L^n = |\mathrm{N}_{L/K}(y_1 y_2)| = |\mathrm{N}_{L/K}(y_1)\mathrm{N}_{L/K}(y_2)| = |\mathrm{N}_{L/K}(y_1)||\mathrm{N}_{L/K}(y_2)| = |y_1|_L^n |y_2|_L^n$.
    3. Set
    $$\mathcal{O}_L = \{y \in L \mid |y|_L \leq 1\}.$$
    Claim that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ inside L.
        - Let $0 \neq y \in \mathcal{O}_L$ and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ be the minimal polynomial of y. By property of $\mathrm{N}_{L/K}$, there exists $m \geq 1$ such that $\mathrm{N}_{L/K}(y) = \pm a_0^m$. By Corollary 2.1.5, we have $|a_i| \leq \max\left(|\mathrm{N}_{L/K}(y)|^{1/m}, 1\right) = 1$, since $|\mathrm{N}_{L/K}(y)| \leq 1$. Thus $a_i \in \mathcal{O}_K$ for all i, so $f \in \mathcal{O}_K[X]$, so y is integral over $\mathcal{O}_K$.
        - Conversely let $y \in L$ be integral over $\mathcal{O}_K$. Again by property of $\mathrm{N}_{L/K}$, we have $\mathrm{N}_{L/K}(y) = \left(\prod_{\sigma : L \to \overline{K}} \sigma(y)\right)^d$ for $d \geq 1$, where $\overline{K}$ is an algebraic closure of K and σ runs over K-algebra homomorphisms. For all such $\sigma : L \to \overline{K}$, $\sigma(y)$ is integral over $\mathcal{O}_K$. Thus $\mathrm{N}_{L/K}(y) \in K$ is integral over $\mathcal{O}_K$. By Lemma 2.3.8, $\mathrm{N}_{L/K}(y) \in \mathcal{O}_K$, so $|\mathrm{N}_{L/K}(y)| \leq 1$, so $y \in \mathcal{O}_L$.

    Thus $\mathcal{O}_K^{\mathrm{Int}\,L} = \mathcal{O}_L$ and proves the claim. Now we prove 3. Let $x, y \in L$. Without loss of generality assume $|x|_L \leq |y|_L$, then $|x/y|_L \leq 1$, so $x/y \in \mathcal{O}_L$. Since $1 \in \mathcal{O}_L$ and $\mathcal{O}_K^{\mathrm{Int}\,L} = \mathcal{O}_L$, we have $1 + x/y \in \mathcal{O}_L$ and hence $|1 + x/y|_L \leq 1$, so $|x + y|_L \leq |y|_L = \max(|y|_L, |x|_L)$. Thus 3 is satisfied.

    To check $|\cdot|_L$ extends $|\cdot|$ use $\mathrm{N}_{L/K}(x) = x^n$ for $x \in K$. If $|\cdot|_L'$ is another absolute value on L extending $|\cdot|$, then note that $|\cdot|_L$ and $|\cdot|_L'$ are norms on L. By Theorem 2.3.5, $|\cdot|_L'$ and $|\cdot|_L$ induce the same topology on L, so $|\cdot|_L' = |\cdot|_L^c$ for some $c > 0$. Since $|\cdot|_L'$ extends $|\cdot|$, we have $c = 1$.

2. Since $|\cdot|_L$ defines a norm on K, Theorem 2.3.5 implies L is complete with respect to $|\cdot|_L$.

□

Lecture 7 Friday 23/10/20

Corollary 2.3.9. *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field and L/K a finite extension. Then*

1. *L is discretely valued with respect to $|\cdot|_L$, and*
2. *$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.*

Proof.

1. Let v be a valuation on K, and let v_L be a valuation on L such that v_L extends v. If $y \in L^\times$, then $|y|_L = |\mathrm{N}_{L/K}(y)|^{1/n}$ for $n = [L : K]$, so $v_L(y) = (1/n)\, v(\mathrm{N}_{L/K}(y))$. Thus $v_L(L^\times) \subseteq (1/n)\, v(K^\times)$, so v_L is discrete.
2. Proved in the last lecture.

□

Corollary 2.3.10. *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field and $\overline{K}/K$ an algebraic closure. Then $|\cdot|$ extends to a unique absolute value $|\cdot|_{\overline{K}}$ on $\overline{K}$.*

Proof. If $x \in \overline{K}$, then $x \in L$ for some L/K finite. Define $|x|_{\overline{K}} = |x|_L$. Well-defined, that is independent of L, by the uniqueness in Theorem 2.3.1. The axioms for $|\cdot|_{\overline{K}}$ to be an absolute value can be checked over finite extensions. Uniqueness is clear. □

Remark. $|\cdot|_{\overline{K}}$ on $\overline{K}$ is never discrete. For example, if $K = \mathbb{Q}_p$, then $\sqrt[n]{p} \in \overline{\mathbb{Q}_p}$ for all $n \in \mathbb{N}_{>0}$. Then $\mathrm{v}_p(\sqrt[n]{p}) = (1/n)\, \mathrm{v}_p(p) = 1/n$, so $\overline{\mathbb{Q}_p}$ is not complete with respect to $|\cdot|_{\overline{\mathbb{Q}_p}}$. By example sheet 2, if $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_{\overline{\mathbb{Q}_p}}$, then $\mathbb{C}_p$ is algebraically closed.

3 Local fields

Definition 3.0.1. Let $(K,|\cdot|)$ be a valued field. Then K is a **local field** if it is complete and locally compact.

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

3.1 Non-archimedean local fields

Proposition 3.1.1. *Let $(K,|\cdot|)$ be a non-archimedean complete valued field. The following are equivalent.*

1. *K is locally compact.*
2. *$\mathcal{O}_K$ is compact.*
3. *v is discrete and $\kappa = \mathcal{O}_K/\mathfrak{m}$ is finite.*

Proof.

$1 \implies 2$. Let $U \ni 0$ be a compact neighbourhood of zero. 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, so $\mathcal{O}_K$ is compact, since $x^{-1} : x\mathcal{O}_K \to \mathcal{O}_K$ is homeomorphism.

$2 \implies 1$. If $\mathcal{O}_K$ is compact, then $a + \mathcal{O}_K$ is compact for all $a \in K$, so K is locally compact.

$2 \implies 3$. Let $x \in \mathfrak{m}$, and $A_x \subseteq \mathcal{O}_K$ be a set of coset representatives for $\mathcal{O}_K/x\mathcal{O}_K$. Then

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

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, so $\mathcal{O}_K/\mathfrak{m}$ is finite. Suppose v is not discrete. Let $x = x_1, x_2, \dots$ such that $v(x_1) > v(x_2) > \dots > 0$. Then $x_1\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq \dots \subsetneq \mathcal{O}_K$. But $\mathcal{O}_K/x\mathcal{O}_K$ is finite so can only have finitely many subgroups, a contradiction.

$3 \implies 2$. Since $\mathcal{O}_K$ is a metric space, it suffices to show $\mathcal{O}_K$ 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 in $\mathcal{O}_K$. Since $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong \kappa$, $\mathcal{O}_K/\pi^i\mathcal{O}_K$ is finite for all i, since $\mathcal{O}_K \supseteq \dots \supseteq \pi^i\mathcal{O}_K$. 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 $(x_{1,n})_{n=1}^\infty$ such that $x_{1,n} \equiv a_1 \mod \pi$. We define $y_1 = x_{1,1}$. 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 $(x_{2,n})_{n=1}^\infty$ of $(x_{1,n})_{n=1}^\infty$ such that $x_{2,n} \equiv a_2 \mod \pi^2$. Define $y_2 = x_{2,2}$. Continuing in this fashion, we obtain sequences $(x_{i,n})_{n=1}^\infty$ for $i = 1, 2, \dots$ such that

- $(x_{i+1,n})_{n=1}^\infty$ is a subsequence of $(x_{i,n})_{n=1}^\infty$, and
- for any i, there exists $a_i \in \mathcal{O}_K/\pi^i\mathcal{O}_K$ such that $x_{i,n} \equiv a_i \mod \pi^i$ for all n.

Then necessarily $a_i \equiv a_{i+1} \mod \pi^i$ for all i. Now choose $y_i = x_{ii}$. This defines a subsequence $(y_n)_{n=1}^\infty$. Moreover $y_i \equiv a_i \equiv a_{i+1} \equiv y_{i+1} \mod \pi^i$. Thus y_i is Cauchy, hence converges by completeness.

□

Example.

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

Let $(A_n)_{n=1}^\infty$ be a sequence of sets or groups or rings and $\phi_n : A_{n+1} \to A_n$ homomorphisms.

Definition 3.1.2. Assume A_n is finite. The **profinite topology** on $A = \varprojlim_n A_n$ is the weakest topology on A such that $A \to A_n$ is continuous for all n, where A_n are equipped with the discrete topology.

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

Proposition 3.1.3. *Let K be a 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 uniformiser, the topology on $\mathcal{O}_K$ coincides with the profinite topology.*

Proof. One checks that the sets

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

where A_{π^n} is a set of coset representatives for $\mathcal{O}_K/\pi^n\mathcal{O}_K$, is a basis of open sets in both topologies. For $|\cdot|$, this is clear. For the profinite topology, $\mathcal{O}_K \to \mathcal{O}_K/\pi^n\mathcal{O}_K$ is continuous if and only if $a + \pi^n\mathcal{O}_K$ is open for all $a \in A_{\pi^n}$. Thus B is a basis for the profinite topology. $\square$

Remark. This gives another proof that $\mathcal{O}_K$ is compact.

Lecture 8 Monday 26/10/20

Lemma 3.1.4. *Let K be a non-archimedean local field and L/K a finite extension. Then L is a local field.*

Proof. By Theorem 2.3.1, L is complete and discretely valued. It suffices to show $\kappa_L = \mathcal{O}_L/\mathfrak{m}_L$ is finite. Let $\alpha_1, \dots, \alpha_n$ be a basis for L as a K-vector space. The sup norm $\|\cdot\|_{\sup}$ is equivalent to $|\cdot|_L$ implies there exists $r > 0$ such that $\mathcal{O}_L \subseteq \left\{x \in L \;\middle|\; \|x\|_{\sup} \leq r\right\}$. Take $a \in K$ such that $|a| \geq r$, then $\mathcal{O}_L \subseteq \bigoplus_{i=1}^n a\alpha_i\mathcal{O}_K$, so $\mathcal{O}_L$ is finitely generated as a module over $\mathcal{O}_K$. Thus κ_L is finitely generated over κ. $\square$

Theorem 3.1.5. *Let K be a local field. Then either*

- *$K \cong \mathbb{R}$ or $K \cong \mathbb{C}$,*
- *K is a finite extension of $\mathbb{Q}_p$, or*
- *$K \cong \mathbb{F}_{p^n}((t))$ for p prime and $n \geq 1$.*

Definition 3.1.6. A discretely valued field $(K,|\cdot|)$ has **equal characteristic** if $\operatorname{ch} K = \operatorname{ch}\kappa$. Otherwise it has **mixed characteristic**.

Example. $\operatorname{ch}\mathbb{Q}_p = 0$ and $\operatorname{ch}\mathbb{F}_p = p$, so $\mathbb{Q}_p$ has mixed characteristic.

Note that if K is a non-archimedean local field, $\operatorname{ch}\kappa = p > 0$ and hence K has equal characteristic if $\operatorname{ch} K = p$, or mixed characteristic if $\operatorname{ch} K = 0$.

Theorem 3.1.7. *Let K be a non-archimedean local field of equal characteristic $p > 0$. Then $K \cong \mathbb{F}_{p^n}((t))$ for some $n \geq 1$.*

Proof. K is complete discretely valued and $\operatorname{ch} K > 0$. Moreover $\kappa \cong \mathbb{F}_{p^n}$ is finite, hence perfect. By Theorem 2.2.7, $K \cong \mathbb{F}_{p^n}((t))$. $\square$

3.2 Witt vectors*

For motivation, consider $\mathbb{Z}_p$. Let $x = \sum_{i=0}^\infty [x_i]\, p^i \in \mathbb{Z}_p$ and $y = \sum_{i=0}^\infty [y_i]\, p^i \in \mathbb{Z}_p$ for $x_i, y_i \in \mathbb{F}_p$. Suppose $x + y = s = \sum_{i=0}^\infty [s_i]\, p^i$. Can we write s_i in terms of x_j and y_j? Reducing modulo p we obtain

$$x_0 + y_0 = s_0 \in \mathbb{F}_p,$$

so s_0 is determined by x_0 and y_0. What about s_1? Reducing modulo p^2, $[x_0]+[y_0]+p\,[x_1]+p\,[y_1] \equiv [s_0]+p\,[s_1] \mod p^2$, so

$$p\,[s_1] \equiv [x_0] + [y_0] - [s_0] + p\,[x_1] + p\,[y_1] \mod p^2,$$

and $[x_0] + [y_0] - [s_0] \in p\mathbb{Z}_p$. So we need $[x_0] + [y_0] - [s_0] \mod p^2$. Note $\left[x_0^{1/p}\right] + \left[y_0^{1/p}\right] \equiv \left[s_0^{1/p}\right] \mod p$, so by Lemma 2.2.4

$$[s_0] \equiv \left(\left[x_0^{\frac{1}{p}}\right] + \left[y_0^{\frac{1}{p}}\right]\right)^p \equiv [x_0] + [y_0] + \sum_{d=1}^{p-1} \binom{p}{d} \left[x_0^{\frac{d}{p}}\right] \left[y_0^{\frac{p-d}{p}}\right] \mod p^2.$$

Thus

$$s_1 = x_1 + y_1 - \sum_{d=1}^{p-1} \frac{1}{p}\binom{p}{d} \left[x_0^{\frac{d}{p}}\right] \left[y_0^{\frac{p-d}{p}}\right].$$

Can find similar expressions for $s_2, s_3, \dots$. Witt noticed the general pattern.

Definition 3.2.1. The **n-th Witt polynomial** w_n is defined by

$$\mathrm{w}_n\left(X_0, \dots, X_n\right) = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \in \mathbb{Z}\left[X_0, \dots, X_n\right].$$

Define $\mathrm{S}_n \in \mathbb{Q}\left[X_0, Y_0, \dots, X_n, Y_n\right]$ inductively by the equation

$$\mathrm{w}_n\left(\mathrm{S}_0, \dots, \mathrm{S}_n\right) = \mathrm{w}_n\left(X_0, \dots, X_n\right) + \mathrm{w}_n\left(Y_0, \dots, Y_n\right),$$

where the only term containing S_n is $p^n \mathrm{S}_n$.

Fact (Witt)**.** $\mathrm{S}_n \in \mathbb{Z}\left[X_0, Y_0, \dots, X_n, Y_n\right]$.

Example. $\mathrm{S}_0 = X_0 + Y_0$ and

$$\mathrm{S}_1 = X_1 + Y_1 + \sum_{d=1}^{p-1} \frac{1}{p} \binom{p}{d} X_0^d Y_0^{p-d}.$$

Theorem 3.2.2. *Suppose that*

$$\sum_{i=0}^{\infty} \left[x_i\right] p^i + \sum_{i=0}^{\infty} \left[y_i\right] p^i = \sum_{i=0}^{\infty} \left[s_i\right] p^i \in \mathbb{Z}_p.$$

Then we have

$$s_n = \mathrm{S}_n\left(x_0^{\frac{1}{p^n}}, y_0^{\frac{1}{p^n}}, \dots, x_n, y_n\right).$$

Proof. Example sheet 2. A hint is Lemma 2.2.4. □

Similarly, defines $\mathrm{Z}_n \in \mathbb{Q}\left[X_0, Y_0, \dots, X_n, Y_n\right]$ by

$$\mathrm{w}_n\left(\mathrm{Z}_0, \dots, \mathrm{Z}_n\right) = \mathrm{w}_n\left(X_0, \dots, X_n\right) \mathrm{w}_n\left(Y_0, \dots, Y_n\right),$$

Fact (Witt)**.** $\mathrm{Z}_n \in \mathbb{Z}\left[X_0, Y_0, \dots, X_n, Y_n\right]$.

We have

$$\sum_{i=0}^{\infty} \left[x_i\right] p^i \sum_{i=0}^{\infty} \left[y_i\right] p^i = \sum_{i=0}^{\infty} \left[z_i\right] p^i,$$

where

$$z_n = \mathrm{Z}_n\left(x_0^{\frac{1}{p^n}}, y_0^{\frac{1}{p^n}}, \dots, x_n, y_n\right).$$

The conclusion is that the ring structure on $\mathbb{Z}_p$ can be reconstructed from the arithmetic of $\mathbb{F}_p$.

Definition 3.2.3. A ring A is a **strict p-ring** if it is p-adically complete, p is not a zero divisor in A, and A/pA is a perfect ring of characteristic p.

Theorem 3.2.4 (Existence of Witt vectors)**.** *Let R be a perfect ring of characteristic p.*

1. *There exists a strict p-ring $\mathrm{W}(R)$, called the* ***Witt vectors*** *of R, such that $\mathrm{W}(R)/p\mathrm{W}(R) \cong R$ which is unique up to isomorphism.*

2. *If R' is another perfect ring and $f : R \to R'$ is a ring homomorphism. Then there exists a unique ring homomorphism $F : \mathrm{W}(R) \to \mathrm{W}(R')$ such that the diagram*

$$\begin{tikzcd} \mathrm{W}(R) \arrow[r, "F"] \arrow[d] & \mathrm{W}(R') \arrow[d] \\ R \arrow[r, "f"'] & R' \end{tikzcd}$$

   commutes, so $\mathrm{W}(R)$ is the mixed characteristic analogue of $R[[t]]$.

Proof. See Rabinoff's The theory of Witt vectors.

1. Define
$$\mathrm{W}(R) = \{(a_n)_{n=0}^{\infty} \mid a_n \in R\}.$$
Define addition and multiplication by $(a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty} = (s_n)_{n=0}^{\infty}$ and $(a_n)_{n=0}^{\infty}(b_n)_{n=0}^{\infty} = (z_n)_{n=0}^{\infty}$ where [1]
$$s_n = \mathrm{S}_n(a_0, b_0, \dots, a_n, b_n), \qquad z_n = \mathrm{Z}_n(a_0, b_0, \dots, a_n, b_n).$$
For $a = (a_0, a_1, \dots) \in \mathrm{W}(R)$, we compute
$$pa = (0, a_0^p, a_1^p, \dots),$$
so p is not a zero divisor. Moreover
$$\mathrm{W}(R)/p^i\mathrm{W}(R) = \left\{(a_n)_{n=0}^{i-1} \;\middle|\; a_n \in R\right\}.$$
Compute explicitly
$$\mathrm{W}(R) \cong \varprojlim_i \mathrm{W}(R)/p^i\mathrm{W}(R).$$

2. For $f : R \to R'$, define
$$\begin{array}{cccc} F & : & \mathrm{W}(R) & \longrightarrow & \mathrm{W}(R') \\ & & (a_0, a_1, \dots) & \longmapsto & (f(a_0), f(a_1), \dots) \end{array}.$$

□

Remark. If $R = \mathbb{F}_p$, then $\mathrm{W}(\mathbb{F}_p) \cong \mathbb{Z}_p$. The isomorphism is given by
$$(a_0, a_1, \dots) \mapsto \sum_{i=0}^{\infty} \left[a_i^{\frac{1}{p^i}}\right] p^i.$$

Proposition 3.2.5. *Let $(K,|\cdot|)$ be a complete discretely valued field such that $p \in \mathcal{O}_K$ is a uniformiser and $\kappa = \mathcal{O}_K/\mathfrak{m}$ is perfect. Then $\mathcal{O}_K \cong \mathrm{W}(\kappa)$.*

Proof. By uniqueness of $\mathrm{W}(\kappa)$, it suffices to check that $\mathcal{O}_K$ is a strict p-ring. This is clear from properties of $\mathcal{O}_K$. □

Lecture 9 Wednesday 28/10/20

Remark. Let κ be a perfect field. If $K = \mathrm{Frac}\,\mathrm{W}(\kappa)$, then K is a complete discretely valued field with $\mathcal{O}_K \cong \mathrm{W}(\kappa)$ and $p = \mathrm{ch}\,\kappa \in \mathcal{O}_K$ is a uniformiser.

Proposition 3.2.6. *Let $(K,|\cdot|)$ be a complete discretely valued field with $\kappa = \mathcal{O}_K/\mathfrak{m}$ perfect of characteristic p, then $\mathcal{O}_K$ is finite over $\mathrm{W}(\kappa)$.*

Proof. Consider the subset $R \subseteq \mathcal{O}_K$ defined by
$$R = \left\{\sum_{i=0}^{\infty} [a_i] p^i \;\middle|\; a_i \in \kappa\right\}.$$
Calculating as in the example of $\mathbb{Z}_p$ shows that $R \cong \mathrm{W}(\kappa)$. Let π be a uniformiser in $\mathcal{O}_K$ and let $e \in \mathbb{N}$ such that $ev(\pi) = v(p)$. Let
$$M = \bigoplus_{i=0}^{e-1} \pi^i R \subseteq \mathcal{O}_K,$$
an R-submodule. Since $\sum_{n=0}^{\infty} [x_n] \pi^n \equiv \sum_{n=0}^{e-1} [x_n] \pi^n \mod p$, M generates $\mathcal{O}_K/p\mathcal{O}_K$ as an R-module, so $\mathcal{O}_K = M + p\mathcal{O}_K$. Iterating,
$$\mathcal{O}_K = M + \dots + p^{m-1}M + p^m\mathcal{O}_K = M + p^m\mathcal{O}_K,$$
so $M \to \mathcal{O}_K/p^m\mathcal{O}_K$ is surjective for all m. Then since $M \cong \varprojlim_n M/p^nM$, we have $M \to \mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/p^n\mathcal{O}_K$ is surjective. Thus $M = \mathcal{O}_K$. □

[1] Exercise: check this defines a ring structure

Theorem 3.2.7. *Let K be a non-archimedean local field of mixed characteristic. Then K is a finite extension of $\mathbb{Q}_p$.*

Proof. Let $\kappa = \mathbb{F}_{p^n}$ for some prime p. Then by Proposition 3.2.6, K is a finite extension of $\operatorname{Frac} \mathrm{W}(\mathbb{F}_{p^n})$. It suffices to show that $\mathrm{W}(\mathbb{F}_{p^n})$ is finite over $\mathbb{Z}_p$. Let $e_1, \dots, e_n \in \mathbb{F}_{p^n}$ be a basis of $\mathbb{F}_{p^n}$ as an $\mathbb{F}_p$-vector space, and we write

$$M = \bigoplus_{i=1}^{n} \mathrm{W}(\mathbb{F}_p)[e_i] \subseteq \mathrm{W}(\mathbb{F}_{p^n}),$$

a $\mathrm{W}(\mathbb{F}_p)$-submodule. For $x = \sum_{i=0}^{\infty} [x_i] p^i \in \mathrm{W}(\mathbb{F}_{p^n})$, let $x_0 = \sum_{i=1}^{n} \lambda_i e_i$ for $\lambda_i \in \mathbb{F}_p$. Then $x - \sum_{i=1}^{n} [\lambda_i][e_i] \in p\mathrm{W}(\mathbb{F}_{p^n})$, since $[\lambda_i] \in \mathrm{W}(\mathbb{F}_p)$ by commutativity of

$$\begin{tikzcd} \mathbb{F}_p \arrow[r, "{[\cdot]}"] \arrow[d] & \mathrm{W}(\mathbb{F}_p) \arrow[d] \\ \mathbb{F}_{p^n} \arrow[r, "{[\cdot]}"'] & \mathrm{W}(\mathbb{F}_{p^n}) \end{tikzcd},$$

so $\mathrm{W}(\mathbb{F}_{p^n}) = M + p\mathrm{W}(\mathbb{F}_{p^n})$. Arguing as in Proposition 3.2.6 shows $M = \mathrm{W}(\mathbb{F}_{p^n})$. $\square$

3.3 Classification of local fields

We consider the archimedean case.

