Local Fields: lecture 1 | Basic Theory.

Question: Find, for $f(X_1, \