Lemma 3.3.1. *An absolute value $|\cdot|$ on a field is non-archimedean if and only if $|n|$ is bounded for all $n \in \mathbb{Z}$.*

Proof.

$\Longrightarrow$ Since $|-1| = 1, |-n| = |n|$, thus it suffices to show that $|n|$ is bounded for $n \geq 1$. Then $|n| = |1 + \dots + 1| \leq 1$.

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

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

Taking m-th roots gives

$$|x + y| \leq |y| ((m+1) B)^{\frac{1}{m}} \to |y|, \qquad m \to \infty.$$

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

$\square$

Corollary 3.3.2. *If $(K, |\cdot|)$ is a valued field with $\operatorname{ch} K > 0$, then K is non-archimedean.*

Theorem 3.3.3 (Ostrowski's theorem)**.** *Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the usual absolute value $|\cdot|_\infty$ or the p-adic absolute value $|\cdot|_p$ for some prime p.*

Proof.

Case 1. $|\cdot|$ is archimedean. We fix $b > 1$ an integer such that $|b| > 1$, which exists by Lemma 3.3.1. Let $a > 1$ be an integer and write b^n in base a, so $b^n = c_m a^m + \dots + c_0$ for $0 \leq c_i < a$. Let $B = \max_{0 \leq c < a} |c|$, then we have $|b^n| \leq (m+1) B \max(|a|^m, 1)$, so

$$|b| \leq ((n \log_a b + 1) B)^{\frac{1}{n}} \max\left(|a|^{\log_a b}, 1\right) \to \max\left(|a|^{\log_a b}, 1\right), \qquad n \to \infty,$$

so $|b| \leq \max\left(|a|^{\log_a b}, 1\right)$. Then $|b| > 1$ and

$$|b| \leq |a|^{\log_a b}. \tag{1}$$

Switching the roles of a and b, we obtain

$$|a| \leq |b|^{\log_b a}. \tag{2}$$

By (1) and (2),

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

using $\log_a b = \log b / \log a$, so $|a| = a^\lambda$ for all $a \in \mathbb{Z}$ such that $a > 1$, so $|x| = |x|_\infty^\lambda$ for all $x \in \mathbb{Q}$. Hence $|\cdot|$ is equivalent to $|\cdot|_\infty$.

Case 2. $|\cdot|$ is non-archimedean. As in Lemma 3.3.1, we have $|n| \leq 1$ for all $n \in \mathbb{Z}$. Since $|\cdot|$ is non-trivial, there exists $n \in \mathbb{Z}_{>1}$ such that $|n| < 1$. Write $n = p_1^{e_1} \dots p_r^{e_r}$, a decomposition into prime factors. Then $|p| < 1$ for some $p \in \{p_1, \dots, p_r\}$. Suppose $|q| < 1$ for some prime q such that $q \neq p$. Write $1 = rp + sq$ for $r, s \in \mathbb{Z}$. Then $1 = |rp + sq| \leq \max(|rp|, |sq|) < 1$, a contradiction. Thus $|p| = \alpha < 1$ and $|q| = 1$ for all primes $q \neq p$, so $|\cdot|$ is equivalent to $|\cdot|_p$.

□

Theorem 3.3.4. *Let $(K, |\cdot|)$ be an archimedean local field. Then $K = \mathbb{R}$ or $K = \mathbb{C}$ and $|\cdot|$ is equivalent to the usual absolute value $|\cdot|_\infty$.*

Proof. If $\operatorname{ch} K > 0$, then K is non-archimedean by Corollary 3.3.2. Therefore $\operatorname{ch} K = 0$, and hence $\mathbb{Q} \subseteq K$. Since $|\cdot|$ is archimedean, $|\cdot||_{\mathbb{Q}}$ is equivalent to $|\cdot|_\infty$ by Ostrowski. Therefore, since K is complete, we have $\mathbb{R} \subseteq K$.

- We first consider the case $\mathbb{C} \subseteq K$. Then by uniqueness of extensions of absolute values, $|\cdot||_{\mathbb{C}}$ is equivalent to $|\cdot|_\infty$. Suppose $\alpha \in K \setminus \mathbb{C}$. Then $f(X) = |X - \alpha|$ is a continuous function on $\mathbb{C}$, hence attains a lower bound at $b \in \mathbb{C}$ say, since $\mathbb{C} \subseteq K$ is closed. Set $\beta = \alpha - b$ and we let $c \in \mathbb{C}$ such that $0 < |c| < |\beta|$. We have $|\beta - a| \geq |\beta|$ for all $a \in \mathbb{C}$. Hence

$$\frac{|\beta - c|}{|\beta|} \leq \frac{|\beta - c|}{|\beta|} \prod_{\zeta^n = 1,\ \zeta \neq 1} \frac{|\beta - \zeta c|}{|\beta|} = \frac{|\beta^n - c^n|}{|\beta|^n} = \left|1 - \left(\frac{c}{\beta}\right)^n\right| \to 1,$$

  as $n \to \infty$, since $|c/\beta| < 1$ implies that $(c/\beta)^n \to 0$. Then $|\beta - c| \leq |\beta|$, so $|\beta - c| = |\beta|$. Replacing β by $\beta - c$ and iterating, we obtain $|\beta - mc| = |\beta|$ for all $m \in \mathbb{N}$, so

$$|m||c| = |mc| \leq |\beta - mc| + |\beta| = 2|\beta|.$$

  This contradicts Lemma 3.3.1, hence $K = \mathbb{C}$.

- Now suppose K does not contain $\mathbb{C}$. Define $L = K(i)$ where $i^2 = -1$. Can extend $|\cdot|$ to an absolute value $|\cdot|_L$ on L given by

$$|a + ib|_L = \sqrt{|a|^2 + |b|^2}, \qquad a, b \in K.$$

  Applying the above argument gives $K(i) = L = \mathbb{C}$, hence $K = \mathbb{R}$.

□

Proof of Theorem 3.1.5.

- $|\cdot|$ archimedean is Theorem 3.3.4.
- $|\cdot|$ non-archimedean and $\operatorname{ch} K = 0$ is Theorem 3.2.7.
- $|\cdot|$ non-archimedean and $\operatorname{ch} K > 0$ is Theorem 3.1.7.

□

3.4 Global fields

Lecture 10
Friday
30/10/20

Definition 3.4.1. A **global field** is a field which is either

- an algebraic number field, or
- a **global function field**, the rational function field of an algebraic curve over a finite field, or equivalently a finite extension of $\mathbb{F}_p(t)$.

We mainly focus on the number field. We show that local fields are completions of global fields.

Lemma 3.4.2. *Let $(K, |\cdot|)$ be a complete discretely valued field and L/K a Galois extension and $|\cdot|_L$ the unique extension of $|\cdot|$ to L. 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 also another absolute value on L extending $|\cdot|$ on K, Lemma 3.4.2 follows from uniqueness of $|\cdot|_L$. ☐

Lemma 3.4.3 (Krasner's lemma)**.** *Let $(K, |\cdot|)$ a complete discretely valued field. Let $f(X) \in K[X]$ be a separable irreducible polynomial with roots $\alpha_1, \dots, \alpha_n \in K^{\mathrm{sep}}$, a separable closure of K. Suppose $\beta \in \overline{K}$ with $|\beta - \alpha_1| < |\beta - \alpha_i|$ for $i = 2, \dots, n$. Then $\alpha_1 \in K(\beta)$.*

Proof. Let $L = K(\beta)$ and $L' = L(\alpha_1, \dots, \alpha_n)$. Then L'/L is a Galois extension. Let $\sigma \in \mathrm{Gal}(L'/L)$. We have $|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1|$, by Lemma 3.4.2. Thus $\sigma(\alpha_1) = \alpha_1$, so $\alpha_1 \in K(\beta)$. ☐

Proposition 3.4.4 (Nearby polynomials define the same extension)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field and $f(X) = \sum_{i=0}^n a_i X^i \in \mathcal{O}_K[X]$ be a separable irreducible monic polynomial. Let $\alpha \in \overline{K}$ be a root of f. Then there exists $\epsilon > 0$ such that for any $g(X) = \sum_{i=0}^n b_i X^i \in \mathcal{O}_K[X]$ monic with $|a_i - b_i| < \epsilon$, there exists a root β of $g(X)$ such that $K(\alpha) = K(\beta)$.*

Proof. Let $\alpha = \alpha_1, \dots, \alpha_n \in \overline{K}$ be the roots of f which are necessarily distinct. Then $f'(\alpha) \neq 0$. We choose ϵ sufficiently small such that $|g(\alpha)| < |f'(\alpha)|^2$ and $|f'(\alpha) - g'(\alpha)| < |f'(\alpha)|$. Then we have $|g(\alpha)| < |f'(\alpha)|^2 = |g'(\alpha)|^2$. By Hensel's lemma applied to the field $K(\alpha)$, there exists $\beta \in K(\alpha)$ such that $g(\beta) = 0$ and $|\beta - \alpha| < |g'(\alpha)|$. Then

$$|g'(\alpha)| = |f'(\alpha)| = \prod_{i=2}^n |\alpha - \alpha_i| \le |\alpha - \alpha_i|, \qquad i = 2, \dots, n,$$

using $|\alpha - \alpha_i| \le 1$. Since $|\beta - \alpha| < |g'(\alpha)| = |f'(\alpha)| \le |\alpha - \alpha_i| = |\beta - \alpha_i|$ for $i = 2, \dots, n$, by Krasner's lemma, $\alpha \in K(\beta)$, so $K(\alpha) = K(\beta)$. ☐

Theorem 3.4.5. *Let K be a local field, then K is the completion of a global field.*

Proof.

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

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

Case 3. $|\cdot|$ is non-archimedean of mixed characteristic. Then $K \cong \mathbb{Q}_p(\alpha)$ for 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 3.4.4. Then $K = \mathbb{Q}_p(\beta)$ for β a root of $g(X)$. Since $\beta \in \overline{\mathbb{Q}}$, we have $\mathbb{Q}(\beta) \subseteq \mathbb{Q}_p(\beta) = K$, so K is the completion of $\mathbb{Q}(\beta)$.

☐

4 Dedekind domains

The global analogue of a DVR is a Dedekind domain.

4.1 Dedekind domains and DVRs

Definition 4.1.1. A **Dedekind domain** is a ring R such that

- R is a Noetherian integral domain,
- R is integrally closed in $\operatorname{Frac} R$, and
- every non-zero prime ideal is maximal.

Example.

- The ring of integers in a number field is a Dedekind domain.
- Any PID, hence DVR, is a Dedekind domain.

Theorem 4.1.2. *A ring R is a DVR if and only if R is a Dedekind domain with exactly one non-zero prime ideal.*

Lemma 4.1.3. *Let R be a Noetherian ring and $I \subseteq R$ a non-zero ideal. Then there exist non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r \subseteq R$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq I$.*

Proof. Suppose not. Since R is Noetherian, we may choose I maximal without this property. Then I is not prime, so there exists $x, y \in R \setminus I$ such that $xy \in I$. Let $I_1 = I + \langle x \rangle$ and $I_2 = I + \langle y \rangle$. Then by maximality of I, there exists $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ prime ideals such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq I_1$ and $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq I_2$, so $\mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq I_1 I_2 \subseteq I$, a contradiction. ☐

Lemma 4.1.4. *Let R be an integral domain which is integrally closed in $K = \operatorname{Frac} R$. Let $I \subseteq R$ be a non-zero finitely generated ideal and $x \in K$. Then if $xI \subseteq I$, we have $x \in R$.*

Proof. Let $I = \langle c_1, \dots, c_n \rangle$. We write $xc_i = \sum_{i=1}^n a_{ij} c_i$ for some $a_{ij} \in R$. Let A be the matrix $A = (a_{ij})_{1 \le i,j \le n}$ and set $B = x\mathrm{I}_n - A \in \operatorname{Mat}_{n \times n} K$. Then $B \begin{pmatrix} c_1 & \dots & c_n \end{pmatrix}^\intercal = 0$ in K^n. Multiplying by the adjugate matrix for B, $(\det B)\, \mathrm{I}_n \begin{pmatrix} c_1 & \dots & c_n \end{pmatrix}^\intercal = 0$, so $\det B = 0$. But $\det B$ is a monic polynomial in x with coefficients in R. Thus x is integral over R, so $x \in R$. ☐

Proof of Theorem 4.1.2.

$\implies$ Clear.

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

Step 1. $\mathfrak{m}$ is principal. Let $0 \ne x \in \mathfrak{m}$. By Lemma 4.1.3, $\langle x \rangle \supseteq \mathfrak{m}^n$ for some $n \ge 1$. Let n be minimal such that $\langle x \rangle \supseteq \mathfrak{m}^n$, then we may choose $y \in \mathfrak{m}^{n-1} \setminus \langle x \rangle$. Set $\pi = x/y$. Then we have $y\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq \langle x \rangle$, so $\pi^{-1}\mathfrak{m} \subseteq R$. If $\pi^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, then $\pi^{-1} \in R$ by Lemma 4.1.4 and $y \in \langle x \rangle$, a contradiction. Hence $\pi^{-1}\mathfrak{m} = R$, so $\mathfrak{m} = \pi R$ is principal.

Step 2. R is a PID. Let $I \subseteq R$ be a non-zero ideal. Consider the sequence of fractional ideals $I \subseteq \pi^{-1} I \subseteq \dots$ in K. Then $\pi^{-k} I \ne \pi^{-(k+1)} I$ for all k by Lemma 4.1.4. Therefore since R is Noetherian, we may choose n maximal such that $\pi^{-n} I \subseteq R$. If $\pi^{-n} I \subseteq \mathfrak{m} = \langle \pi \rangle$, then $\pi^{-(n+1)} I \subseteq R$, a contradiction. Thus $\pi^{-n} I = R$, so $I = \langle \pi^n \rangle$.

☐

Lecture 11 Monday 02/11/20

Let R be an integral domain and $S \subseteq R$ a multiplicatively closed subset, so if $x, y \in S$ then $xy \in S$. 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 $\mathfrak{p}$ is a prime ideal in R, we write $R_{(\mathfrak{p})}$ for the localisation with respect to $S = R \setminus \mathfrak{p}$.

Example.

- If $\mathfrak{p} = 0$, then $R_{(\mathfrak{p})} = \operatorname{Frac} R$.
- If $R = \mathbb{Z}$, then $\mathbb{Z}_{(\langle p \rangle)} = \{a/p^n \mid a \in \mathbb{Z},\ n \in \mathbb{Z}_{\geq 0}\}$.

Fact.

- If R is Noetherian, then $S^{-1}R$ is Noetherian.
- There exists a bijection

$$\left\{ \text{ prime ideals } \mathfrak{p}S^{-1}R \subseteq S^{-1}R \right\} \qquad \leftrightsquigarrow \qquad \left\{ \text{ prime ideals } \mathfrak{p} \subseteq R \text{ such that } \mathfrak{p} \cap S = \emptyset \right\}.$$

Corollary 4.1.5. *Let R be a Dedekind domain and $\mathfrak{p} \subseteq R$ is a non-zero prime ideal. Then $R_{(\mathfrak{p})}$ is a DVR.*

Proof. By properties of localisation, $R_{(\mathfrak{p})}$ is a Noetherian integral domain with a unique non-zero prime ideal $\mathfrak{p}R_{(\mathfrak{p})}$. It suffices to show that $R_{(\mathfrak{p})}$ is integrally closed in $\operatorname{Frac} R_{(\mathfrak{p})} = \operatorname{Frac} R$, since then $R_{(\mathfrak{p})}$ is Dedekind, so by Theorem 4.1.2, $R_{(\mathfrak{p})}$ is a DVR. Let $x \in \operatorname{Frac} R$ be integral over $R_{(\mathfrak{p})}$. Multiplying by denominators of a monic polynomial satisfied by x, we obtain $sx^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ for $a_i \in R$ and $s \in S$. By multiplying by s^{n-1}, xs is integral over R. Thus $xs \in R$, so $x \in R_{(\mathfrak{p})}$. □

Definition 4.1.6. If R is a Dedekind domain and $\mathfrak{p} \subseteq R$ a non-zero prime ideal, we write $\mathrm{v}_{\mathfrak{p}}$ for the normalised valuation on $\operatorname{Frac} R = \operatorname{Frac} R_{(\mathfrak{p})}$ corresponding to the DVR $R_{(\mathfrak{p})}$.

Example. If $R = \mathbb{Z}$ and $\mathfrak{p} = \langle p \rangle$, then $\mathrm{v}_{\mathfrak{p}}$ is the p-adic valuation.

Theorem 4.1.7. *Let R be a Dedekind domain. Then every non-zero ideal $I \subseteq R$ can be written uniquely as a product of prime ideals, $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ for $\mathfrak{p}_i$ distinct.*

Remark. This is clear for PIDs, since PID implies UFD.

Proof. We quote the following properties of localisation.

1. If $I \subsetneq J$ then $IR_{(\mathfrak{p})} \subsetneq JR_{(\mathfrak{p})}$.
2. $I = J$ if and only if $IR_{(\mathfrak{p})} = JR_{(\mathfrak{p})}$, for all $\mathfrak{p}$ prime ideals.

Let $I \subseteq R$ be a non-zero ideal. Then by Lemma 4.1.3, there are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_r^{\beta_r} \subseteq I$, where $\beta_i > 0$. Then

$$IR_{(\mathfrak{p})} = \begin{cases} R_{(\mathfrak{p})} & \mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \\ \mathfrak{p}^{\alpha_i} R_{(\mathfrak{p})} & \mathfrak{p} = \mathfrak{p}_i \end{cases}.$$

Here, $0 < \alpha_i \leq \beta_i$, and the second case follows from Corollary 4.1.5. Thus $I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$ by property 2. 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 $\mathfrak{p}_i^{\alpha_i} R_{(\mathfrak{p}_i)} = \mathfrak{p}_i^{\gamma_i} R_{(\mathfrak{p}_i)}$, so $\alpha_i = \gamma_i$ by unique factorisation in DVRs. □

4.2 Extensions of Dedekind domains

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

$$\begin{array}{ccc} L & \longrightarrow & L \\ y & \longmapsto & xy \end{array}.$$

If L/K is separable such that $[L : K] = n$ and $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ denote the embeddings of L into a separable closure K^{sep}, then

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

Lemma 4.2.1. *Let L/K be a finite separable extension of fields. Then the symmetric bilinear pairing*

$$\begin{array}{rcccl} (,) & : & L \times L & \longrightarrow & K \\ & & (x,y) & \longmapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

is non-degenerate.

Proof. By the primitive element theorem, $L = K(\alpha)$ for some $\alpha \in L$. We consider the matrix A for $(,)$ in the K-basis for L given by $1, \dots, \alpha^{n-1}$. Then $A_{ij} = \mathrm{Tr}_{L/K}\left(\alpha^{i+j}\right) = \left[BB^\intercal\right]_{ij}$ where B is the $n \times n$ matrix with

$$B = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ \sigma_1\left(\alpha^{n-1}\right) & \dots & \sigma_n\left(\alpha^{n-1}\right) \end{pmatrix},$$

so the Vandermonde determinant is

$$\det A = (\det B)^2 = \left[\prod_{1 \le i < j \le n} \left(\sigma_i(\alpha) - \sigma_j(\alpha)\right)\right]^2 \ne 0,$$

since $\sigma_i(\alpha) \ne \sigma_j(\alpha)$ for $i \ne j$, by separability. ☐

Remark. In fact a finite extension of fields L/K is separable if and only if the trace form is non-degenerate.

Theorem 4.2.2. *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. Since $\mathcal{O}_L \subseteq L$, it is an integral domain. We need to show the following.

- $\mathcal{O}_L$ is Noetherian. 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 $(,)$. Let $x \in \mathcal{O}_L$ and write $x = \sum_{i=1}^n \lambda_i f_i$ for $\lambda_i \in K$. Then $\lambda_i = \mathrm{Tr}_{L/K}(xe_i) \in \mathcal{O}_K$, since for any $z \in \mathcal{O}_L$, $\mathrm{Tr}_{L/K}(z)$ is a sum of elements which are integral over $\mathcal{O}_K$, so $\mathrm{Tr}_{L/K}(z)$ is integral over $\mathcal{O}_K$, so $\mathrm{Tr}_{L/K}(z) \in \mathcal{O}_K$. Thus $\mathcal{O}_L \subseteq \mathcal{O}_K f_1 + \dots + \mathcal{O}_K f_n$. Since $\mathcal{O}_K$ is Noetherian and $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$-module, hence $\mathcal{O}_L$ is Noetherian.
- $\mathcal{O}_L$ is integrally closed in L. Example sheet 2.
- Every non-zero prime ideal $\mathfrak{P}$ in $\mathcal{O}_L$ is maximal. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}_L$, and define $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ a prime ideal of $\mathcal{O}_K$. Let $x \in \mathfrak{P}$, then x satisfies an equation $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ for $a_i \in \mathcal{O}_K$ with $a_0 \ne 0$. Then $a_0 \in \mathfrak{P} \cap \mathcal{O}_K$ is a non-zero element of $\mathfrak{p}$, so $\mathfrak{p}$ is non-zero, so $\mathfrak{p}$ is maximal. We have $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$, and $\mathcal{O}_L/\mathfrak{P}$ is a finite-dimensional vector space over $\mathcal{O}_K/\mathfrak{p}$. Since $\mathcal{O}_L/\mathfrak{P}$ is an integral domain, it is a field, using the rank-nullity theorem applied to the map $y \mapsto zy$.

☐

Remark. Theorem 4.2.2 in fact holds without the assumption that L/K is separable.

Corollary 4.2.3. *The ring of integers inside a number field is a Dedekind domain.*

By convention, if $\mathcal{O}_K$ is the ring of integers of a number field and $\mathfrak{p} \subseteq \mathcal{O}_K$ is a non-zero prime ideal, we normalise $|\cdot|_{\mathfrak{p}}$, the absolute value associated to $\mathrm{v}_{\mathfrak{p}}$, by

$$|x|_{\mathfrak{p}} = \mathrm{N}(\mathfrak{p})^{-\mathrm{v}_{\mathfrak{p}}(x)}, \qquad \mathrm{N}(\mathfrak{p}) = \#\left(\mathcal{O}_K/\mathfrak{p}\right).$$

Lecture 12 Wednesday 04/11/20

Lemma 4.2.4. *Let $\mathcal{O}_K$ be a Dedekind domain. Let $0 \ne x \in \mathcal{O}_K$. Then*

$$\langle x \rangle = \prod_{\mathfrak{p} \ne 0 \text{ prime ideals}} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(x)}.$$

Note the product is finite.

Proof. $x\mathcal{O}_{K,(\mathfrak{p})} = \left(\mathfrak{p}\mathcal{O}_{K,(\mathfrak{p})}\right)^{\mathrm{v}_{\mathfrak{p}}(x)}$ by definition of $\mathrm{v}_{\mathfrak{p}}(x)$. Lemma 4.2.4 follows from properties of localisation, where $I = J$ if and only if $I\mathcal{O}_{K,(\mathfrak{p})} = J\mathcal{O}_{K,(\mathfrak{p})}$ for all prime ideals $\mathfrak{p}$. ☐

Notation. Let $\mathcal{O}_K$ be a Dedekind domain, let L/K be a finite separable extension, and let $\mathfrak{P} \subseteq \mathcal{O}_L$ and $\mathfrak{p} \subseteq \mathcal{O}_K$ be non-zero prime ideals. We write $\mathfrak{P} \mid \mathfrak{p}$ if

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}, \qquad \mathfrak{P} \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}, \qquad e_i > 0.$$

Theorem 4.2.5. *Let $\mathcal{O}_K$ be a Dedekind domain and L a finite separable extension of $K = \operatorname{Frac} \mathcal{O}_K$. For $\mathfrak{p}$ a non-zero prime ideal of $\mathcal{O}_K$, we write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ for $e_i > 0$. Then the absolute values on L extending $|\cdot|_{\mathfrak{p}}$, up to equivalence, are precisely $|\cdot|_{\mathfrak{P}_1}, \dots, |\cdot|_{\mathfrak{P}_r}$.*

Proof. By Lemma 4.2.4, for any $x \in \mathcal{O}_K$ and $i = 1, \dots, r$, we have $\mathrm{v}_{\mathfrak{P}_i}(x) = e_i \mathrm{v}_{\mathfrak{p}}(x)$. Hence up to equivalence, $|\cdot|_{\mathfrak{P}_i}$ extends $|\cdot|_{\mathfrak{p}}$. Now suppose $|\cdot|$ is an absolute value on L extending $|\cdot|_{\mathfrak{p}}$. Then $|\cdot|$ is bounded on $\mathbb{Z}$, hence $|\cdot|$ is non-archimedean. Let

$$R = \{x \in L \mid |x| \le 1\} \subseteq L$$

be the valuation ring for L with respect to $|\cdot|$. Then $\mathcal{O}_K \subseteq R$, and since R is integrally closed in L, by lecture 6, we have $\mathcal{O}_L \subseteq R$. Set

$$\mathfrak{P} = \{x \in \mathcal{O}_L \mid |x| < 1\}. \tag{3}$$

It is easy to check $\mathfrak{P}$ is a non-zero prime ideal. For example,

- if $x, y \in \mathfrak{P}$ then $x + y \in \mathfrak{P}$ by (3),
- if $r \in \mathcal{O}_L$ and $x \in \mathfrak{P}$ then $rx \in \mathfrak{P}$ by $\mathcal{O}_L \subseteq R$ and (3),
- if $x, y \in \mathcal{O}_L$ and $xy \in \mathfrak{P}$ then $x \in \mathfrak{P}$ or $y \in \mathfrak{P}$ by (3), and
- $\mathfrak{p} \subseteq \mathfrak{P}$, hence $\mathfrak{P}$ is non-zero.

Then $\mathcal{O}_{L,(\mathfrak{P})} \subseteq R$, since if $s \in \mathcal{O}_L \setminus \mathfrak{P}$ then $|s| = 1$. But $\mathcal{O}_{L,(\mathfrak{P})}$ is a DVR, hence a maximal subring of L, so $\mathcal{O}_{L,(\mathfrak{P})} = R$. Hence $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{P}}$. Since $|\cdot|$ extends $|\cdot|_{\mathfrak{p}}$, $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Thus $\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{P}$, so $\mathfrak{P} = \mathfrak{P}_i$ 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, by example sheet 2, denoted by $|\cdot|_\sigma$.

Corollary 4.2.6. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then any absolute value on K is either*

- *$|\cdot|_{\mathfrak{p}}$ for some non-zero prime ideal of $\mathcal{O}_K$, or*
- *$|\cdot|_\sigma$ for some $\sigma : K \to \mathbb{R}, \mathbb{C}$.*

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 4.2.5 implies $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}}$ for $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ dividing $\langle p \rangle$.

Case 2. $|\cdot|$ is archimedean. Example sheet.

☐

4.3 Completions of number fields

Now let L/K be an extension of number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ and $\mathfrak{P} \subseteq \mathcal{O}_L$ be non-zero prime ideals such that $\mathfrak{P}$ divides $\mathfrak{p}$. We write $K_{\mathfrak{p}}$ and $L_{\mathfrak{P}}$ for the completion of K and L with respect to $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathfrak{P}}$ respectively.

Lemma 4.3.1.

- *The natural map $L \otimes_K K_{\mathfrak{p}} \to L_{\mathfrak{P}}$ is surjective.*
- *$[L_{\mathfrak{P}} : K_{\mathfrak{p}}] \le [L : K]$.*

Proof. Let $M = LK_{\mathfrak{p}} \subseteq L_{\mathfrak{P}}$. Then M is a finite extension of $K_{\mathfrak{p}}$ and $[M : K_{\mathfrak{p}}] \le [L : K]$. Moreover M is complete and since $L \subseteq M \subseteq L_{\mathfrak{P}}$, we have $L_{\mathfrak{P}} = M$. ☐

Lemma 4.3.2 (Chinese remainder theorem)**.** *Let R be a ring. Let $I_1, \dots, I_n \subseteq R$ be ideals such that $I_i + I_j = R$ for all $i \ne j$. Then*

- $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i = I$, *and*
- $R / I \cong \prod_{i=1}^n R / I_i$.

Proof. Example sheet 2. □

Theorem 4.3.3.

$$L \otimes_K K_{\mathfrak{p}} \cong \prod_{\mathfrak{P} \mid \mathfrak{p}} L_{\mathfrak{P}}.$$

Proof. Write $L = K(\alpha)$, by separability, and let $f(X) \in K[X]$ be the minimal polynomial of α. Let $f(X) = f_1(X) \dots f_r(X)$ in $K_{\mathfrak{p}}[X]$ where $f_i(X) \in K_{\mathfrak{p}}[X]$ are distinct irreducible. Then $L \cong K[X] / \langle f(X) \rangle$, and hence by CRT,

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

Set $L_i = K_{\mathfrak{p}}[X] / \langle f_i(X) \rangle$, a finite extension of $K_{\mathfrak{p}}$. Then L_i contains both L and $K_{\mathfrak{p}}$, using the map of fields $K[X] / \langle f(X) \rangle \hookrightarrow K_{\mathfrak{p}}[X] / \langle f_i(X) \rangle$ is injective. Moreover L is dense inside L_i. Indeed since K is dense in $K_{\mathfrak{p}}$, can approximate coefficients of an element of $K_{\mathfrak{p}}[X] / \langle f_i(X) \rangle$ with an element of $K[X] / \langle f(X) \rangle$. Then Theorem 4.3.3 follows from the following three claims.

- $L_i \cong L_{\mathfrak{P}}$ for a prime $\mathfrak{P}$ of $\mathcal{O}_L$ dividing $\mathfrak{p}$. Since $[L_i : K_{\mathfrak{p}}] < \infty$, there is a unique absolute value $|\cdot|$ on L_i extending $|\cdot|_{\mathfrak{p}}$. By Theorem 4.2.5, $|\cdot||_L$ is equivalent to $|\cdot|_{\mathfrak{P}}$ for some $\mathfrak{P} \mid \mathfrak{p}$. Since L is dense in L_i and L_i is complete, we have $L_i \cong L_{\mathfrak{P}}$.
- Each $\mathfrak{P}$ appears at most once. Suppose $\phi : L_i \cong L_j$ is an isomorphism preserving L and $K_{\mathfrak{p}}$, then $\phi : K_{\mathfrak{p}}[X] / \langle f_i(X) \rangle \xrightarrow{\sim} K_{\mathfrak{p}}[X] / \langle f_j(X) \rangle$ takes X to X. Hence $f_i(X) = f_j(X)$, so $i = j$.
- Each $\mathfrak{P}$ appears at least once. By Lemma 4.3.1, the natural map $\pi_{\mathfrak{P}} : L \otimes_K K_{\mathfrak{p}} \to L_{\mathfrak{P}}$ is surjective for any $\mathfrak{P} \mid \mathfrak{p}$. Since $L_{\mathfrak{P}}$ is a field, $\pi_{\mathfrak{P}}$ factors through L_i for some i, and hence $L_i \cong L_{\mathfrak{P}}$ by surjectivity of $\pi_{\mathfrak{P}}$.

□

Example. Let $K = \mathbb{Q}$, let $L = \mathbb{Q}(i)$, and let $f(X) = X^2 + 1$. By Hensel, $\sqrt{-1} \in \mathbb{Q}_5$. Thus $\langle 5 \rangle$ splits in $\mathbb{Q}(i)$, that is $5\mathcal{O}_L = \mathfrak{p}_1 \mathfrak{p}_2$.

Corollary 4.3.4. *For $x \in L$,*

$$\mathrm{N}_{L/K}(x) = \prod_{\mathfrak{P} \mid \mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}} / K_{\mathfrak{p}}}(x).$$

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$. Let $\mathcal{B}_1, \dots, \mathcal{B}_r$ be bases for $L_{\mathfrak{P}_1}, \dots, L_{\mathfrak{P}_r}$ as $K_{\mathfrak{p}}$-vector spaces. Then $\mathcal{B} = \bigcup_{i=1}^r \mathcal{B}_i$ is a basis for $L \otimes_K K_{\mathfrak{p}}$ over $K_{\mathfrak{p}}$. Let $[\cdot x]_{\mathcal{B}}$ and $[\cdot x]_{\mathcal{B}_i}$ denote the matrices for $\cdot x : L \otimes_K K_{\mathfrak{p}} \to L \otimes_K K_{\mathfrak{p}}$ and $\cdot x : L_{\mathfrak{P}_i} \to L_{\mathfrak{P}_i}$ with respect to the bases $\mathcal{B}$ and $\mathcal{B}_i$ respectively. Then

$$[\cdot x]_{\mathcal{B}} = \begin{pmatrix} [\cdot x]_{\mathcal{B}_1} & & 0 \\ & \ddots & \\ 0 & & [\cdot x]_{\mathcal{B}_r} \end{pmatrix},$$

so

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

□

4.4 Decomposition groups

Lecture 13 Friday 06/11/20

Let $\mathcal{O}_K$ be a Dedekind domain, L a finite separable extension of $K = \operatorname{Frac} \mathcal{O}_K$, and $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L. By lecture 11, if $0 \ne \mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal, then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ where $\mathfrak{P}_i$ are distinct prime ideals of $\mathcal{O}_L$. Note that for any i, $\mathfrak{p} \subseteq \mathcal{O}_K \cap \mathfrak{P}_i \subsetneq \mathcal{O}_K$, hence $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}_i$.

Definition 4.4.1. e_i is the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$. We say $\mathfrak{p}$ **ramifies** in L if some $e_i > 1$.

Example. Let $\mathcal{O}_K = \mathbb{C}[t]$, let $\mathcal{O}_L = \mathbb{C}[T]$, and let

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_L \\ t & \longmapsto & T^n \end{array}.$$

We have $t\mathcal{O}_L = T^n\mathcal{O}_L$, so the ramification index of $\langle T \rangle$ over $\langle t \rangle$ is n. Corresponds geometrically to the degree n covering of Riemann surfaces

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & x^n \end{array},$$

having a ramification at zero with ramification index n.

Definition 4.4.2. $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is the **residue class degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Theorem 4.4.3.

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

Proof. Let $S = \mathcal{O}_K \setminus \mathfrak{p}$. We have the following whose proofs are left as an exercise.

1. $S^{-1}\mathcal{O}_L$ is the integral closure of $S^{-1}\mathcal{O}_K$ in L.
2. $S^{-1}\mathfrak{p}S^{-1}\mathcal{O}_L \cong S^{-1}\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$.
3. $S^{-1}\mathcal{O}_L/S^{-1}\mathfrak{P}_i \cong \mathcal{O}_L/\mathfrak{P}_i$ and $S^{-1}\mathcal{O}_K/S^{-1}\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$.

In particular, 2 and 3 imply e_i and f_i do not 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

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{P}_i^{e_i}. \tag{4}$$

Note that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a $\kappa = \mathcal{O}_K/\mathfrak{p}$-module, that is a κ-vector space. We count dimensions of both sides in (4). For each i, we have a decreasing sequence of κ-subspaces

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

Thus $\dim_\kappa \mathcal{O}_L/\mathfrak{P}_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_\kappa \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$. Note that $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is an $\mathcal{O}_L/\mathfrak{P}_i$-module and $x \in \mathfrak{P}_i^j \setminus \mathfrak{P}_i^{j+1}$ is a generator. For example, can prove this after localising at $\mathfrak{P}_i$. Then $\dim_\kappa \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1} = f_i$ and we have $\dim_\kappa \mathcal{O}_L/\mathfrak{P}_i^{e_i} = e_i f_i$. Recall that $\mathcal{O}_K$ is a DVR. By the structure theorem for modules over PIDs, $\mathcal{O}_L$ is a free module over $\mathcal{O}_K$ of rank $n = [L : K]$. Thus $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_K/\mathfrak{p})^n$ as $\mathcal{O}_K$-modules and hence $\dim_\kappa \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$. $\square$

Theorem 4.4.3 is the algebraic analogue of the fact that for a degree n covering $X \to Y$ of compact Riemann surfaces, and $y \in Y$ we have

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

where e_x is the ramification index of x. Now assume L/K is Galois. Then for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathfrak{P}_i) \cap \mathcal{O}_K = \mathfrak{p}$ and hence $\sigma(\mathfrak{P}_i) \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$, so $\mathrm{Gal}(L/K)$ acts on $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$.

Proposition 4.4.4. *The action of* $\mathrm{Gal}(L/K)$ *on* $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$ *is transitive.*

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

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

Since $\mathfrak{P}_j$ is prime, there exists $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(x) \in \mathfrak{P}_j$, so $x \in \tau^{-1}(\mathfrak{P}_j)$, that is $x \equiv 0 \mod \tau^{-1}(\mathfrak{P}_j)$, a contradiction. $\square$

Corollary 4.4.5. *Suppose L/K is Galois. Then $e_1 = \dots = e_r = \mathrm{e}$ and $f_1 = \dots = f_r = \mathrm{f}$, and we have $n = \mathrm{ef}r$.*

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

- $\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathfrak{P}_1)^{e_1} \dots \sigma(\mathfrak{P}_r)^{e_r}$, so $e_1 = \dots = e_r$, and
- $\mathcal{O}_L/\mathfrak{P}_i = \mathcal{O}_L/\sigma(\mathfrak{P}_i)$, so $f_1 = \dots = f_r$.

□

Let L/K be complete discretely valued fields with normalised valuations v_L and v_K and uniformisers π_L and π_K. The **ramification index** is $\mathrm{e} = \mathrm{e}_{L/K} = \mathrm{v}_L(\pi_K)$, that is $\pi_L^{\mathrm{e}}\mathcal{O}_L = \pi_K\mathcal{O}_L$. The **residue class degree** is $\mathrm{f} = \mathrm{f}_{L/K} = [\kappa_L : \kappa]$.

Corollary 4.4.6. *Suppose either*

1. *L/K is finite separable, or*
2. *f is finite.*

Then $[L : K] = \mathrm{ef}$.

Proof.

1. Theorem 4.4.3.
2. Can apply the same proof as in Theorem 4.4.3 if we know $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$-module. As before, $\dim_\kappa \mathcal{O}_L/\pi_K\mathcal{O}_L = \mathrm{ef} < \infty$. Let $x_1, \dots, x_m \in \mathcal{O}_L$ be a set of coset representatives for a κ-basis for $\mathcal{O}_L/\pi_K\mathcal{O}_L$. For $y \in \mathcal{O}_L$, can write
$$y = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{m} a_{ij} x_j \right) \pi_K^i = \sum_{j=1}^{m} \left(\sum_{i=0}^{\infty} a_{ij} \pi_K^i \right) x_j, \qquad a_{ij} \in \mathcal{O}_K,$$
by Proposition 1.3.5, so $\mathcal{O}_L$ is finitely generated over $\mathcal{O}_K$.

□

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

Definition 4.4.7. Let L/K be finite Galois. The **decomposition group** at a prime $\mathfrak{P}$ of $\mathcal{O}_L$ is the subgroup of $\mathrm{Gal}(L/K)$ defined by
$$\mathrm{G}_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Proposition 4.4.4 shows that for any $\mathfrak{P}$ and $\mathfrak{P}'$ dividing $\mathfrak{p}$, $\mathrm{G}_{\mathfrak{P}}$ and $\mathrm{G}_{\mathfrak{P}'}$ are conjugate and $\mathrm{G}_{\mathfrak{P}}$ has size ef. Recall we write $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ for the completions of L and K with respect to $|\cdot|_{\mathfrak{P}}$ and $|\cdot|_{\mathfrak{p}}$ respectively.

Proposition 4.4.8. *Suppose L/K is finite Galois and $\mathfrak{P}$ is a prime ideal of L dividing $\mathfrak{p}$. Then*

1. *$L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois, and*
2. *there is a natural map $\mathrm{res} : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$ which is injective and has image $\mathrm{G}_{\mathfrak{P}}$.*

Proof.

1. Since L/K is Galois, L is the splitting field of a separable polynomial $f(X) \in K[X]$. Then $L_{\mathfrak{P}}$ is the splitting field of f considered as an element of $K_{\mathfrak{p}}[X]$, so $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois.
2. Let $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, then $\sigma(L) = L$ since L/K is normal, hence we have a map $\mathrm{res} : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L/K)$. Since L is dense in $L_{\mathfrak{P}}$, res is injective. By Lemma 3.4.2 $|\sigma(x)|_{\mathfrak{P}} = |x|_{\mathfrak{P}}$ for all $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ and $x \in L_{\mathfrak{P}}$. Then $\sigma(\mathfrak{P}) = \mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, so $\mathrm{res}\,\sigma \in \mathrm{G}_{\mathfrak{P}}$ for all $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. To show surjectivity it suffices to show that $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = \mathrm{ef} = |\mathrm{G}_{\mathfrak{P}}|$. We have already seen $|\mathrm{G}_{\mathfrak{P}}| = \mathrm{ef}$. We can apply Corollary 4.4.6 to $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ noting that e and f do not change when we take completions.

□

5 Ramification theory

5.1 Unramified and totally ramified extensions

Lecture 14 Monday 09/11/20

Let K be a non-archimedean local field and L a finite separable extension of K. Then L is a local field. Then

$$[L : K] = \mathrm{e}_{L/K}\mathrm{f}_{L/K}. \tag{5}$$

Lemma 5.1.1. *Let $M/L/K$ be finite separable extensions of local fields. Then*

1. $\mathrm{e}_{M/K} = \mathrm{e}_{M/L}\mathrm{e}_{L/K}$, *and*
2. $\mathrm{f}_{M/K} = \mathrm{f}_{M/L}\mathrm{f}_{L/K}$.

Proof.

2. $\mathrm{f}_{M/K} = [\kappa_M : \kappa] = [\kappa_M : \kappa_L][\kappa_L : \kappa] = \mathrm{f}_{M/L}\mathrm{f}_{L/K}$.
1. 2 and (5).

□

Definition 5.1.2. The extension L/K is said to be

- **unramified** if $\mathrm{e}_{L/K} = 1$, if and only if $\mathrm{f}_{L/K} = [L : K]$,
- **ramified** if $\mathrm{e}_{L/K} > 1$, if and only if $\mathrm{f}_{L/K} < [L : K]$, and
- **totally ramified** if $\mathrm{e}_{L/K} = [L : K]$, if and only if $\mathrm{f}_{L/K} = 1$.

Theorem 5.1.3. *Let L/K be a finite separable extension of local fields, then there exists a field K_0 such that $K \subseteq K_0 \subseteq L$ and such that*

- *K_0/K is unramified, and*
- *L/K_0 is totally ramified.*

Moreover $[K_0 : K] = \mathrm{f}_{L/K}$ and $[L : K_0] = \mathrm{e}_{L/K}$, and K_0/K is Galois.

Proof. Let $\kappa = \mathbb{F}_q$, so that $\kappa_L = \mathbb{F}_{q^{\mathrm{f}}}$ for $\mathrm{f} = \mathrm{f}_{L/K}$. Set $m = q^{\mathrm{f}} - 1$. Let $[\cdot] : \mathbb{F}_{q^{\mathrm{f}}}^\times \to L^\times$ be the Teichmüller map for L and let $\zeta_m = [a]$ where a is a generator of $\mathbb{F}_{q^{\mathrm{f}}}^\times$. Then ζ_m is a primitive m-th root of unity, by lecture 5. We set

$$K_0 = K(\zeta_m) \subseteq L.$$

Then K_0 is the splitting field of the separable polynomial $f(X) = X^m - 1 \in K[X]$, hence K_0/K is Galois. Since $|\zeta_m| = 1$, we have $\zeta_m \in \mathcal{O}_{K_0}^\times$. Since $X^m - 1$ is separable over $\mathbb{F}_q$, ζ_m is a primitive m-th root of unity in $\kappa_0 = \mathcal{O}_{K_0}/\mathfrak{m}_0$, so $\kappa_0 \cong \mathbb{F}_{q^{\mathrm{f}}} = \kappa_L$. Now $\mathrm{Gal}(K_0/K)$ preserves $\mathcal{O}_{K_0}$ and $\mathfrak{m}_0$, using $|x| = |\sigma(x)|$ for all $x \in K_0$ and $\sigma \in \mathrm{Gal}(K_0/K)$. Thus there is a natural map

$$\mathrm{res} : \mathrm{Gal}(K_0/K) \to \mathrm{Gal}(\kappa_0/\kappa).$$

For $\sigma \in \mathrm{Gal}(K_0/K)$ we have $\sigma(\zeta_m) = \zeta_m$ if $\sigma(\zeta_m) \equiv \zeta_m \mod \mathfrak{m}_0$. This follows from the fact that $\sigma(\zeta_m) = [(\mathrm{res}\,\sigma)(\zeta_m \mod \mathfrak{m}_0)]$. Thus res is injective. It follows that $|\mathrm{Gal}(K_0/K)| \le |\mathrm{Gal}(\kappa_0/\kappa)| = \mathrm{f} = \mathrm{f}_{L/K}$, so $[K_0 : K] = \mathrm{f}_{L/K}$ and res is an isomorphism. Thus K_0/K is unramified. Since $\kappa_0 \cong \kappa_L$, $\mathrm{f}_{L/K_0} = 1$ and hence L/K_0 is totally ramified. □

We obtain the following description of unramified extensions.

Theorem 5.1.4. *Let K be a non-archimedean local field with $\kappa \cong \mathbb{F}_q$. For any $n \ge 1$, there is a unique unramified extension L/K of degree n. Moreover L/K is Galois and the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa)$ is an isomorphism. In particular $\mathrm{Gal}(L/K)$ is cyclic group generated by an element $\mathrm{Fr}_{L/K}$ such that*

$$\mathrm{Fr}_{L/K}(x) \equiv x^q \mod \mathfrak{m}_L, \qquad x \in \mathcal{O}_L.$$

Proof. For $n \geq 1$, we take $L = K(\zeta_m)$ where $m = q^n - 1$ and $\zeta_m \in \overline{K}^\times$ is a primitive m-th root of unity. Then as in the proof of Theorem 5.1.3,

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(\kappa_L/\kappa) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q),$$

and is cyclic and generated by a lift of $x \mapsto x^q$. Uniqueness is clear since for L/K degree n unramified, we have $\zeta_m \in L$ and hence $L = K(\zeta_m)$ by degree reasons. □

Corollary 5.1.5. *Let K be a non-archimedean local field, and let L/K be finite Galois. Then the natural map* $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa)$ *is surjective.*

Proof. With the notation of Theorem 5.1.3 the map res factors as

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K_0/K) \xrightarrow{\sim} \mathrm{Gal}(\kappa_L/\kappa).$$

□

Definition 5.1.6. Let L/K be a finite Galois extension of local fields. The **inertia subgroup** $\mathrm{I}_{L/K} \subseteq \mathrm{Gal}(L/K)$ is defined to be the kernel of the surjective map $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(\kappa_L/\kappa)$.

Since $\mathrm{e}_{L/K}\mathrm{f}_{L/K} = [L : K]$, we have $\left|\mathrm{I}_{L/K}\right| = \mathrm{e}_{L/K}$. There is an exact sequence

$$0 \to \mathrm{I}_{L/K} \xrightarrow{\iota} \mathrm{Gal}(L/K) \xrightarrow{\rho} \mathrm{Gal}(\kappa_L/\kappa) \to 0.$$

By exactness, $\mathrm{I}_{L/K} = \ker\rho$ and $\mathrm{Gal}(\kappa_L/\kappa) = \mathrm{coker}\,\iota$. Then $\mathrm{I}_{L/K} = \mathrm{Gal}(L/K_0)$, where L/K_0 is totally ramified.

Definition 5.1.7. Let K be a non-archimedean local field, with normalised valuation v. Let $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathcal{O}_K[X]$. We say $f(X)$ is **Eisenstein** if $\mathrm{v}(a_i) \geq 1$ for all i and $\mathrm{v}(a_0) = 1$.

Fact. If $f(X)$ is Eisenstein, then $f(X)$ is irreducible.

Theorem 5.1.8.

1. *If L/K is a finite totally ramified extension of non-archimedean local fields, then the minimal polynomial of $\pi_L \in \mathcal{O}_L$ is an Eisenstein polynomial and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, so $L = K(\pi_L)$.*

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

Proof.

1. Let v_L be the normalised valuation for L and set $\mathrm{e} = [L : K]$. Let $f(X) = X^m + a_{m-1}X^{m-1} + \dots + a_0 \in \mathcal{O}_K[X]$ be the minimal polynomial for π_L, which is monic since $\mathcal{O}_L$ is integral over $\mathcal{O}_K$. Then $m \leq \mathrm{e}$. Since $\mathrm{v}_L(K^\times) = \mathrm{e}\mathbb{Z}$, we have $\mathrm{v}_L\left(a_i\pi_L^i\right) \equiv i \mod \mathrm{e}$ for $i < m$, so that these terms all have different residues modulo e. We have $\pi_L^m = -\sum_{i=0}^{m-1} a_i\pi_L^i$ hence

   $$m = \mathrm{v}_L(\pi_L^m) = \min_{0 \leq i \leq m-1} (i + \mathrm{e}\mathrm{v}_K(a_i)),$$

   so $\mathrm{v}_K(a_i) \geq 1$ for all i, $m = \mathrm{e}$, and $\mathrm{v}_K(a_0) = 1$. Thus $f(X)$ is Eisenstein, and $L = K(\pi_L)$. For $y \in L$, we write $y = \sum_{i=0}^{\mathrm{e}-1} \pi_L^i b_i$ for $b_i \in K$. Then

   $$\mathrm{v}_L(y) = \min_{0 \leq i \leq m-1} (i + \mathrm{e}\mathrm{v}_K(b_i)).$$

   Thus $y \in \mathcal{O}_L$ if and only if $\mathrm{v}_L(y) \geq 0$, if and only if $\mathrm{v}_K(b_i) \geq 0$ for all i, if and only if $y \in \mathcal{O}_K[\pi_L]$.

2. Let $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ be Eisenstein and let $\mathrm{e} = \mathrm{e}_{L/K}$. Thus $\mathrm{v}_L(a_i) \geq \mathrm{e}$ and $\mathrm{v}_L(a_0) = \mathrm{e}$. If $\mathrm{v}_L(\alpha) \leq 0$ we have $\mathrm{v}_L(\alpha^n) < \mathrm{v}_L\left(\sum_{i=0}^{n-1} a_i\alpha^i\right)$ hence $\mathrm{v}_L(\alpha) > 0$. For $i \neq 0$, $\mathrm{v}_L\left(a_i\alpha^i\right) > \mathrm{e} = \mathrm{v}_L(a_0)$. It follows that $\mathrm{v}_L\left(-\sum_{i=0}^{n-1} a_i\alpha^i\right) = \mathrm{e}$ and hence $\mathrm{v}_L(\alpha^n) = \mathrm{e}$, so $n\mathrm{v}_L(\alpha) = \mathrm{e}$. But $n = [L : K] \geq \mathrm{e}$, so $n = \mathrm{e}$ and L is totally ramified.

□

5.2 Structure of units

Lecture 15
Wednesday
11/11/20

Let $[K : \mathbb{Q}_p] < \infty$, with normalised valuation v_K and uniformiser π, and let $\mathrm{e} = \mathrm{e}_{K/\mathbb{Q}_p}$, the **absolute ramification index**.

Proposition 5.2.1. *If $r > \mathrm{e}/(p-1)$, then the series*

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

converges on $\pi^r \mathcal{O}_K$ and $\exp$ *determines an isomorphism $(\pi^r \mathcal{O}_K, +) \xrightarrow{\sim} (1 + \pi^r \mathcal{O}_K, \times)$.*

Proof. By example sheet 1,

$$\mathrm{v}_K(n!) = \mathrm{e}\mathrm{v}_p(n!) = \mathrm{e}\left(\frac{n - \mathrm{s}_p(n)}{p-1}\right) \le \mathrm{e}\left(\frac{n-1}{p-1}\right).$$

For $x \in \pi^r \mathcal{O}_K$, we have for $n \ge 1$,

$$\mathrm{v}_K\left(\frac{x^n}{n!}\right) \ge nr - \mathrm{e}\left(\frac{n-1}{p-1}\right) = r + (n-1)\left(r - \frac{\mathrm{e}}{p-1}\right) \to \infty,$$

as $n \to \infty$. Thus $\exp x$ converges. Since $\mathrm{v}_K(x^n/n!) \ge r$ for $n \ge 1$, $\exp x \in 1 + \pi^r \mathcal{O}_K$. Similarly consider

$$\begin{array}{rccl} \log & : & 1 + \pi^r \mathcal{O}_K & \longrightarrow & \pi^r \mathcal{O}_K \\ & & 1 + x & \longmapsto & \displaystyle\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n \end{array}.$$

Can check convergence as before. Recall properties of power series

$$\exp(X + Y) = \exp X \exp Y, \qquad \exp \log X = X, \qquad \log \exp X = X.$$

Thus $\exp : (\pi^r \mathcal{O}_K, +) \to (1 + \pi^r \mathcal{O}_K, \times)$ is an isomorphism of groups. ∎

Now let K be a non-archimedean local field. We define a filtration on $\mathcal{O}_K^\times$. Write $\mathrm{U}_K = \mathcal{O}_K^\times$.

Definition 5.2.2. For $s \in \mathbb{Z}_{\ge 1}$, the **s-th unit group** $\mathrm{U}_K^{(s)}$ is defined by

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

We set $\mathrm{U}_K^{(0)} = \mathrm{U}_K$. Then we have

$$\dots \subseteq \mathrm{U}_K^{(s)} \subseteq \dots \subseteq \mathrm{U}_K^{(1)} \subseteq \mathrm{U}_K^{(0)} = \mathrm{U}_K.$$

Proposition 5.2.3. *We have*

1. $\mathrm{U}_K^{(0)}/\mathrm{U}_K^{(1)} \cong (\kappa^\times, \times)$ *for $\kappa = \mathcal{O}_K/\pi\mathcal{O}_K$, and*
2. $\mathrm{U}_K^{(s)}/\mathrm{U}_K^{(s+1)} \cong (\kappa, +)$ *for $s \ge 1$.*

Proof.

1. Reduction modulo π gives a natural surjection $\mathcal{O}_K^\times \to \kappa^\times$. The kernel is $1 + \pi\mathcal{O}_K = \mathrm{U}_K^{(1)}$.
2. Define
$$\begin{array}{rccl} f & : & \mathrm{U}_K^{(s)} & \longrightarrow & \kappa \\ & & 1 + \pi^s x & \longmapsto & x \mod \pi \end{array}.$$
Then $(1 + \pi^s x)(1 + \pi^s y) = 1 + \pi^s(x + y + \pi^s xy)$ and $x + y + \pi^s xy \equiv x + y \mod \pi$, hence f is a group homomorphism. It is easy to see f is surjective and $\ker f = \mathrm{U}_K^{(s+1)}$.

∎

Corollary 5.2.4. *Let $[K : \mathbb{Q}_p] < \infty$. Then $\mathcal{O}_K^\times$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

Proof. If $r > \mathrm{e}/(p-1)$, then $(\mathcal{O}_K, +) \cong \mathrm{U}_K^{(r)}$, so $\mathrm{U}_K^{(r)} \subseteq \mathrm{U}_K$ is finite index by Proposition 5.2.3. ☐

Example. If $\mathbb{Z}_p$ for $p > 2$, then $\mathrm{e} = 1$ and can take $r = 1$. Then there is an isomorphism

$$\begin{array}{ccc} \mathbb{Z}_p^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \\ x & \longmapsto & \left(x \mod p, \dfrac{x}{[x \mod p]}\right) \end{array}.$$

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

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

Get another proof that

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

5.3 Higher ramification groups

Let L/K be a finite Galois extension of local fields. We define an analogous filtration of $\mathrm{Gal}(L/K)$.

Definition 5.3.1. Let v_L be the normalised valuation on L. For $s \in \mathbb{R}_{\geq -1}$, we define the ***s*-th ramification group** by

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

Example. $\mathrm{G}_{-1}(L/K) = \mathrm{Gal}(L/K)$. If π_L is a uniformiser in L, then

$$\mathrm{G}_0(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \forall x \in \mathcal{O}_L,\ \sigma(x) \equiv x \mod \pi_L\} = \ker(\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(\kappa_L/\kappa)) = \mathrm{I}_{L/K}.$$

Note that for $s \in \mathbb{Z}_{\geq 0}$

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

hence $\mathrm{G}_s(L/K)$ is normal in $\mathrm{Gal}(L/K)$. We have for $s \in \mathbb{Z}_{\geq -1}$

$$\dots \subseteq \mathrm{G}_s \subseteq \dots \subseteq \mathrm{G}_0 \subseteq \mathrm{G}_{-1} = \mathrm{Gal}(L/K).$$

Remark. G_s only changes at the integers. The definition for $s \in \mathbb{R}_{\geq -1}$ will be used later.

Theorem 5.3.2.

1. *Let $\pi_L \in \mathcal{O}_L$ be a uniformiser. For $s \geq 0$,*

$$\mathrm{G}_s = \{\sigma \in \mathrm{G}_0 \mid \mathrm{v}_L(\sigma(\pi_L) - \pi_L) \geq s + 1\}.$$

2. *$\bigcap_{n=0}^{\infty} \mathrm{G}_n = \{1\}$.*
3. *Let $s \in \mathbb{Z}_{\geq 0}$. There is an injective group homomorphism induced by the map*

$$\begin{array}{ccc} \mathrm{G}_s/\mathrm{G}_{s+1} & \longrightarrow & \mathrm{U}_L^{(s)}/\mathrm{U}_L^{(s+1)} \\ \sigma & \longmapsto & \dfrac{\sigma(\pi_L)}{\pi_L} \end{array}.$$

   This map is independent of the choice of π_L.

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

1. By Theorem 5.1.8, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Suppose $\mathrm{v}_L(\sigma(\pi_L) - \pi_L) \geq s + 1$. Let $x \in \mathcal{O}_L$, then $x = f(\pi_L)$ for $f(X) \in \mathcal{O}_K[X]$. Then

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

   where $g(X) \in \mathcal{O}_K[X]$, using $X^n - Y^n = (X - Y)\left(X^{n-1} + \dots + Y^{n-1}\right)$. Thus $\mathrm{v}_L(\sigma(x) - x) = \mathrm{v}_L(\sigma(\pi_L) - \pi_L) + \mathrm{v}_L(g(\pi_L)) \geq s + 1$.

2. Suppose $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma \neq \mathrm{id}$. Then $\sigma(\pi_L) \neq \pi_L$ because $L = K(\pi_L)$, and hence $\mathrm{v}_L(\sigma(\pi_L) - \pi_L) < \infty$. Thus $\sigma \notin \mathrm{G}_s$ for $s \gg 0$.

3. Note that for $\sigma \in \mathrm{G}_s$ and $s \in \mathbb{Z}_{\geq 0}$, $\sigma(\pi_L) \in \pi_L + \pi_L^{s+1}\mathcal{O}_L$, so $\sigma(\pi_L)/\pi_L \in 1 + \pi_L^s\mathcal{O}_L$. We claim

$$\begin{array}{rcccc} \phi & : & \mathrm{G}_s & \longrightarrow & \mathrm{U}_L^{(s)}/\mathrm{U}_L^{(s+1)} \\ & & \sigma & \longmapsto & \dfrac{\sigma(\pi_L)}{\pi_L} \end{array}$$

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

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

But $\sigma(u) \in u + \pi_L^{s+1}\mathcal{O}_L$ since $\sigma \in \mathrm{G}_s$ thus $\sigma(u)/u \in \mathrm{U}_L^{(s+1)}$ and hence

$$\frac{\sigma\tau(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \cdot \frac{\tau(\pi_L)}{\pi_L} \mod \mathrm{U}_L^{(s+1)},$$

so ϕ is a group homomorphism. Moreover

$$\ker\phi = \left\{\sigma \in \mathrm{G}_s \;\middle|\; \sigma(\pi_L) \equiv \pi_L \mod \pi_L^{s+2}\right\} = \mathrm{G}_{s+1}.$$

If $\pi_L' = a\pi_L$ is another uniformiser for $a \in \mathrm{U}_L$, then

$$\frac{\sigma(\pi_L')}{\pi_L'} = \frac{\sigma(a)}{a} \cdot \frac{\sigma(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \mod \mathrm{U}_L^{(s+1)}.$$

$\square$

Lecture 16 Friday 13/11/20

Corollary 5.3.3. *Let L/K be a finite Galois extension of non-archimedean local fields. Then* $\mathrm{Gal}(L/K)$ *is solvable.*

Proof. By Proposition 5.2.3, Theorem 5.3.2, and Theorem 5.1.4, for $s \in \mathbb{Z}_{\geq -1}$

$$\mathrm{G}_s/\mathrm{G}_{s+1} \hookrightarrow \begin{cases} \mathrm{Gal}(\kappa_L/\kappa) & s = -1 \\ (\kappa_L^\times, \times) & s = 0 \\ (\kappa_L, +) & s \geq 1 \end{cases}.$$

Thus $\mathrm{G}_s/\mathrm{G}_{s+1}$ is abelian for $s \geq -1$. Conclude using Theorem 5.3.2.2. $\square$

Let $\mathrm{ch}\,\kappa = p$. Then $|\mathrm{G}_0/\mathrm{G}_1|$ is coprime to p and $|\mathrm{G}_1| = p^n$ for some $n \geq 0$. Thus G_1 is the unique, since normal, Sylow p-subgroup of $\mathrm{G}_0 = \mathrm{I}_{L/K}$.

Definition 5.3.4. The group G_1 is called the **wild inertia group** and $\mathrm{G}_0/\mathrm{G}_1$ is the **tame quotient**. Say L/K, not necessarily Galois, is **tamely ramified** if $\mathrm{ch}\,\kappa = p \nmid \mathrm{e}_{L/K}$, which is if and only if $\mathrm{G}_1 = \{1\}$ if L/K is Galois. Otherwise it is **wildly ramified**.

Thus

$$\begin{tikzcd} L \arrow[dd, dash] \arrow[dr, dash, "\text{totally wildly ramified}"] & \\ & K' \arrow[d, dash, "\text{totally tamely ramified}"] \\ K \arrow[r, phantom] & K_0 \arrow[l, dash, "\text{unramified}"] \end{tikzcd} .$$

Example. Let $K = \mathbb{Q}_p$. Let ζ_{p^n} be a primitive p^n-th root of unity, and let $L = \mathbb{Q}_p(\zeta_{p^n})$. Then the p^n-th cyclotomic polynomial

$$\Phi_{p^n}(X) = X^{p^{n-1}(p-1)} + \dots + 1$$

is the minimal polynomial of ζ_{p^n}. By example sheet 3,

- $\Phi_{p^n}(X)$ is irreducible,
- $L/\mathbb{Q}_p$ is Galois and totally ramified of degree $p^{n-1}(p-1)$, and
- $\pi = \zeta_{p^n} - 1$ is a uniformiser of $\mathcal{O}_L$, and hence $\mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^n} - 1] = \mathbb{Z}_p[\zeta_{p^n}]$.

We have an isomorphism of abelian groups

$$\begin{array}{rcl} (\mathbb{Z}/p^n\mathbb{Z})^\times & \longrightarrow & \mathrm{Gal}(L/\mathbb{Q}_p) \\ m & \longmapsto & \left(\sigma_m : \zeta_{p^n} \mapsto \zeta_{p^n}^m\right) \end{array} .$$

Thus $\sigma_m(\pi) - \pi = \zeta_{p^n}^m - \zeta_{p^n} = \left(\zeta_{p^n}^{m-1} - 1\right)\zeta_{p^n}$. 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 $L' = \mathbb{Q}_p\left(\zeta_{p^n}^{m-1}\right)$. Thus

$$\mathrm{v}_L(\sigma_m(\pi) - \pi) = \mathrm{v}_L(\pi') = \mathrm{e}_{L/L'} = \frac{\mathrm{e}_{L/\mathbb{Q}_p}}{\mathrm{e}_{L'/\mathbb{Q}_p}} = \frac{[L : \mathbb{Q}_p]}{[L' : \mathbb{Q}_p]} = \frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k.$$

By Theorem 5.3.2.1, $\sigma_m \in \mathrm{G}_i$ if and only if $p^k \ge i + 1$. Thus

$$\mathrm{G}_i \cong \begin{cases} (\mathbb{Z}/p^n\mathbb{Z})^\times & i \le 0 \\ \left(1 + p^k\mathbb{Z}\right)/p^n\mathbb{Z} & p^{k-1} - 1 < i \le p^k - 1, \ 1 \le k \le n - 1 \\ \{1\} & i > p^{n-1} - 1 \end{cases},$$

which is reminiscent of $\mathrm{U}_{\mathbb{Q}_p}^{(k)}$.

5.4 Upper numbering of ramification groups

G_s behaves well with respect to taking subgroups.

Proposition 5.4.1. *Let $L/F/K$ be finite extensions of non-archimedean local fields, and let L/K be Galois. Then for $s \in \mathbb{R}_{\ge -1}$,*

$$\mathrm{G}_s(L/F) = \mathrm{G}_s(L/K) \cap \mathrm{Gal}(L/F).$$

Proof.

$$\mathrm{G}_s(L/F) = \{\sigma \in \mathrm{Gal}(L/F) \mid \forall x \in \mathcal{O}_L, \ \mathrm{v}_L(\sigma(x) - x) \ge s + 1\} = \mathrm{Gal}(L/F) \cap \mathrm{G}_s(L/K).$$

□

However G_s behaves badly with respect to taking quotients. Fix this by renumbering. Let L/K be finite Galois. Define a function by

$$\begin{array}{rcccl} \phi = \phi_{L/K} & : & \mathbb{R}_{\ge -1} & \longrightarrow & \mathbb{R} \\ & & s & \longmapsto & \displaystyle\int_0^s \frac{1}{[\mathrm{G}_0 : \mathrm{G}_t]} \, \mathrm{d}t \end{array} .$$

By convention, if $t \in [-1, 0)$, then

$$\frac{1}{[\mathrm{G}_0 : \mathrm{G}_t]} = [\mathrm{G}_t : \mathrm{G}_0].$$

We have for $m \le s < m + 1$ for $m \in \mathbb{Z}_{\ge -1}$,

$$\phi(s) = \begin{cases} s & m = -1 \\ \dfrac{1}{|\mathrm{G}_0|}\left(|\mathrm{G}_1| + \dots + |\mathrm{G}_m| + (s - m)|\mathrm{G}_{m+1}|\right) & m \ge 0 \end{cases}.$$

Thus

- ϕ is continuous and piecewise linear, and
- ϕ is strictly increasing.

Notation. Let $L/F/K$ be finite extensions of non-archimedean local fields with L/K and F/K Galois, and let $\mathrm{G} = \mathrm{Gal}(L/K)$ and $\mathrm{H} = \mathrm{Gal}(L/F)$, so $\mathrm{G}/\mathrm{H} = \mathrm{Gal}(F/K)$. If $s \in \mathbb{R}_{\geq -1}$, then G_s, H_s, and $(\mathrm{G}/\mathrm{H})_s$ are the s-th higher ramification groups for G, H, and G/H respectively.

Theorem 5.4.2 (Herbrand's theorem)**.** *Let $L/F/K$ as above. Then for $s \in \mathbb{R}_{\geq -1}$ we have*

$$\mathrm{G}_s\mathrm{H}/\mathrm{H} = (\mathrm{G}/\mathrm{H})_{\phi_{L/F}(s)}.$$

As $\phi_{L/K}$ is continuous and strictly increasing, we may define $\psi_{L/K} = \phi_{L/K}^{-1}$.

Definition 5.4.3. Let L/K be finite Galois. The **higher ramification groups in upper numbering** is defined by

$$\mathrm{G}^s(L/K) = \mathrm{G}_{\psi_{L/K}(s)}(L/K).$$

Can rephrase Theorem 5.4.2 as follows.

Lemma 5.4.4. *Let $L/F/K$ as above.*

1. $\phi_{L/K} = \phi_{F/K} \circ \phi_{L/F}$.
2. $\psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}$.

Proof. Since $\psi = \phi^{-1}$, it suffices to prove 1. Then $\phi_{L/K}$ and $\phi_{F/K} \circ \phi_{L/F}$ are continuous and piecewise linear and $\phi_{L/K}(0) = \left(\phi_{F/K} \circ \phi_{L/F}\right)(0) = 0$. Thus it suffices to show derivatives are equal. Let $r = \phi_{L/F}(s)$. By the fundamental theorem of calculus,

$$\left(\phi_{F/K} \circ \phi_{L/F}\right)'(s) = \phi'_{L/F}(s)\,\phi'_{F/K}(r) = \frac{|\mathrm{H}_s|}{|\mathrm{H}_0|} \cdot \frac{|(\mathrm{G}/\mathrm{H})_r|}{|(\mathrm{G}/\mathrm{H})_0|} = \frac{|\mathrm{H}_s|}{\mathrm{e}_{L/F}} \cdot \frac{|(\mathrm{G}/\mathrm{H})_r|}{\mathrm{e}_{F/K}}.$$

Theorem 5.4.2 implies $(\mathrm{G}/\mathrm{H})_r = \mathrm{G}_s\mathrm{H}/\mathrm{H} = \mathrm{G}_s/(\mathrm{G}_s \cap \mathrm{H}) = \mathrm{G}_s/\mathrm{H}_s$, by Proposition 5.4.1. Thus

$$\phi'_{L/K}(s) = \frac{|\mathrm{G}_s|}{|\mathrm{G}_0|} = \frac{|\mathrm{H}_s||(\mathrm{G}/\mathrm{H})_r|}{\mathrm{e}_{L/K}} = \frac{|\mathrm{H}_s|}{\mathrm{e}_{L/F}} \cdot \frac{|(\mathrm{G}/\mathrm{H})_r|}{\mathrm{e}_{F/K}}.$$

□

Corollary 5.4.5. *For $t \in [-1, \infty)$*

$$\mathrm{G}^t\mathrm{H}/\mathrm{H} = (\mathrm{G}/\mathrm{H})^t.$$

Proof. Let $r = \psi_{F/K}(t)$. Then by Theorem 5.4.2,

$$(\mathrm{G}/\mathrm{H})^t = (\mathrm{G}/\mathrm{H})_r = \mathrm{G}_{\psi_{L/F}(r)}\mathrm{H}/\mathrm{H} = \mathrm{G}^t\mathrm{H}/\mathrm{H},$$

since $\mathrm{G}_{\psi_{L/F}(r)} = \mathrm{G}_{\psi_{L/K}(t)} = \mathrm{G}^t$, by Lemma 5.4.4. □

5.5 Proof of Herbrand's theorem

Lecture 17 Monday 16/11/20

We introduce an auxiliary function.

Definition 5.5.1. Let L/K be finite Galois, and let $\mathrm{id} \neq \sigma \in \mathrm{Gal}(L/K)$. Define

$$\begin{array}{rcccl} \mathrm{i}_{L/K} & : & \mathrm{Gal}(L/K) & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ & & \sigma & \longmapsto & \min_{x \in \mathcal{O}_L} \mathrm{v}_L(\sigma(x) - x) = \max\{i \in \mathbb{Z} \mid \sigma \in \mathrm{G}_{i-1}\} \end{array}.$$

By convention, $\mathrm{i}_{L/K}(\mathrm{id}) = \infty$.

Note that

$$\mathrm{G}_s(L/K) = \left\{\sigma \in \mathrm{Gal}(L/K) \;\middle|\; \mathrm{i}_{L/K}(\sigma) \geq s + 1\right\}.$$

Lemma 5.5.2. *Let L/K be finite Galois. Let $x \in \mathcal{O}_L$ such that $\mathcal{O}_K[x] = \mathcal{O}_L$. Then*

1. $\mathrm{i}_{L/K}(\sigma) = \mathrm{v}_L(\sigma(x) - x)$, *and*
2. *we have*
$$\mathrm{G}_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \mathrm{v}_L(\sigma(x) - x) \geq s + 1\}.$$

Proof. Let $y \in \mathcal{O}_L$, then $y = f(x)$ for $f(x) \in \mathcal{O}_K[x]$. The same argument as in Theorem 5.3.2.1 shows that $\sigma(x) - x \mid \sigma(y) - y$ in $\mathcal{O}_L$, so $\mathrm{v}_L(\sigma(y) - y) \geq \mathrm{v}_L(\sigma(x) - x)$, which implies 1 and 2. ☐

Proposition 5.5.3. *Let $L/F/K$ as above, and let $\sigma \in \mathrm{G}$. Then we have*
$$\mathrm{i}_{F/K}(\sigma\mathrm{H}) = \mathrm{e}_{L/F}^{-1} \sum_{\tau \in \mathrm{H}} \mathrm{i}_{L/K}(\sigma\tau).$$

Proof. When $\sigma \in \mathrm{H}$, we interpret as $\infty = \infty$. Thus assume $\sigma \notin \mathrm{H}$. Let v_L and v_F be the normalised valuations on L and F. Let $x \in \mathcal{O}_F$ and $y \in \mathcal{O}_L$, such that $\mathcal{O}_F = \mathcal{O}_K[x]$ and $\mathcal{O}_L = \mathcal{O}_K[y]$. Define
$$a = \sigma(x) - x \in \mathcal{O}_L, \qquad b = \prod_{\tau \in \mathrm{H}} (\sigma\tau(y) - y) \in \mathcal{O}_L.$$

Then by Lemma 5.5.2,
$$\mathrm{e}_{L/F}\mathrm{i}_{F/K}(\sigma\mathrm{H}) = \mathrm{e}_{L/F}\mathrm{v}_F(\sigma(x) - x) = \mathrm{v}_L(\sigma(x) - x) = \mathrm{v}_L(a).$$

And
$$\sum_{\tau \in \mathrm{H}} \mathrm{i}_{L/K}(\sigma\tau) = \sum_{\tau \in \mathrm{H}} \mathrm{v}_L(\sigma\tau(y) - y) = \mathrm{v}_L\left(\prod_{\tau \in \mathrm{H}} (\sigma\tau(y) - y)\right) = \mathrm{v}_L(b).$$

Need to show $\mathrm{v}_L(a) = \mathrm{v}_L(b)$. We show that $a \mid b$ and $b \mid a$ in $\mathcal{O}_L$.

$a \mid b$. Let $f \in \mathcal{O}_F[X]$ be the minimal polynomial for y over $\mathcal{O}_F$. Then $f(X) = \prod_{\tau \in \mathrm{H}} (X - \tau(y))$ and $\sigma(f)(X) = \prod_{\tau \in \mathrm{H}} (X - \sigma\tau(y))$. Since $\mathcal{O}_F = \mathcal{O}_K[x]$, $a = \sigma(x) - x$ divides $\sigma(z) - z$ for all $z \in \mathcal{O}_F$, by Lemma 5.5.2. Thus a divides all coefficients of $\sigma(f)(X) - f(X)$, so
$$a \mid \sigma(f)(y) - f(y) = \sigma(f)(y) = \pm b.$$

$b \mid a$. Let $g \in \mathcal{O}_K[X]$ such that $x = g(y)$. Then $g(X) - x \in \mathcal{O}_F[X]$ has y as a root, so $g(X) - x = f(X)h(X)$ for some $h \in \mathcal{O}_F[X]$. Applying σ and evaluating at y gives
$$\sigma(g)(y) - \sigma(x) = \sigma(f)(y)\sigma(h)(y) = \pm b\sigma(h)(y),$$
where $\sigma(h)(y) \in \mathcal{O}_L$. But $\sigma(g)(y) = g(y) = x$ and hence $b \mid a$.

☐

Lemma 5.5.4. *Let L/K be finite Galois, and let $\sigma \in \mathrm{G} = \mathrm{Gal}(L/K)$. Then*
$$\phi_{L/K}(s) = -1 + \frac{1}{|\mathrm{G}_0|} \sum_{\sigma \in \mathrm{G}} \min\left(\mathrm{i}_{L/K}(\sigma), s + 1\right), \qquad s \in \mathbb{R}_{\geq -1}.$$

Proof. Both sides are piecewise linear and continuous. Let $\theta(s)$ be the right hand side. Then $\phi_{L/K}(-1) = -1 = \theta(-1)$. Thus it suffices to show $\theta' = \phi'_{L/K}$, and
$$\theta'(s) = \frac{1}{|\mathrm{G}_0|} \cdot \#\left\{\sigma \in \mathrm{G} \mid \mathrm{i}_{L/K}(\sigma) \geq s + 1\right\} = \frac{|\mathrm{G}_s|}{|\mathrm{G}_0|} = \phi'_{L/K}(s).$$

☐

Proof of Theorem 5.4.2. Want $\mathrm{G}_s\mathrm{H}/\mathrm{H} = (\mathrm{G}/\mathrm{H})_{\phi_{L/F}(s)}$. Define a function by

$$\begin{array}{rcccl} j & : & \mathrm{G}/\mathrm{H} & \longrightarrow & \mathbb{Z}\cup\{\infty\} \\ & & \sigma\mathrm{H} & \longmapsto & \max_{\tau\in\mathrm{H}}\left\{\mathrm{i}_{L/K}(\sigma\tau)\right\} \end{array}, \qquad \sigma\in\mathrm{G}.$$

Then we have $\sigma\mathrm{H}\in\mathrm{G}_s\mathrm{H}/\mathrm{H}$ if and only if $j(\sigma\mathrm{H})-1\geq s$, if and only if $\phi_{L/F}(j(\sigma\mathrm{H})-1)\geq\phi_{L/F}(s)$, since ϕ is strictly increasing. On the other hand, we have $\sigma\mathrm{H}\in(\mathrm{G}/\mathrm{H})_{\phi_{L/F}(s)}$ if and only if $\mathrm{i}_{F/K}(\sigma\mathrm{H})-1\geq\phi_{L/F}(s)$. Thus it suffices to show

$$\phi_{L/F}(j(\sigma\mathrm{H})-1)=\mathrm{i}_{F/K}(\sigma\mathrm{H})-1.$$

Can assume $\sigma\notin\mathrm{H}$. Upon replacing σ by another element in $\sigma\mathrm{H}$ we may assume $j(\sigma\mathrm{H})=\mathrm{i}_{L/K}(\sigma)=m$, that is $\sigma\in\mathrm{G}_{m-1}\setminus\mathrm{G}_m$. If $\tau\in\mathrm{H}_{m-1}=\mathrm{G}_{m-1}\cap\mathrm{H}$, then $\sigma\tau\in\mathrm{G}_{m-1}$. Then $\mathrm{i}_{L/K}(\sigma\tau)\geq m$, so $\mathrm{i}_{L/K}(\sigma\tau)=m$ by maximality of m. On the other hand if $\tau\notin\mathrm{H}_{m-1}$, then $\sigma\tau\notin\mathrm{G}_{m-1}$, so $\mathrm{i}_{L/K}(\sigma\tau)<m$ and $\mathrm{i}_{L/K}(\sigma\tau)=\mathrm{i}_{L/K}(\tau)$. In either case, we have for any $\tau\in\mathrm{H}$, $\mathrm{i}_{L/K}(\sigma\tau)=\min\left(\mathrm{i}_{L/K}(\tau),m\right)$. By Proposition 5.5.3, we have

$$\mathrm{i}_{F/K}(\sigma\mathrm{H})=\mathrm{e}_{L/F}^{-1}\sum_{\tau\in\mathrm{H}}\min\left(\mathrm{i}_{L/K}(\tau),m\right).$$

But $\mathrm{i}_{L/K}(\tau)=\mathrm{i}_{L/F}(\tau)$ and $\mathrm{e}_{L/F}=|\mathrm{H}_0|$. Thus Lemma 5.5.4 implies

$$\mathrm{i}_{F/K}(\sigma\mathrm{H})=\frac{1}{|\mathrm{H}_0|}\sum_{\tau\in\mathrm{H}}\min\left(\mathrm{i}_{L/F}(\tau),m\right)=\phi_{L/F}(m-1)+1=\phi_{L/F}(j(\sigma\mathrm{H})-1)+1.$$

□

Example. Let $K=\mathbb{Q}_p$, and let $L=\mathbb{Q}_p(\zeta_{p^n})$. Then $\mathrm{G}\cong(\mathbb{Z}/p^n\mathbb{Z})^\times$. Let $k\in\mathbb{Z}$ such that $1\leq k\leq n-1$. For $p^{k-1}-1<s\leq p^k-1$,

$$\mathrm{G}_s\cong\left\{m\in(\mathbb{Z}/p^n\mathbb{Z})^\times\;\middle|\;m\equiv1\mod p^k\right\}.$$

Let us compute $\phi_{L/K}$. Since G_s jumps at p^k-1, $\phi_{L/K}$ is linear on $\left(p^{k-1}-1,p^k-1\right]$. It suffices to determine $\phi_{L/K}\left(p^k-1\right)$. Claim that

$$\phi_{L/K}\left(p^k-1\right)=k,\qquad 1\leq k\leq n-1.$$

Since $[\mathrm{G}_0:\mathrm{G}_t]=p^{t-1}(p-1)$,

$$\begin{aligned}\phi\left(p^k-1\right)&=\frac{1}{p^0(p-1)}\left(\left(p^1-1\right)-\left(p^0-1\right)\right)+\dots+\frac{1}{p^{k-1}(p-1)}\left(\left(p^k-1\right)-\left(p^{k-1}-1\right)\right)\\&=1+\dots+1=k.\end{aligned}$$

Thus

$$\mathrm{G}^s\cong\begin{cases}(\mathbb{Z}/p^n\mathbb{Z})^\times & s\leq0\\ \left(1+p^k\mathbb{Z}\right)/p^n\mathbb{Z} & k-1<s\leq k,\ 1\leq k\leq n-1\\ \{1\} & s>n-1\end{cases},$$

which seems much more natural. Note that $\phi\left(p^k-1\right)$ is an integer, which is a priori not clear.

Definition 5.5.5. We say i is a **jump** in the filtration $\{\mathrm{G}^s\}_{s\in\mathbb{R}_{\geq-1}}$ if $\mathrm{G}^i\neq\mathrm{G}^j$ for all $j>i$.

Theorem 5.5.6 (Hasse-Arf)**.** *If* $\mathrm{Gal}(L/K)$ *is abelian, then the jumps of the filtration* $\{\mathrm{G}^s\}_{s\in\mathbb{R}_{\geq-1}}$ *can only be integers.*

Proof. Omit. See Serre, Local fields, Chapter 4, Section 7. □

6 Local class field theory

6.1 Infinite Galois theory

Lecture 18
Wednesday
18/11/20

Let L/K be an algebraic extension of fields.

Definition 6.1.1. L/K is **separable** if for every $\alpha \in L$, the minimal polynomial $f_\alpha(X) \in K[X]$ for α is separable. It is **normal** if $f_\alpha(X)$ splits in L for all $\alpha \in L$. We say the extension L/K is **Galois** if it is separable and normal. In this case we write $\mathrm{Gal}(L/K) = \mathrm{Aut}_K L$.

If L/K is finite and Galois, the Galois correspondence is a one-to-one correspondence

$$\begin{array}{rcl} \{\text{subextensions } K \subseteq K' \subseteq L\} & \longrightarrow & \{\text{subgroups of } \mathrm{Gal}(L/K)\} \\ K' & \longmapsto & \mathrm{Gal}(L/K') \end{array}.$$

For L/K infinite, need to introduce a topology. Let $(I, \le)$ be a partially ordered set. We say that I is a **directed set** if for all $i, j \in I$ there is some $k \in I$ such that $i \le k$ and $j \le k$.

Example.

- Any total order, such as $(\mathbb{N}, \le)$.
- $(\mathbb{N}_{\ge 1}, |)$ ordered by divisibility.

Definition 6.1.2. Let $(I, \le)$ be a directed set and $(G_i)_{i \in I}$ a collection of groups together with transition maps $\phi_{ij} : G_j \to G_i$ for $i \le j$ such that $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$ whenever $i \le j \le k$ and $\phi_{ii} = \mathrm{id}$. We say $\left((G_i)_{i \in I}, \phi_{ij}\right)$ is an **inverse system**. The **inverse limit** of $\left((G_i)_{i \in I}, \phi_{ij}\right)$ is defined by

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

Remark.

- For $(\mathbb{N}, \le)$, recovers the previous definition.
- There exist projection maps $\psi_j : \varprojlim_{i \in I} G_i \to G_j$.
- $\varprojlim_{i \in I} G_i$ satisfies the universal property.

If all G_i are finite, we define the **profinite topology** on $\varprojlim_{i \in I} G_i$ as the weakest topology such that ψ_j are continuous for all $j \in I$.

Proposition 6.1.3. *Let L/K be Galois.*

- *The set*
$$I = \{F/K \text{ finite Galois} \mid F \subseteq L\}$$
is a directed set under $\subseteq$.
- *For $F, F' \in I$ such that $F \subseteq F'$, there is a restriction map $\mathrm{res}_{F,F'} : \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$ and the natural map*
$$\mathrm{Gal}(L/K) \to \varprojlim_{F \in I} \mathrm{Gal}(F/K)$$
is an isomorphism.

Proof. Example sheet 4. $\square$

Thus $\mathrm{Gal}(L/K)$ packages information of $\mathrm{Gal}(F/K)$ for all finite Galois subextensions, and is endowed with the profinite topology.

Example. Let $K = \mathbb{F}_q$, and let $L = \overline{\mathbb{F}_q}$ be an algebraic closure. There is a one-to-one correspondence

$$\begin{array}{ccc} \mathbb{N}_{\ge 1} & \longrightarrow & \{F/K \text{ finite Galois}\} \\ n & \longmapsto & \mathbb{F}_{q^n} \end{array},$$

since $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ if and only if $m \mid n$. Then

$$\begin{array}{ccccc} \mathrm{Fr}_q & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & \twoheadrightarrow & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) & \mathrm{Fr}_q \\ \updownarrow & \wr\Vert & & \wr\Vert & \updownarrow \\ 1 & \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\text{mod } m]{} & \mathbb{Z}/m\mathbb{Z} & 1 \end{array},$$

so

$$\begin{array}{ccc} \mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right) & \cong & \widehat{\mathbb{Z}} = \varprojlim_{n \in (\mathbb{N}_{\ge 1}, \mid)} \mathbb{Z}/n\mathbb{Z} \\ \mathrm{Fr}_q & \longleftrightarrow & 1 \\ \langle \mathrm{Fr}_q \rangle & \longleftrightarrow & \mathbb{Z} \end{array}.$$

By example sheet 3,

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

Theorem 6.1.4 (Fundamental theorem of Galois theory)**.** *Let L/K be Galois. There is a bijection*

$$\begin{array}{ccc} \{F/K \textit{ subextensions of } L/K\} & \longleftrightarrow & \{\textit{closed subgroups of } \mathrm{Gal}(L/K)\} \\ F & \longmapsto & \mathrm{Gal}(L/F) \\ L^H & \longleftarrow & H \end{array}.$$

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

Proof. Omit. □

6.2 The Weil group

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

Definition 6.2.1.

- L/K is **unramified** if F/K is unramified for all F/K finite subextensions.
- L/K is **totally ramified** if F/K is totally ramified for all F/K finite subextensions.

Proposition 6.2.2. *Let L/K be unramified. Then L/K is Galois and*

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\kappa_L/\kappa).$$

Proof. Every finite subextension F/K is unramified hence Galois, so L/K is normal and separable, hence L/K is Galois. Moreover, there exists a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\text{res}} & \mathrm{Gal}(\kappa_L/\kappa) \\ {\scriptstyle 6.1.3}\downarrow\wr & & \downarrow{\scriptstyle i} \\ \varprojlim_{F/K \text{ finite},\ F \subseteq L} \mathrm{Gal}(F/K) & \xrightarrow[\sim]{} & \varprojlim_{F/K \text{ finite},\ F \subseteq L} \mathrm{Gal}(\kappa_F/\kappa) \end{array}.$$

By Theorem 5.1.4 and Proposition 6.1.3,

$$\varprojlim_{F/K \text{ finite},\ F \subseteq L} \mathrm{Gal}(\kappa_F/\kappa) \cong \varprojlim_{\ell/\kappa \text{ finite},\ \ell \subseteq \kappa_L} \mathrm{Gal}(\ell/\kappa) \cong \mathrm{Gal}(\kappa_L/\kappa),$$

so i is an isomorphism. □

By example sheet 3, if L_1/K and L_2/K are finite unramified, then L_1L_2/K is unramified. Thus for any L/K, there exists a maximal unramified subextension K_0/K. There is a surjection

$$\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(K_0/K) \cong \mathrm{Gal}(\kappa_L/\kappa),$$

and we write $\mathrm{I}_{L/K}$ for the kernel of res, the **inertia subgroup**. We let $\mathrm{Fr}_{\kappa_L/\kappa} \in \mathrm{Gal}(\kappa_L/\kappa)$ be the Frobenius $x \mapsto x^{|\kappa|}$, and we let $\langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle$ be the subgroup generated by $\mathrm{Fr}_{\kappa_L/\kappa}$.

Definition 6.2.3. Let L/K be Galois. The **Weil group** $\mathrm{W}(L/K)$ is the subgroup of $\mathrm{Gal}(L/K)$ which maps to $\langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle \subseteq \mathrm{Gal}(\kappa_L/\kappa)$, that is $\mathrm{res}^{-1}\left(\langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle\right)$.

Remark. If κ_L/κ is finite $\mathrm{W}(L/K) = \mathrm{Gal}(L/K)$. There exists a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{I}_{L/K} \arrow[r] \arrow[d, phantom, "\cong"] & \mathrm{W}(L/K) \arrow[r] \arrow[d, hook] & \langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathrm{I}_{L/K} \arrow[r] & \mathrm{Gal}(L/K) \arrow[r] & \mathrm{Gal}(\kappa_L/\kappa) \arrow[r] & 0
\end{tikzcd},$$

with exact rows. We endow $\mathrm{W}(L/K)$ with the weakest topology such that $\mathrm{I}_{L/K}$ is an open subgroup of $\mathrm{W}(L/K)$ equipped with its subspace topology as $\mathrm{I}_{L/K} \subseteq \mathrm{Gal}(L/K)$. A warning is if κ_L/κ is infinite, this is not the subspace topology on $\mathrm{W}(L/K) \subseteq \mathrm{Gal}(L/K)$.

Proposition 6.2.4. *Let L/K be a Galois extension.*

1. $\mathrm{W}(L/K)$ *is dense in* $\mathrm{Gal}(L/K)$.
2. *If F/K is a finite subextension of L/K, then* $\mathrm{W}(L/F) = \mathrm{W}(L/K) \cap \mathrm{Gal}(L/F)$.
3. *If F/K is a finite Galois subextension, then* $\mathrm{W}(L/K)/\mathrm{W}(L/F) \cong \mathrm{Gal}(F/K)$.

Proof.

1. $\mathrm{W}(L/K)$ is dense in $\mathrm{Gal}(L/K)$ if and only if for all F/K finite Galois subextensions, $\mathrm{W}(L/K)$ intersects every coset of $\mathrm{Gal}(L/F)$, if and only if for all F/K finite Galois, $\mathrm{W}(L/K) \twoheadrightarrow \mathrm{Gal}(F/K)$. We have a diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{I}_{L/K} \arrow[r] \arrow[d, "a"] & \mathrm{W}(L/K) \arrow[r] \arrow[d, "b"] & \langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & \mathrm{I}_{F/K} \arrow[r] & \mathrm{Gal}(F/K) \arrow[r] & \mathrm{Gal}(\kappa_F/\kappa) \arrow[r] & 0
\end{tikzcd}.$$

   By example sheet 4, a is surjective. Since $\mathrm{Gal}(\kappa_F/\kappa)$ is generated by $\mathrm{Fr}_{\kappa_F/\kappa}$, c is surjective. By a diagram chase, b is surjective.

2. Let F/K be finite. There exists a diagram

$$\begin{tikzcd}
\mathrm{Gal}(L/K) \arrow[r, two heads] & \mathrm{Gal}(\kappa_L/\kappa) & \supset & \langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle \\
\mathrm{Gal}(L/F) \arrow[r, two heads] \arrow[u, hook] & \mathrm{Gal}(\kappa_L/\kappa_F) \arrow[u, hook] & \supset & \langle \mathrm{Fr}_{\kappa_L/\kappa_F} \rangle \arrow[u, hook]
\end{tikzcd}.$$

   Hence for $\sigma \in \mathrm{Gal}(L/F)$, $\sigma \in \mathrm{W}(L/F)$ if and only if $\sigma|_{\kappa_L} \in \langle \mathrm{Fr}_{\kappa_L/\kappa_F} \rangle$, if and only if $\sigma|_{\kappa_L} \in \langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle$ using $\mathrm{Gal}(\kappa_L/\kappa_F) \cap \langle \mathrm{Fr}_{\kappa_L/\kappa} \rangle = \langle \mathrm{Fr}_{\kappa_L/\kappa_F} \rangle$, if and only if $\sigma \in \mathrm{W}(L/K)$.

3. $$\begin{aligned}
\mathrm{W}(L/K)/\mathrm{W}(L/F) &= \mathrm{W}(L/K)/(\mathrm{W}(L/K) \cap \mathrm{Gal}(L/F)) && \text{by } 2 \\
&\cong \mathrm{W}(L/K)\,\mathrm{Gal}(L/F)/\mathrm{Gal}(L/F) \\
&= \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) && \text{by } 1 \\
&\cong \mathrm{Gal}(F/K).
\end{aligned}$$

$\square$

6.3 Statements of local class field theory

Lecture 19 Friday 20/11/20

Let K be a non-archimedean local field.

Definition 6.3.1. An extension L/K is **abelian** if it is Galois and $\mathrm{Gal}(L/K)$ is an abelian group.

Fact. Let L_1/K and L_2/K be abelian.

1. $L_1 L_2/K$ is abelian.
2. If $L_1 \cap L_2 = K$, there is a canonical isomorphism

$$\mathrm{Gal}(L_1 L_2/K) \xrightarrow{\sim} \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

By fact 1, there exists a maximal abelian extension K^{ab} of K.

Example. Let K^{ur} denote the maximal unramified extension of K inside K^{sep}. If $|\kappa| = q$, then

$$K^{\mathrm{ur}} = \bigcup_{m=1}^{\infty} K(\zeta_{q^m-1}), \qquad \kappa_{K^{\mathrm{ur}}} \cong \overline{\mathbb{F}_q}, \qquad \mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right) \cong \widehat{\mathbb{Z}},$$

so K^{ur} is abelian and hence $K^{\mathrm{ur}} \subseteq K^{\mathrm{ab}}$. There exists an exact sequence

$$0 \to \mathrm{I}_{K^{\mathrm{ab}}/K} \to \mathrm{W}\left(K^{\mathrm{ab}}/K\right) \to \mathbb{Z} \to 0.$$

For L/K unramified, let $\mathrm{Fr}_{L/K} \in \mathrm{Gal}(L/K)$ correspond to $\mathrm{Fr}_{\kappa_L/\kappa} \in \mathrm{Gal}(\kappa_L/\kappa)$.

Theorem 6.3.2 (Local Artin reciprocity)**.**

- *There exists a unique topological isomorphism, so an isomorphism of groups and a homeomorphism,*

$$\mathrm{Art}_K : K^\times \to \mathrm{W}\left(K^{\mathrm{ab}}/K\right),$$

  called the ***Artin reciprocity map****, satisfying the following properties.*

  - *For any uniformiser $\pi \in K$,*

$$\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Fr}_{K^{\mathrm{ur}}/K}.$$

  - *For each finite subextension L/K in K^{ab}/K,*

$$\mathrm{Art}_K\left(\mathrm{N}_{L/K}\left(L^\times\right)\right)\big|_L = \mathrm{id}.$$

- *Let L/K be finite abelian. Then Art_K induces an isomorphism*

$$K^\times/\mathrm{N}_{L/K}\left(L^\times\right) \cong \mathrm{W}\left(K^{\mathrm{ab}}/K\right)/\mathrm{W}\left(K^{\mathrm{ab}}/L\right) \cong \mathrm{Gal}(L/K).$$

Remark. $\mathrm{Fr}_{K^{\mathrm{ur}}/K}$ lifts $x \mapsto x^q$ in $\mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right)$. This is the **arithmetic Frobenius**, and $\mathrm{Fr}_{K^{\mathrm{ur}}/K}^{-1}$ is called the **geometric Frobenius**. There is another normalisation of Art_K with

$$\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Fr}_{K^{\mathrm{ur}}/K}^{-1}.$$

Definition 6.3.3. Let L/K be Galois. For $s \in \mathbb{R}_{\geq -1}$ we define

$$\mathrm{G}^s(L/K) = \left\{\sigma \in \mathrm{Gal}(L/K) \mid \forall F/K \text{ finite Galois subextension, } \sigma|_F \in \mathrm{G}^s(F/K)\right\}.$$

By Corollary 5.4.5, $\mathrm{G}^s(L/K)$ is well-defined.

Proposition 6.3.4. *The following are properties of the Artin reciprocity map.*

- *(Existence theorem) For $H \subseteq K^\times$ an open finite index subgroup, there is a finite abelian extension L/K such that $\mathrm{N}_{L/K}(L^\times) = H$. In particular, Art_K induces an inclusion reversing isomorphism of posets*
$$\begin{array}{rcl} \{\text{open finite index subgroups of } K^\times\} & \longleftrightarrow & \{\text{finite abelian extensions } L/K\} \\ H & \longmapsto & \left(K^{\mathrm{ab}}\right)^{\mathrm{Art}_K(H)} \\ \mathrm{N}_{L/K}\left(L^\times\right) & \longleftarrow & L/K \end{array}.$$
- *(Norm functoriality) Let L/K be a finite separable extension. There is a commutative diagram*
$$\begin{tikzcd} L^\times \arrow[r, "\mathrm{Art}_L"] \arrow[d, "\mathrm{N}_{L/K}"'] & \mathrm{W}\left(L^{\mathrm{ab}}/L\right) \arrow[d, "\mathrm{res}"] \\ K^\times \arrow[r, "\mathrm{Art}_K"'] & \mathrm{W}\left(K^{\mathrm{ab}}/K\right) \end{tikzcd}.$$
- *(Compatibility with higher ramification groups) Let $s \in \mathbb{Z}_{\geq 0}$. Then*
$$\mathrm{Art}_K\left(\mathrm{U}_K^{(s)}\right) = \mathrm{G}^s\left(K^{\mathrm{ab}}/K\right).$$

Note that
$$\mathrm{G}^s\left(K^{\mathrm{ab}}/K\right) \subseteq \mathrm{I}_{K^{\mathrm{ab}}/K} \subseteq \mathrm{W}\left(K^{\mathrm{ab}}/K\right), \qquad s \geq 0.$$

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

Recall that
$$\mathbb{Q}_p^{\mathrm{ur}} = \bigcup_{m=1}^\infty \mathbb{Q}_p\left(\zeta_{p^m-1}\right) = \bigcup_{p \nmid m} \mathbb{Q}_p\left(\zeta_m\right).$$

By example sheet 3, $\mathbb{Q}_p\left(\zeta_{p^n}\right)/\mathbb{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$, with $\theta_n : \mathrm{Gal}\left(\mathbb{Q}_p\left(\zeta_{p^n}\right)/\mathbb{Q}_p\right) \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$. For $n \geq m \geq 1$, there is a diagram
$$\begin{tikzcd} \mathrm{Gal}\left(\mathbb{Q}_p\left(\zeta_{p^n}\right)/\mathbb{Q}_p\right) \arrow[r, two heads] \arrow[d, "\theta_n"', "\sim"] & \mathrm{Gal}\left(\mathbb{Q}_p\left(\zeta_{p^m}\right)/\mathbb{Q}_p\right) \arrow[d, "\theta_n", "\sim"'] \\ \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \arrow[r, two heads, "\bmod m"'] & \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times \end{tikzcd}.$$

Set
$$\mathbb{Q}_p\left(\zeta_{p^\infty}\right) = \bigcup_{n=1}^\infty \mathbb{Q}_p\left(\zeta_{p^n}\right).$$

Then $\mathbb{Q}_p\left(\zeta_{p^\infty}\right)/\mathbb{Q}_p$ is Galois and we have
$$\theta : \mathrm{Gal}\left(\mathbb{Q}_p\left(\zeta_{p^\infty}\right)/\mathbb{Q}_p\right) \xrightarrow{\sim} \varprojlim_{n \geq 1} \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \cong \mathbb{Z}_p^\times.$$

We have $\mathbb{Q}_p\left(\zeta_{p^\infty}\right) \cap \mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p$, since $\mathbb{Q}_p\left(\zeta_{p^\infty}\right)$ is totally ramified and $\mathbb{Q}_p^{\mathrm{ur}}$ is unramified. It follows that there is an isomorphism
$$\mathrm{Gal}\left(\mathbb{Q}_p\left(\zeta_{p^\infty}\right)\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p\right) \cong \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

Theorem 6.4.1 (Local Kronecker-Weber)**.**
$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{ur}}\mathbb{Q}_p\left(\zeta_{p^\infty}\right).$$

The Artin map can now be constructed as follows. We have an isomorphism

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z}_p^\times & \longrightarrow & \mathbb{Q}_p^\times \\ (n, u) & \longmapsto & p^n u \end{array}.$$

Then

$$\mathrm{Art}_{\mathbb{Q}_p}(p^n u) = \left(\mathrm{Fr}^n_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}, \theta^{-1}(u)\right) \in \mathrm{Gal}\left(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p\right) \times \mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p\right).$$

Remark. The definition of $\mathrm{Art}_{\mathbb{Q}_p}$ involves the choice of a totally ramified $\mathbb{Q}_p(\zeta_{p^\infty})$, and there is no maximal totally ramified extension of $\mathbb{Q}_p$, such as by example sheet 3 question 6(b), and the choice of a uniformiser p, which determines the isomorphism $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$. These choices are related, since the choices cancel out so $\mathrm{Art}_{\mathbb{Q}_p}$ is in fact canonical.

Thus $\mathrm{Art}_{\mathbb{Q}_p}$ was constructed by constructing a totally ramified extension $\mathbb{Q}_p(\zeta_{p^n})$ with

$$\theta_n : \mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p\right) \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathcal{O}_{\mathbb{Q}_p}^\times/\mathrm{U}_{\mathbb{Q}_p}^{(n)}.$$

In general, let K be a local field, and let π be a uniformiser of K. We construct for $n \geq 1$ a totally ramified Galois extension $K_{\pi,n}/K$ satisfying

1. $K \subseteq K_{\pi,1} \subseteq K_{\pi,2} \subseteq \dots$,
2. for $n \geq m \geq 1$ there exists a diagram

$$\begin{tikzcd} \mathrm{Gal}(K_{\pi,n}/K) \arrow[r, two heads] \arrow[d, "\psi_n"', "\sim"] & \mathrm{Gal}(K_{\pi,m}/K) \arrow[d, "\sim"', "\psi_m"] \\ \mathcal{O}_K^\times/\mathrm{U}_K^{(n)} \arrow[r, two heads, "\bmod m"'] & \mathcal{O}_K^\times/\mathrm{U}_K^{(m)} \end{tikzcd},$$

3. setting $K_{\pi,\infty} = \bigcup_{n=1}^\infty K_{\pi,n}$, we have
$$K^{\mathrm{ab}} = K^{\mathrm{ur}} K_{\pi,\infty}.$$

Since $\mathcal{O}_K^\times \cong \varprojlim_n \mathcal{O}_K^\times/\mathrm{U}_K^{(n)}$, by 2, there exists an isomorphism

$$\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathcal{O}_K^\times.$$

Can define Art_K by

$$\begin{array}{ccc} K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right) \\ \pi^n u \leftrightarrow (n, u) & \longmapsto & \left(\mathrm{Fr}^n_{K^{\mathrm{ur}}/K}, \psi^{-1}(u)\right) \end{array}.$$

Thus

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}_p^{\mathrm{ab}} \arrow[dl, no head] \arrow[dr, no head] & & & & K^{\mathrm{ab}} \arrow[dl, no head] \arrow[dr, no head] & \\ \mathbb{Q}_p^{\mathrm{ur}} \arrow[dr, no head, "\widehat{\mathbb{Z}}"'] & & \mathbb{Q}_p(\zeta_{p^\infty}) \arrow[dl, no head, "\mathbb{Z}_p^\times"] & \Longrightarrow & K^{\mathrm{ur}} \arrow[dr, no head, "\widehat{\mathbb{Z}}"'] & & K_{\pi,\infty} \arrow[dl, no head, "\mathcal{O}_K^\times"] \\ & \mathbb{Q}_p & & & & K & \end{tikzcd}.$$

The goal is to construct $K_{\pi,n}$.

7 Lubin-Tate theory

7.1 Formal group laws

Lecture 20
Monday
23/11/20

If R is a ring,

$$R[[X_1, \dots, X_n]] = \left\{ \sum_{k_1, \dots, k_n \geq 0} a_{k_1 \dots k_n} X_1^{k_1} \dots X_n^{k_n} \;\middle|\; a_{k_1 \dots k_n} \in R \right\}$$

is the ring of formal power series in n variables over R.

Definition 7.1.1. A **one-dimensional commutative formal group law** over R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying

- $F(X, Y) \equiv X + Y \mod \deg 2$,
- associativity $F(X, F(Y, Z)) = F(F(X, Y), Z)$, and
- commutativity $F(X, Y) = F(Y, X)$.

Example.

- $\widehat{\mathbb{G}_{\mathrm{a}}}(X, Y) = X + Y$ is the **formal additive group**.
- $\widehat{\mathbb{G}_{\mathrm{m}}}(X, Y) = X + Y + XY$ is the **formal multiplicative group**.

Lemma 7.1.2. *Let R be a ring, and let F be a formal group law over R. Then*

- *$F(X, 0) = X$ and $F(0, Y) = Y$, and*
- *there exists a unique power series $\iota(X) \in XR[[X]]$ such that $F(X, \iota(X)) = 0$.*

Proof. Example sheet 4. ◻

Let K be a complete non-archimedean valued field, and F a formal group law over $\mathcal{O}_K$. Then $F(x, y)$ converges for all $x, y \in \mathfrak{m}$ to an element in $\mathfrak{m}$. Defining $x \cdot_F y = F(x, y)$, this turns $(\mathfrak{m}, \cdot_F)$ into a commutative group.

Example. If $\widehat{\mathbb{G}_{\mathrm{m}}}$ is over $\mathbb{Z}_p$, then $x \cdot_{\widehat{\mathbb{G}_{\mathrm{m}}}} y = x + y + xy$, and there is an isomorphism

$$\begin{array}{ccc} \left(p\mathbb{Z}_p, \cdot_{\widehat{\mathbb{G}_{\mathrm{m}}}}\right) & \longrightarrow & (1 + p\mathbb{Z}_p, \times) \\ x & \longmapsto & 1 + x \end{array}.$$

Definition 7.1.3. Let F and G be formal group laws over R. A **homomorphism** $f : F \to G$ is an element $f(X) \in XR[[X]]$ such that

$$f(F(X, Y)) = G(f(X), f(Y)).$$

We define $\operatorname{End}_R F$ to be the set of homomorphisms $f : F \to F$.

Lemma 7.1.4. *$\operatorname{End}_R F$ is a ring with addition given by $(f +_F g)(X) = F(f(X), g(X))$ and multiplication is given by composition.*

Proof. Let $f, g \in \operatorname{End}_R F$. Using associativity and commutativity,

$$\begin{aligned} (f +_F g)(F(X, Y)) &= F(f(F(X, Y)), g(F(X, Y))) = F(F(f(X), f(Y)), F(g(X), g(Y))) \\ &= F(F(f(X), g(X)), F(f(Y), g(Y))) = F((f +_F g)(X), (f +_F g)(Y)), \end{aligned}$$

so $f +_F g \in \operatorname{End}_R F$, and $f \circ g \circ F = f \circ F \circ g = F \circ f \circ g$, so $f \circ g \in \operatorname{End}_R F$. The ring axioms are an exercise. [2] ◻

[2] Exercise

7.2 Lubin-Tate formal group laws

Let K be a non-archimedean local field, let π be a uniformiser, and let $|\kappa| = q$.

Definition 7.2.1. A **formal $\mathcal{O}_K$-module** is a formal group law $F(X,Y) \in \mathcal{O}_K[[X,Y]]$ together with a ring homomorphism $[\cdot]_F : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K} F$ such that

$$[a]_F(X) \equiv aX \mod X^2, \qquad a \in \mathcal{O}_K.$$

Definition 7.2.2. A **Lubin-Tate series** for π is a power series $f(X) \in \mathcal{O}_K[[X]]$ such that

- $f(X) \equiv \pi X \mod X^2$, and
- $f(X) \equiv X^q \mod \pi$.

Example. If $K = \mathbb{Q}_p$, then $f(X) = (X+1)^p - 1$ is a Lubin-Tate series for p.

Theorem 7.2.3. *Let $f(X)$ be a Lubin-Tate series for π.*

1. *There exists a unique formal group law F_f over $\mathcal{O}_K$ such that $f \in \mathrm{End}_{\mathcal{O}_K} \mathrm{F}_f$.*
2. *There is a ring homomorphism $[\cdot]_{\mathrm{F}_f} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K} \mathrm{F}_f$ satisfying $[\pi]_{\mathrm{F}_f}(X) = f(X)$ and which endows F_f with the structure of a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$.*
3. *If $g(X)$ is another Lubin-Tate series, $\mathrm{F}_f \cong \mathrm{F}_g$ as formal $\mathcal{O}_K$-modules. Here an isomorphism $\theta : F \to G$ of formal $\mathcal{O}_K$-modules is an isomorphism of formal groups such that $\theta \circ [a]_F = [a]_G \circ \theta$ for all $a \in \mathcal{O}_K$.*

Then F_f is the **Lubin-Tate formal group law** for π, which only depends on π up to isomorphism.

Example. If $K = \mathbb{Q}_p$ and $f(X) = (X+1)^p - 1$, then the Lubin-Tate formal group law F_f associated to f is $\widehat{\mathbb{G}_\mathrm{m}}$. To see this it suffices to show $f \circ \widehat{\mathbb{G}_\mathrm{m}} = \widehat{\mathbb{G}_\mathrm{m}} \circ f$, and

$$f\left(\widehat{\mathbb{G}_\mathrm{m}}(X,Y)\right) = (1+X)^p(1+Y)^p - 1 = \widehat{\mathbb{G}_\mathrm{m}}(f(X), f(Y)).$$

Lemma 7.2.4 (Key lemma)**.** *Let $f(X)$ and $g(X)$ be Lubin-Tate series for π, and let $L(X_1, \dots, X_n) = \sum_{i=1}^n a_i X_i$ for $a_i \in \mathcal{O}_K$. There is a unique power series $F(X_1, \dots, X_n) \in \mathcal{O}_K[[X_1, \dots, X_n]]$ such that*

1. *$F(X_1, \dots, X_n) \equiv L(X_1, \dots, X_n) \mod \deg 2$,*
2. *$f(F(X_1, \dots, X_n)) = F(g(X_1), \dots, g(X_n))$.*

Proof. We show by induction there are unique polynomials $F_m \in \mathcal{O}_K[X_1, \dots, X_n]$ of total degree at most m such that

1′. $f(F_m(X_1, \dots, X_n)) \equiv F_m(g(X_1), \dots, g(X_n)) \mod \deg(m+1)$,

2′. $F_m(X_1, \dots, X_n) \equiv L(X_1, \dots, X_n) \mod \deg 2$, and

3′. $F_m \equiv F_{m+1} \mod \deg(m+1)$.

For $m = 1$, take $F_1 = L$. Then

$$f(F_1(X_1, \dots, X_n)) \equiv \pi L(X_1, \dots, X_n) \equiv F_1(g(X_1), \dots, g(X_n)) \mod \deg 2.$$

Suppose F_m are constructed for $m \ge 1$. Set $F_{m+1} = F_m + h$ where $h \in \mathcal{O}_K[X_1, \dots, X_n]$ is homogeneous of degree $m+1$. We have

$$f \circ (F_m + h) \equiv f \circ F_m + \pi h \mod \deg(m+2),$$

since $f(X) \equiv \pi X \mod X^2$, such as using $f(X+Y) = f(X) + f'(X)Y + \dots$. Similarly,

$$(F_m + h) \circ g \equiv F_m \circ g + h(\pi X_1, \dots, \pi X_n) \equiv F_m \circ g + \pi^{m+1} h \mod \deg(m+2),$$

since $g(X) \equiv \pi X \mod X^2$. Thus 1′, 2′, and 3′ are satisfied for h if and only if

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

But $f(X) \equiv g(X) \equiv X^q \mod \pi$. Thus

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

Thus $f \circ F_m - F_m \circ g \in \pi \mathcal{O}_K[X_1, \dots, X_n]$. Let $r(X_1, \dots, X_n)$ be the degree $m+1$ terms in $f \circ F_m - F_m \circ g$. Then set

$$h = \frac{1}{\pi(\pi^m - 1)} r \in \mathcal{O}_K[X_1, \dots, X_n],$$

so that F_{m+1} satisfies $1'$, $2'$, and $3'$. Unique since h is determined by property $1'$. Set $F = \lim_{m \to \infty} F_m$, then $F(X_1, \dots, X_n)$ satisfies 1 and 2. Uniqueness of F follows from uniqueness of F_m. □

Lecture 21 Wednesday 25/11/20

Proof of Theorem 7.2.3.

1. By Lemma 7.2.4, there exists a unique $\mathrm{F}_f(X, Y) \in \mathcal{O}_K[[X, Y]]$ such that
   - $\mathrm{F}_f(X, Y) \equiv X + Y \mod \deg 2$, and
   - $f(\mathrm{F}_f(X, Y)) = \mathrm{F}_f(f(X), f(Y))$.

   Then F_f is a formal group law.
   - Associativity, since

     $$\mathrm{F}_f(X, \mathrm{F}_f(Y, Z)) \equiv X + Y + Z \equiv \mathrm{F}_f(\mathrm{F}_f(X, Y), Z) \mod \deg 2,$$

     and

     $$f(\mathrm{F}_f(X, \mathrm{F}_f(Y, Z))) = \mathrm{F}_f(f(X), f(\mathrm{F}_f(Y, Z))) = \mathrm{F}_f(f(X), \mathrm{F}_f(f(Y), f(Z))),$$

     and similarly

     $$f(\mathrm{F}_f(\mathrm{F}_f(X, Y), Z)) = \mathrm{F}_f(\mathrm{F}_f(f(X), f(Y)), f(Z)),$$

     thus $\mathrm{F}_f(X, \mathrm{F}_f(Y, Z)) = \mathrm{F}_f(\mathrm{F}_f(X, Y), Z)$ by uniqueness in Lemma 7.2.4.
   - Commutativity is similar, by uniqueness.
   - $F(X, 0) = X$ and $F(0, Y) = Y$, by uniqueness.

2. By Lemma 7.2.4, for $a \in \mathcal{O}_K$, there exists $[a]_{\mathrm{F}_f} \in \mathcal{O}_K[[X]]$ such that $[a]_{\mathrm{F}_f}(X) \equiv aX \mod X^2$ and $f \circ [a]_{\mathrm{F}_f} = [a]_{\mathrm{F}_f} \circ f$. Then,

   $$[a]_{F_f} \circ \mathrm{F}_f \equiv aX + aY \equiv \mathrm{F}_f \circ [a]_{\mathrm{F}_f} \mod \deg 2,$$

   and

   $$f \circ [a]_{\mathrm{F}_f} \circ \mathrm{F}_f = [a]_{\mathrm{F}_f} \circ f \circ \mathrm{F}_f = [a]_{\mathrm{F}_f} \circ \mathrm{F}_f \circ f, \qquad f \circ \mathrm{F}_f \circ [a]_{\mathrm{F}_f} = \mathrm{F}_f \circ f \circ [a]_{\mathrm{F}_f} = \mathrm{F}_f \circ [a]_{\mathrm{F}_f} \circ f,$$

   so $[a]_{\mathrm{F}_f} \circ \mathrm{F}_f = \mathrm{F}_f \circ [a]_{\mathrm{F}_f}$, that is $[a]_{\mathrm{F}_f} \in \mathrm{End}_{\mathcal{O}_K} \mathrm{F}_f$. We have
   - the map $[\cdot]_{\mathrm{F}_f} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K} \mathrm{F}_f$ is a ring homomorphism, by uniqueness,
   - F_f is a formal $\mathcal{O}_K$-module, and
   - $[\pi]_{\mathrm{F}_f} = f$, by uniqueness.

3. If g is another Lubin-Tate series for π, let $\theta \in \mathcal{O}_K[[X]]$ be the unique power series such that $\theta(f(X)) = g(\theta(X))$ and $\theta(X) \equiv X \mod X^2$. Then $\theta \circ \mathrm{F}_f = \mathrm{F}_g \circ \theta$, by uniqueness. Thus $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(\mathrm{F}_f, \mathrm{F}_g)$. Reversing the roles of f and g, obtain $\theta^{-1} \in \mathcal{O}_K[[X]]$ such that $\theta^{-1} \in \mathrm{Hom}_{\mathcal{O}_K}(\mathrm{F}_g, \mathrm{F}_f)$ with $\theta^{-1}(g(X)) = f\left(\theta^{-1}(X)\right)$. Then $\theta^{-1}(\theta(X)) = X$ and $\theta\left(\theta^{-1}(X)\right) = X$, by uniqueness, so θ is an isomorphism. By uniqueness, $\theta\left([a]_{\mathrm{F}_f}(X)\right) = [a]_{\mathrm{F}_g}(\theta(X))$ for all $a \in \mathcal{O}_K$ and hence θ is an isomorphism of formal $\mathcal{O}_K$-modules.

□

7.3 Lubin-Tate extensions

Let $\overline{K}$ be the algebraic closure of K, and let $\overline{\mathfrak{m}} \subseteq \mathcal{O}_{\overline{K}}$ be the maximal ideal.

Lemma 7.3.1. *Let F be a formal $\mathcal{O}_K$-module. Then $\overline{\mathfrak{m}}$ becomes a genuine $\mathcal{O}_K$-module with operations*

$$x +_F y = F(x, y), \qquad a \cdot_F x = [a]_F(x), \qquad x, y \in \overline{\mathfrak{m}}, \qquad a \in \mathcal{O}_K.$$

Proof. Note that $\overline{K}$ is not complete. If $x \in \overline{\mathfrak{m}}$, then $x \in \mathfrak{m}_L$ for some L/K finite. Since $[a]_F \in \mathcal{O}_K[[X]]$, $[a]_F(x)$ converges in L, and since $\mathfrak{m}_L$ is closed, $[a]_F(x) \in \mathfrak{m}_L \subseteq \overline{\mathfrak{m}}$. Similarly $x +_F y \in \overline{\mathfrak{m}}$. The module structure follows from definitions. ☐

Definition 7.3.2. Let f be a Lubin-Tate series for π and F_f the associated formal $\mathcal{O}_K$-module. The **π^n-torsion group** is defined to be

$$\mu_{f,n} = \left\{x \in \overline{\mathfrak{m}} \mid \pi^n \cdot_{\mathrm{F}_f} x = 0\right\} = \{x \in \overline{\mathfrak{m}} \mid f_n(x) = (f \circ \dots \circ f)(x) = 0\}.$$

Fact.

- $\mu_{f,n}$ is an $\mathcal{O}_K$-module.
- $\mu_{f,n} \subseteq \mu_{f,n+1}$ for all n.

Example. If $K = \mathbb{Q}_p$ and $f(X) = (X+1)^p - 1$ is a Lubin-Tate series for p, then

$$[p^n]_{\mathrm{F}_f}(X) = (f \circ \dots \circ f)(X) = (X+1)^{p^n} - 1,$$

such as by induction on n. Thus

$$\mu_{f,n} = \left\{\zeta_{p^n}^i - 1 \mid i = 0, \dots, p^n - 1\right\}.$$

Now let $f(X)$ be the Lubin-Tate series $f(X) = \pi X + X^q$. Then

$$f_n(X) = f(f_{n-1}(X)) = f_{n-1}(X)\left(\pi + f_{n-1}(X)^{q-1}\right).$$

Set

$$\mathrm{h}_n(X) = \frac{f_n(X)}{f_{n-1}(X)} = \pi + f_{n-1}(X)^{q-1}.$$

Proposition 7.3.3.

1. *$\mathrm{h}_n(X)$ is a separable Eisenstein polynomial of degree $q^{n-1}(q-1)$.*
2. *$\mu_{f,n}$ is a free $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module of rank one.*

Proof.

1. $\mathrm{h}_1(X) = \pi + X^{q-1}$. Clear that $\mathrm{h}_n(X)$ is monic of degree $q^{n-1}(q-1)$. Since $f(X) \equiv X^q \mod \pi$, $f_{n-1}(X)^{q-1} \equiv X^{q^{n-1}(q-1)} \mod \pi$. Since $f_{n-1}(X)$ has zero constant term $\mathrm{h}_n(X) = \pi + f_{n-1}(X)^{q-1}$ has constant term π. Thus $\mathrm{h}_n(X)$ is Eisenstein. Since $\mathrm{h}_n(X)$ is irreducible, $\mathrm{h}_n(X)$ is separable if $\operatorname{ch} K = 0$ or if $\operatorname{ch} K = p$ and $\mathrm{h}_n'(X) \neq 0$. Assume $\operatorname{ch} K = p$ and induct on n.
   - $\mathrm{h}_1(X) = \pi + X^{q-1}$ is separable.
   - Suppose $\mathrm{h}_{n-1}(X), \dots, \mathrm{h}_1(X)$ are separable. Then $f_{n-1}(X) = \mathrm{h}_{n-1}(X) \dots \mathrm{h}_1(X) X$ is separable, as a product of irreducible polynomials of different degrees. Since $\mathrm{h}_n(X) = \pi + f_{n-1}(X)^{q-1}$, $\mathrm{h}_n'(X) = (q-1) f_{n-1}'(X) f_{n-1}(X)^{q-2} \neq 0$, so $\mathrm{h}_n(X)$ is separable.
2. Let α be a root of $\mathrm{h}_n(X)$. Since $\mathrm{h}_n(X)$ and $f_{n-1}(X)$ are coprime, $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$. Then the map

$$\begin{array}{cccc} \widetilde{\phi} & : & \mathcal{O}_K & \longrightarrow & \mu_{f,n} \\ & & a & \longmapsto & a \cdot_{\mathrm{F}_f} \alpha \end{array}$$

   is an $\mathcal{O}_K$-module homomorphism with $\pi^n\mathcal{O}_K \subseteq \ker \widetilde{\phi}$. As $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$, $\pi^{n-1} \cdot_{\mathrm{F}_f} \alpha \neq 0$ thus $\pi^n\mathcal{O}_K = \ker \widetilde{\phi}$. Thus $\widetilde{\phi}$ induces an injection $\phi : \mathcal{O}_K/\pi^n\mathcal{O}_K \to \mu_{f,n}$. Since $f_n(X)$ is separable, $|\mu_{f,n}| = \deg f_n(X) = q^n = |\mathcal{O}_K/\pi^n\mathcal{O}_K|$. Thus ϕ is an isomorphism by counting.

☐

Since $x \in \mu_{f,n}$ is a root of $f_n(X)$, x is algebraic.

Proposition 7.3.4. *Let g be another Lubin-Tate series for π. Then*

- $\mu_{f,n} \cong \mu_{g,n}$ *as $\mathcal{O}_K$-modules, and*
- $K(\mu_{f,n}) = K(\mu_{g,n})$.

Proof. Let $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(\mathrm{F}_f, \mathrm{F}_g)$ be an isomorphism of formal $\mathcal{O}_K$-modules. Then θ induces an isomorphism $\theta : \left(\overline{\mathfrak{m}}, +_{\mathrm{F}_f}\right) \xrightarrow{\sim} \left(\overline{\mathfrak{m}}, +_{\mathrm{F}_g}\right)$ of $\mathcal{O}_K$-modules, and hence $\mu_{f,n} \cong \mu_{g,n}$. Since $\mu_{f,n}$ is algebraic, $K(\mu_{f,n})/K$ is finite, hence complete. Since $\theta \in \mathcal{O}_K[[X]]$, for $x \in \mu_{f,n}$, $\theta(x) \in K(\mu_{f,n})$, so $K(\mu_{g,n}) \subseteq K(\mu_{f,n})$. Thus $K(\mu_{g,n})/K$ is finite. Applying the same argument to θ^{-1} gives $K(\mu_{f,n}) \subseteq K(\mu_{g,n})$, so $K(\mu_{f,n}) = K(\mu_{g,n})$. ☐

Definition 7.3.5. $K_{\pi,n} = K(\mu_{f,n})$ is the **Lubin-Tate extension** of degree n associated to π.

Remark.

- $K_{\pi,n}$ does not depend on the Lubin-Tate series f by Proposition 7.3.4.
- $K_{\pi,n} \subseteq K_{\pi,n+1}$.

Lecture 22 Friday 27/11/20

Theorem 7.3.6.

1. *$K_{\pi,n}$ is a totally ramified Galois extension of degree $q^{n-1}(q-1)$.*
2. *There are isomorphisms*

$$\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\sim} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times/\mathrm{U}_K^{(n)},$$

characterised by

$$\psi_n(\sigma) \cdot_{\mathrm{F}_f} x = \sigma(x), \qquad x \in \mu_{f,n}, \qquad \sigma \in \mathrm{Gal}(K_{\pi,n}/K). \tag{6}$$

Proof.

1. By Proposition 7.3.4, we may choose $f(X) = \pi X + X^q$. Let α be a root of $\mathrm{h}_n(X) = f_n(X)/f_{n-1}(X)$. We show that $K(\alpha) = K(\mu_{f,n}) = K_{\pi,n}$. By Proposition 7.3.3, every element x of $\mu_{f,n}$ is of the form $a \cdot_{\mathrm{F}_f} \alpha$ for some $a \in \mathcal{O}_K$, since $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$. Since $K(\alpha)$ is complete and $[a]_{\mathrm{F}_f}(X) \in \mathcal{O}_K[[X]]$, $x = [a]_{\mathrm{F}_f}(\alpha) \in K(\alpha)$, so $K(\alpha) = K(\mu_{f,n})$. Since $\mathrm{h}_n(X)$ is Eisenstein of degree $q^{n-1}(q-1)$, by Proposition 7.3.3, $K(\alpha)/K$ is totally ramified of degree $q^{n-1}(q-1)$, by Theorem 5.1.8. This is Galois since $K(\alpha) = K(\mu_{f,n})$ is the splitting field of f_n.

2. Let $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$. We show that $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}\mu_{f,n}$. Note that σ preserves $\mu_{f,n}$, and σ acts continuously on $K(\mu_{f,n})$. Since $\mathrm{F}_f(X,Y) \in \mathcal{O}_K[[X,Y]]$ and $[a]_{\mathrm{F}_f} \in \mathcal{O}_K[[X]]$ for all $a \in \mathcal{O}_K$, we have $\sigma\left(x +_{\mathrm{F}_f} y\right) = \sigma(x) +_{\mathrm{F}_f} \sigma(y)$ for all $x, y \in \mu_{f,n}$ and $\sigma\left(a \cdot_{\mathrm{F}_f} x\right) = a \cdot_{\mathrm{F}_f} \sigma(x)$ for all $x \in \mu_{f,n}$ and $a \in \mathcal{O}_K$, by continuity of σ. Thus $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}\mu_{f,n}$. This induces a group homomorphism $\mathrm{Gal}(K_{\pi,n}/K) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}\mu_{f,n}$, injective since $K_{\pi,n} = K(\mu_{f,n})$. Since $\mu_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$,

$$\mathrm{Aut}_{\mathcal{O}_K}\mu_{f,n} \cong \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{O}_K/\pi^n\mathcal{O}_K) \cong (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times,$$

canonically. Obtain $\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \hookrightarrow (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ defined by $\psi_n(\sigma) \in (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ is the unique element such that $\psi_n(\sigma) \cdot_{\mathrm{F}_f} x = \sigma(x)$ for all $x \in \mu_{f,n}$. Then $[K_{\pi,n} : K] = q^{n-1}(q-1) = \left|(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times\right|$, so ψ_n is surjective by counting. Let g be another Lubin-Tate series and $\psi'_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\sim} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$. By Theorem 7.2.3, there exists $\theta : \mathrm{F}_f \to \mathrm{F}_g$ an isomorphism of formal $\mathcal{O}_K$-modules. This induces an isomorphism $\theta : \mu_{f,n} \xrightarrow{\sim} \mu_{g,n}$ of $\mathcal{O}_K$-modules. Since $\theta \in \mathcal{O}_K[[X]]$, $\theta(\sigma(x)) = \sigma(\theta(x))$ for all $x \in \mu_{f,n}$ and $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$, so $\theta\left(\psi_n(\sigma) \cdot_{\mathrm{F}_f} x\right) = \psi'_n(\sigma) \cdot_{\mathrm{F}_g} \theta(x)$. Thus $\psi_n(\sigma) \cdot_{\mathrm{F}_g} \theta(x) = \psi'_n(\sigma) \cdot_{\mathrm{F}_g} \theta(x)$, so $\psi_n(\sigma) = \psi'_n(\sigma)$.

☐

Define

$$K_{\pi,\infty}=\bigcup_{n=1}^{\infty}K_{\pi,n}.$$

Corollary 7.3.7. *There is an isomorphism*

$$\psi:\mathrm{Gal}\left(K_{\pi,\infty}/K\right)\cong\mathcal{O}_K^{\times}.$$

Proof. By (6), there exists a commutative diagram

$$\begin{array}{ccc}\mathrm{Gal}\left(K_{\pi,n+1}/K\right) & \xrightarrow[\sim]{\psi_{n+1}} & \mathcal{O}_K^{\times}/\mathrm{U}_K^{(n+1)} \\ \downarrow & & \downarrow \text{mod } n \\ \mathrm{Gal}\left(K_{\pi,n}/K\right) & \xrightarrow[\psi_n]{\sim} & \mathcal{O}_K^{\times}/\mathrm{U}_K^{(n)}\end{array},$$

so $\mathrm{Gal}\left(K_{\pi,\infty}/K\right)\cong\varprojlim_n\mathcal{O}_K^{\times}/\mathrm{U}_K^{(n)}\cong\mathcal{O}_K^{\times}$. ☐

7.4 The Artin map

Theorem 7.4.1 (Generalised Kronecker-Weber theorem)**.**

$$K^{\mathrm{ab}}=K^{\mathrm{ur}}K_{\pi,\infty}.$$

Example. If $K=\mathbb{Q}_p$ and $f(X)=(X+1)^p-1$, then $\mu_{f,n}=\left\{\zeta_{p^n}^i-1 \mid i=0,\dots,p^n-1\right\}$. Thus Theorem 7.4.1 says

$$\mathbb{Q}_p^{\mathrm{ab}}=\mathbb{Q}_p^{\mathrm{ur}}\mathbb{Q}_p\left(\zeta_{p^\infty}\right)=\mathbb{Q}_p^{\mathrm{ur}}\bigcup_{n=1}^{\infty}\mathbb{Q}_p\left(\zeta_n\right),$$

which is Theorem 6.4.1.

Note $K_{\pi,\infty}\cap K^{\mathrm{ur}}=K$, since $K_{\pi,\infty}$ is totally ramified and K^{ur} is unramified, so

$$\mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)\cong\mathrm{Gal}\left(K^{\mathrm{ur}}/K\right)\times\mathrm{Gal}\left(K_{\pi,\infty}/K\right).$$

Define Art_K by the commutative diagram

$$\begin{array}{ccccc}\pi^n u & & K^{\times} & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right) \\ \updownarrow & & \wr\wr & & \wr\wr \\ (n,u) & & \mathbb{Z}\times\mathcal{O}_K^{\times} & \longrightarrow & \mathrm{Gal}\left(K^{\mathrm{ur}}/K\right)\times\mathrm{Gal}\left(K_{\pi,\infty}/K\right) \\ & & (n,u) & \longmapsto & \left(\mathrm{Fr}_{K^{\mathrm{ur}}/K}^n,\psi^{-1}(u)\right)\end{array}.$$

The image of Art_K lands in $\mathrm{W}\left(K^{\mathrm{ab}}/K\right)$, so $\mathrm{Art}_K:K^{\times}\xrightarrow{\sim}\mathrm{W}\left(K^{\mathrm{ab}}/K\right)$.

Remark. Can show Art_K is independent of the choice of uniformiser π. Proof omitted.

Notation. Let L/K be possibly infinite. Write

$$\mathrm{N}(L/K)=\bigcap_{F/K \text{ finite},\ F\subseteq L}\mathrm{N}_{F/K}\left(F^{\times}\right)\subseteq K^{\times}.$$

Proposition 7.4.2. *Let $x\in K$ with $\mathrm{v}_K(x)>0$, and $\sigma\in\mathrm{Gal}\left(K^{\mathrm{sep}}/K\right)$ such that $\sigma|_{K^{\mathrm{ab}}}=\mathrm{Art}_K(x)$. Set $L=\left(K^{\mathrm{sep}}\right)^{\sigma}$. Then $\mathrm{N}(L/K)=\langle x\rangle$.*

Proof. Omit. Can be proved using Coleman operators in Patrick Allen's notes on non-archimedean local fields. ☐

Theorem 7.4.3 (Norm functoriality)**.** *Let L/K be a finite separable extension. There exists a commutative diagram*

$$\begin{array}{ccc} L^\times & \xrightarrow{\mathrm{Art}_L} & \mathrm{W}\left(L^{\mathrm{ab}}/L\right) \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \sigma\mapsto\sigma|_{K^{\mathrm{ab}}}} \\ K^\times & \xrightarrow[\mathrm{Art}_K]{} & \mathrm{W}\left(K^{\mathrm{ab}}/K\right) \end{array}.$$

Proof. Since the set of uniformisers in $L^\times$ generate $L^\times$, it suffices to show $\mathrm{Art}_L(\pi_L)|_{K^{\mathrm{ab}}} = \mathrm{Art}_K\left(\mathrm{N}_{L/K}(\pi_L)\right)$ where π_L is a uniformiser in L. Let $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/L)$ be a lift of $\mathrm{Art}_L(\pi_L)$ and then $K_\sigma = (K^{\mathrm{sep}})^\sigma$. Let $x = \mathrm{Art}_K^{-1}(\mathrm{Art}_L(\pi_L)|_{K^{\mathrm{ab}}}) \in K^\times$. Need to show $x = \mathrm{N}_{L/K}(\pi_L)$. Then by Proposition 7.4.2, we have $\mathrm{N}(K_\sigma/L) = \langle\pi_L\rangle \subseteq L^\times$ and $\mathrm{N}(K_\sigma/K) = \langle x\rangle \subseteq K^\times$. Thus

$$\left\langle \mathrm{N}_{L/K}(\pi_L)\right\rangle = \mathrm{N}_{L/K}(\langle\pi_L\rangle) = \mathrm{N}_{L/K}(\mathrm{N}(K_\sigma/L)) = \mathrm{N}(K_\sigma/K) = \langle x\rangle \subseteq K^\times.$$

Thus $\mathrm{N}_{L/K}(\pi_L) = x^{\pm 1}$. It suffices to show $\mathrm{v}_K(x) > 0$. Since $\mathrm{Art}_L(\pi_L)|_{L^{\mathrm{ur}}} = \mathrm{Fr}_{L^{\mathrm{ur}}/L}$, $\mathrm{Art}_L(\pi_L)|_{K^{\mathrm{ur}}} = \mathrm{Fr}_{K^{\mathrm{ur}}/K}^{\mathrm{f}_{L/K}}$, [3] so $\mathrm{v}_K(x) > 0$ by definition of Art_K. ☐

Corollary 7.4.4. *Let L/K be finite abelian. Then Art_K induces an isomorphism*

$$K^\times/\mathrm{N}_{L/K}\left(L^\times\right) \cong \mathrm{Gal}(L/K).$$

Proof. Since L/K is abelian, $L^{\mathrm{ab}} = K^{\mathrm{ab}}$. By Theorem 7.4.3 and Proposition 6.2.4.3,

$$K^\times/\mathrm{N}_{L/K}\left(L^\times\right) \cong \mathrm{W}\left(K^{\mathrm{ab}}/K\right)/\mathrm{W}\left(K^{\mathrm{ab}}/L\right) \cong \mathrm{Gal}(L/K).$$

☐

7.5 Proof of generalised local Kronecker-Weber theorem

Lecture 23 Monday 30/11/20

Proposition 7.5.1. *Let $K_{\pi,n}$ denote the Lubin-Tate extension of degree n associated to π. The isomorphism*

$$\psi_n : \mathrm{G} = \mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times/\mathrm{U}_K^{(n)}$$

induces isomorphisms

$$\mathrm{G}_s \cong \begin{cases} \mathrm{U}_K^{(0)}/\mathrm{U}_K^{(n)} & s \le 0 \\ \mathrm{U}_K^{(k)}/\mathrm{U}_K^{(n)} & q^{k-1}-1 < s \le q^k - 1,\ 1 \le k \le n-1 \\ \{1\} & s > q^{n-1}-1 \end{cases}.$$

Proof. If $s \le 0$, then $\mathrm{G}_s = \mathrm{G}_{-1}$ since $K_{\pi,n}/K$ is totally ramified. Let v_n be the normalised valuation on $K_{\pi,n}$. Recall that

$$\begin{array}{cccc} \mathrm{i}_{K_{\pi,n}/K} & : & \mathrm{G} & \longrightarrow & \mathbb{Z}\cup\{\infty\} \\ & & \sigma & \longmapsto & \max\{i \in \mathbb{Z} \mid \sigma \in \mathrm{G}_{i-1}\} \end{array}.$$

Let $f(X) = \pi X + X^q$ and $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$. Then α is a uniformiser in $\mathcal{O}_{K_{\pi,n}}$ and $\mathcal{O}_{K_{\pi,n}} = \mathcal{O}_K[\alpha]$, so $\mathrm{i}_{K_{\pi,n}/K}(\sigma) = \mathrm{v}_n(\sigma(\alpha) - \alpha)$. Fix $\sigma \in \mathrm{G}$ and let $\psi_n(\sigma) = u$, and let $k = \max\left\{r \;\middle|\; u \in \mathrm{U}_K^{(r)}/\mathrm{U}_K^{(n)}\right\}$. Then $u - 1 \in \pi^k\mathcal{O}_K \setminus \pi^{k+1}\mathcal{O}_K$. By definition of G_s, it suffices to show $\mathrm{v}_n(\sigma(\alpha) - \alpha) = q^k$. Let $\beta = (u-1)\cdot_{\mathrm{F}_f}\alpha$. Then $\beta \in \mu_{f,n-k} \setminus \mu_{f,n-k-1}$ and hence β is a uniformiser in $K_{\pi,n-k}$, so $\mathrm{v}_n(\beta) = q^k$. We have

$$\sigma(\alpha) = u \cdot_{\mathrm{F}_f} \alpha = (u-1)\cdot_{\mathrm{F}_f}\alpha +_{\mathrm{F}_f} \alpha \equiv (u-1)\cdot_{\mathrm{F}_f}\alpha + \alpha \mod \alpha\beta.$$

Thus $\mathrm{v}_n(\sigma(\alpha) - \alpha) = \mathrm{v}_n\left((u-1)\cdot_{\mathrm{F}_f}\alpha\right) = q^k$. ☐

Corollary 7.5.2. *ψ_n induces*

$$\mathrm{G}^s \cong \begin{cases} \mathrm{U}_K^{(0)}/\mathrm{U}_K^{(n)} & s \le 0 \\ \mathrm{U}_K^{(k)}/\mathrm{U}_K^{(n)} & k-1 < s \le k,\ 1 \le k \le n-1 \\ \{1\} & s > n-1 \end{cases}.$$

[3] Exercise: check on residue fields

Proof. If $s \leq 0$, then $\mathrm{G}_s = \mathrm{G}^s$. We compute

$$\phi_{K_{\pi,n}/K}(s) = \int_0^s \frac{1}{[\mathrm{G}_0 : \mathrm{G}_t]} \, \mathrm{d}t.$$

We have for $1 \leq k \leq n-1$, $\phi_{K_{\pi,n}/K}$ is linear on $\left(q^{k-1}-1, q^k-1\right]$, and

$$\phi_{K_{\pi,n}/K}\left(q^k-1\right) = \sum_{i=1}^k \frac{\left(q^i-1\right)-\left(q^{i-1}-1\right)}{q^i(q-1)} = \sum_{i=1}^k 1 = k,$$

by the same computation as $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$. The result follows from $\mathrm{G}^{\phi_{K_{\pi,n}/K}(s)} = \mathrm{G}_s$. ☐

Proposition 7.5.3. *Let $\sigma \in \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$ such that $\sigma|_{K^{\mathrm{ur}}} = \mathrm{Fr}_{K^{\mathrm{ur}}/K}$ and set $K_\sigma = \left(K^{\mathrm{ab}}\right)^\sigma$ then*

$$K^{\mathrm{ab}} = K_\sigma K^{\mathrm{ur}}.$$

Fact. By Theorem 6.1.4, $\overline{\langle\sigma\rangle} = \mathrm{Gal}\left(K^{\mathrm{ab}}/K_\sigma\right) \cong \widehat{\mathbb{Z}}$, since there is a splitting

$$1 \to \mathrm{Gal}\left(K^{\mathrm{ab}}/K^{\mathrm{ur}}\right) \to \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right) \xrightarrow{\sigma \leftarrow 1} \widehat{\mathbb{Z}} \to 1.$$

Proof. Let F/K_σ be a finite extension of degree d such that $F \subseteq K^{\mathrm{ab}}$. Want to show $F \subseteq K^{\mathrm{ur}}K_\sigma$. Since $\mathrm{Gal}\left(K^{\mathrm{ab}}/K_\sigma\right) \cong \widehat{\mathbb{Z}}$, there exists a unique degree d extension of K_σ contained in K^{ab} corresponding to $\widehat{\mathbb{Z}}/d\widehat{\mathbb{Z}}$. Since $\sigma|_{K^{\mathrm{ur}}} = \mathrm{Fr}_{K^{\mathrm{ur}}/K}$, $K_\sigma \cap K^{\mathrm{ur}} = K$, since for example $\mathcal{O}_{K_\sigma}/\mathfrak{m}_{K_\sigma} = \kappa$. Thus

$$\mathrm{Gal}(K_d K_\sigma/K_\sigma) \cong \mathrm{Gal}(K_d/K) \cong \mathbb{Z}/d\mathbb{Z},$$

where K_d/K is the degree d unramified extension, so $F = K_d K_\sigma$. ☐

Lemma 7.5.4. *Let $L_1, L_2 \subseteq K^{\mathrm{ab}}$ such that $\mathrm{G}^n(L_1/K) = \{1\}$ and $\mathrm{G}^n(L_2/K) = \{1\}$, then $\mathrm{G}^n(L_1L_2/K) = \{1\}$.*

Proof. Set $H_1 = \mathrm{Gal}(L_1L_2/L_1)$ and $H_2 = \mathrm{Gal}(L_1L_2/L_2)$. Then

$$\mathrm{G}^n(L_1L_2/K)\,H_1/H_1 \cong \mathrm{G}^n(L_1/K) = \{1\}, \qquad \mathrm{G}^n(L_1L_2/K)\,H_2/H_2 \cong \mathrm{G}^n(L_2/K) = \{1\},$$

so $\mathrm{G}^n(L_1L_2/K) \subseteq H_1 \cap H_2 = \{1\}$. ☐

Corollary 7.5.5 (Corollary of Hasse-Arf)**.** *Let L/K be a totally ramified abelian extension, and let $\mathrm{G} = \mathrm{Gal}(L/K)$. If $\mathrm{G}^n = \{1\}$, then*

$$[L : K] \mid q^{n-1}(q-1).$$

Remark. The Hasse-Arf theorem says $K_{\pi,n}$ maxes out the possible jumps. See example sheet 3 question 7.

Proof. Let $m \in \mathbb{Z}_{\geq 0}$ such that $m - 1 < \psi_{L/K}(n) \leq m$. Then

$$\mathrm{G} = \mathrm{G}_0 \supseteq \cdots \supseteq \mathrm{G}_m = \{1\}.$$

Claim that there exist at most $n-1$ distinct G_i for $i \geq 1$ such that $\mathrm{G}_i/\mathrm{G}_{i+1} \neq \{1\}$. By Hasse-Arf, $\mathrm{G}_i/\mathrm{G}_{i+1} \neq \{1\}$ for at most n distinct G_i for $i \geq 0$. If $\mathrm{G}_0 \neq \mathrm{G}_1$, done. Otherwise, $\mathrm{G}_0 = \mathrm{G}_1$ and $\psi_{L/K}(1) = 1$, so $\mathrm{G}^0 = \mathrm{G}_0 = \mathrm{G}_1 = \mathrm{G}^1$, which implies the claim. Then $\mathrm{G}_0/\mathrm{G}_1 \hookrightarrow \kappa_L^\times = \kappa^\times$ and $\mathrm{G}_i/\mathrm{G}_{i+1} \hookrightarrow (\kappa, +)$ for $i \geq 1$, so $[L : K] = |\mathrm{G}| \mid q^{n-1}(q-1)$. ☐

Consider $K^{\mathrm{ur}}K_{\pi,\infty}$. Since $\mathrm{Gal}(K^{\mathrm{ur}}K_{\pi,\infty}/K) \cong \widehat{\mathbb{Z}} \times \mathcal{O}_K^\times$, $K^{\mathrm{ur}}K_{\pi,\infty} \subseteq K^{\mathrm{ab}}$. Theorem 7.4.1 states that $K^{\mathrm{ab}} = K^{\mathrm{ur}}K_{\pi,\infty}$.

Proof of Theorem 7.4.1. Let $\widetilde{\sigma} \in \mathrm{Gal}(K^{\mathrm{ur}}K_{\pi,\infty}/K)$ be corresponding to $\left(\mathrm{Fr}_{K^{\mathrm{ur}}/K}, \mathrm{id}\right) \in \mathrm{Gal}(K^{\mathrm{ur}}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K)$. Let $\sigma \in \mathrm{Gal}\left(K^{\mathrm{ab}}/K\right)$ such that $\sigma|_{K_{\pi,\infty}K^{\mathrm{ur}}} = \widetilde{\sigma}$. Set $K_\sigma = \left(K^{\mathrm{ab}}\right)^\sigma$. Then $K_\sigma \cap K^{\mathrm{ur}} = K$, so K_σ is totally ramified. We have $K_{\pi,\infty} = (K^{\mathrm{ur}}K_{\pi,\infty})^{\widetilde{\sigma}} \subseteq K_\sigma$. By Proposition 7.5.3, it suffices to show $K_{\pi,\infty} = K_\sigma$. Let F/K be finite Galois such that $F \subseteq K_\sigma$. Take $n \geq 1$ such that $\mathrm{G}^n(F/K) = \{1\}$. Let $L = K_{\pi,n}F$. Then by Lemma 7.5.4, $\mathrm{G}^n(L/K) = \{1\}$. Since L/K is totally ramified, by Corollary 7.5.5, $[L : K] \mid q^{n-1}(q-1) = [K_{\pi,n} : K]$, so $L = K_{\pi,n}$. Thus $F \subseteq K_{\pi,n}$, so $K_\sigma = K_{\pi,\infty}$. ☐

8 Quadratic forms*

8.1 Quadratic forms

Let K be a field with $\operatorname{ch} K \neq 2$, and let

$$Q(x_1, \dots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j \in K[x_1, \dots, x_n], \qquad a_{ij} = a_{ji}$$

be a quadratic form of rank n, so $A = (a_{ij})$ is non-degenerate.

Definition 8.1.1. Q **represents** an element $c \in K$ if there exist $\alpha_1, \dots, \alpha_n \in K$ not all zero such that $Q(\alpha_1, \dots, \alpha_n) = c$.

Fact.

- If Q represents zero, then Q represents all $c \in K$.
- If $Q \sim Q'$ are equivalent, Q represents zero if and only if Q' represents zero.
- Every non-degenerate quadratic form of rank n is equivalent to a diagonal form, that is

$$Q = a_1 x_1^2 + \cdots + a_n x_n^2, \qquad a_i \in K.$$

Proposition 8.1.2. *Let $p > 2$, and let $Q = \sum_{i=1}^n a_i x_i^2$ for $a_i \in \mathbb{Q}_p^\times$. Suppose either*

1. *$n \ge 3$, and $a_i \in \mathbb{Z}_p^\times$ for all i, or*
2. *$n \ge 5$.*

Then Q represents zero.

Proof.

1. Without loss of generality $Q = ax^2 + by^2 - z^2$ for $a, b \in \mathbb{Z}_p^\times$. Then the maps given by

$$\begin{array}{ccc} \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ x & \longmapsto & \overline{a}x^2 \end{array}, \qquad \begin{array}{ccc} \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ y & \longmapsto & 1 - \overline{b}y^2 \end{array}$$

   have images of size $(p+1)/2$, hence they overlap, so there exist $x, y \in \mathbb{Z}_p$ such that $ax^2 + by^2 \equiv 1 \mod p$. By Hensel, $ax^2 + by^2 \in \left(\mathbb{Z}_p^\times\right)^2$, so $X^2 - ax^2 + by^2 = 0$ has a solution in $\mathbb{Z}_p$. Thus Q represents zero.

2. Without loss of generality $\mathrm{v}_p(a_i) \in \{0, 1\}$ for all i, by scaling by powers of p. Since $n \ge 5$, without loss of generality $\mathrm{v}_p(a_1) = \mathrm{v}_p(a_2) = \mathrm{v}_p(a_3)$. If these are zero, reduce to case 1. Otherwise divide by p and we are in case 1.

□

8.2 The Hasse-Minkowski theorem

Lecture 24
Wednesday
02/12/20

Theorem 8.2.1 (Hasse-Minkowski)**.** *Let Q be a quadratic form over $\mathbb{Q}$ of rank n. Then Q represents zero in $\mathbb{Q}$ if and only if Q represents zero in $\mathbb{Q}_v$ for $v \in \{2, 3, \dots, \infty\}$, where $\mathbb{Q}_\infty = \mathbb{R}$.*

Remark.

- An example of a local to global principle.
- The result is also true for number fields.

Lemma 8.2.2. *Let $Q = x_1^2 - ax_2^2 - bx_3^2$ for $a, b \in K^\times$ with $\operatorname{ch} K \neq 2$. Then Q represents zero in K if and only if $b \in \mathrm{N}_{L/K}(L^\times)$ for $L = K(\sqrt{a})$.*

Proof.

$\Longrightarrow$ Let $(x, y, z) \in K^3$ be a non-trivial solution. If $z = 0$, then $a = (x/y)^2$, so $L = K$ so $\mathrm{N}_{L/K}(L^\times) = K^\times$. Otherwise $z \neq 0$ and $b = (x/z)^2 - a(y/z)^2 = \mathrm{N}_{L/K}(x/z + (y/z)\sqrt{a})$.

$\Longleftarrow$ If $a \in (K^\times)^2$, then $(\sqrt{a}, 1, 0)$ is a solution. Otherwise $b = \mathrm{N}_{L/K}(x + y\sqrt{a}) = x^2 - ay^2$, so $(x, y, 1)$ is a solution.

□

Definition 8.2.3. For $v \in \{2, 3, \dots, \infty\}$ and $\alpha, \beta \in \mathbb{Q}_v^\times$. The **Hilbert symbol** $(\alpha, \beta)_v \in \{\pm 1\}$ is defined by

$$(\alpha, \beta)_v = \begin{cases} +1 & \alpha x + \beta y^2 - z^2 \text{ represents zero in } \mathbb{Q}_v \\ -1 & \text{otherwise} \end{cases}.$$

By example sheet 4, if $a, b \in \mathbb{Q}^\times$, then

$$\prod_{v \in \{2,3,\dots,\infty\}} (a, b)_v = 1,$$

the **product formula**.

Corollary 8.2.4. *If $Q = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ for $a_1, a_2, a_3 \in \mathbb{Q}$ of rank three represents zero in $\mathbb{R}$ and $\mathbb{Q}_p$ for all but one prime q, then Q represents zero in $\mathbb{Q}_q$.*

Proof. Without loss of generality $Q = a_1x_1^2 + a_2x_2^2 - x_3^2$. Then $(a_1, a_2)_v = 1$ for all v except possibly $v = q$. By the product formula, $(a_1, a_2)_q = 1$. □

Theorem 8.2.5 (Dirichlet's theorem)**.** *For $m, d \in \mathbb{Z}$ such that $(m, d) = 1$, there are infinitely many primes of the form $mb + d$ for $b \in \mathbb{Z}$.*

Proof of Theorem 8.2.1.

$\Longrightarrow$ Clear.

$\Longleftarrow$ Four cases.

$n = 2$. Without loss of generality $Q = x_1^2 + ax_2^2$. Since $-a \in (\mathbb{Q}_p^\times)^2$, $\mathrm{v}_p(a)$ is even for all primes p. Since $-a \in (\mathbb{R}^\times)^2$, $a < 0$. Thus $a = -p_1^{2e_1} \dots p_r^{2e_r} / q_1^{2f_1} \dots q_s^{2f_s}$. Thus $-a \in (\mathbb{Q}^\times)^2$ and Q represents zero in $\mathbb{Q}$.

$n = 3$. Let $Q = x_1^2 - ax_2^2 - bx_3^2$. Without loss of generality $\mathrm{v}_p(a), \mathrm{v}_p(b) \in \{0, 1\}$ for all p, by scaling x_2 and x_3, and $|a| \leq |b|$. We induct on $m = |a| + |b|$.

* If $m = 2$, then $Q = \pm x_1^2 \pm x_2^2 \pm x_3^2$. Exclude all $+$ and all $-$, since Q represents zero over $\mathbb{R}$.
* Suppose $m > 2$, then $|b| \geq 2$. Write $b = \pm p_1 \dots p_k$ for p_i distinct primes. Claim that a is a square modulo p_i for $i = 1, \dots, k$. If $p_i \mid a$ this is clear. Otherwise $\mathrm{v}_{p_i}(a) = 0$. Let $(x, y, z) \in \mathbb{Q}_{p_i}^3$ be a non-trivial solution. Without loss of generality may assume $(x, y, z) \in \mathbb{Z}_{p_i}^3$, and $(x, y, z) \notin (p_i\mathbb{Z}_{p_i})^3$. Thus $x^2 - ay^2 \equiv 0 \mod p_i$. If $y \equiv 0 \mod p_i$, then $x \equiv 0 \mod p_i$, so $z \equiv 0 \mod p_i$, a contradiction. Thus $a \equiv (x/y)^2 \mod p_i$. Since $\mathbb{Z}/b\mathbb{Z} \cong \prod_{i=1}^k \mathbb{Z}/p_i\mathbb{Z}$, a is a square modulo b. That is, there exist $r, s \in \mathbb{Z}$ such that

$$r^2 = a + bs.$$

Without loss of generality $0 \leq r \leq b/2$. Since $sb = r^2 - a$, $sb \in \mathrm{N}_{K/\mathbb{Q}}(K^\times)$ for $K = \mathbb{Q}(\sqrt{a})$. By Lemma 8.2.2 $x_1^2 - ax_2^2 - bx_3^2$ represents zero in $\mathbb{Q}$ or $\mathbb{Q}_v$ if and only if $x_1^2 - ax_2^2 - sx_3^2$ represents zero in $\mathbb{Q}$ or $\mathbb{Q}_v$, since $b \in \mathrm{N}_{K/\mathbb{Q}}(K^\times)$ if and only if $s \in \mathrm{N}_{K/\mathbb{Q}}(K^\times)$. Then $|s| = |(r^2 - a)/b| \leq |b/4| + 1 < |b|$ since $|b| \geq 2$. Write $s = b'u^2$ where b' is square-free and $u \in \mathbb{Z}$. Then $|b'| < |b|$ and by induction $x_1^2 - ax_2^2 - b'x_3^2$ represents zero in $\mathbb{Q}$, so $x_1^2 - ax_2^2 - bx_3^2$ represents zero in $\mathbb{Q}$.

$n = 4$. We reduce to the case $n = 3$. Without loss of generality $Q = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$. Without loss of generality $a_4 < 0$ and $a_1 > 0$. Consider

$$g = a_1x_1^2 + a_2x_2^2, \qquad h = -a_3x_3^2 - a_4x_4^2.$$

Let $p_1, \dots, p_s$ be the odd primes dividing $a_1a_2a_3a_4$. Since Q represents zero in $\mathbb{Q}_p$, there exists $b_p \in \mathbb{Q}_p$ such that g and h both represent b_p in $\mathbb{Q}_p$. Without loss of generality $b_p \neq 0$, since if g represents zero then it represents any $\gamma \in \mathbb{Q}_p$, and $\mathrm{v}_p(b_p) \in \{0, 1\}$. Claim that there exists $a \in \mathbb{Z}_{>0}$ such that

1. $a \equiv b_2 \mod 16$,
2. $a \equiv b_{p_i} \mod p_i^2$ for $i = 1, \dots, s$, and
3. there exists a unique prime $q \notin \{2, p_1, \dots, p_s\}$ such that $q \mid a$.

Set $m = 16p_1^2 \dots p_s^2$. Choose $a' > 0$ satisfying 1 and 2, by CRT. Let $d = (m, a')$. By Dirichlet, there exists $k \in \mathbb{Z}_{>0}$ such that $a'/d + km/d = q$ is prime, so $a = a' + km = dq$ satisfies 1, 2, and 3. Set $g' = g - ax_0^2$ and $h' = h - ax_0^2$. By 1 and 2, $b_{p_i}^{-1}a \equiv 1 \mod p_i$ for $i = 1, \dots, s$ and $b_2^{-1}a \equiv 1 \mod 8$. By Hensel's lemma, $b_{p_i}^{-1}a \in \left(\mathbb{Q}_{p_i}^\times\right)^2$ for $i = 1, \dots, s$ and $b_2^{-1}a \in \left(\mathbb{Q}_2^\times\right)^2$. Thus g' and h' represent zero in $\mathbb{Q}_2$ and $\mathbb{Q}_{p_i}$ for $i = 1, \dots, s$. By Proposition 8.1.2, g' and h' represent zero in $\mathbb{Q}_p$ for $p \notin \{2, p_1, \dots, p_s\}$ and $p \neq q$. Since $a_1 > 0$ and $a_4 < 0$, g' and h' represent zero in $\mathbb{R}$. By Corollary 8.2.4, g' and h' represent zero in $\mathbb{Q}_q$. Thus g' and h' represent zero in $\mathbb{Q}$, so $Q = g' - h'$ represents zero in $\mathbb{Q}$.

$n \geq 5$. Let $Q = \sum_{i=1}^n a_ix_i^2$. By Proposition 8.1.2, Q represents zero in $\mathbb{Q}_p$ for all p. Thus need to show, if Q is indefinite, then Q represents zero in $\mathbb{Q}$. Without loss of generality $a_1 > 0$ and $a_5 < 0$. It suffices to show $Q = \sum_{i=1}^5 a_ix_i^2$ represents zero in $\mathbb{Q}$. Let

$$g = a_1x_1^2 + a_2x_2^2, \qquad h = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2.$$

The same argument as $n = 4$ shows there exists $a \in \mathbb{Z}_{>0}$ such that $g' = g - ax_0^2$ and $h' = h - ax_0^2$ represent zero in $\mathbb{Q}_v$ for $v \in \{2, 3, \dots, \infty\}$. By $n = 3$ and $n = 4$, g' and h' represent zero in $\mathbb{Q}$. Thus Q represents zero in $\mathbb{Q}$.

□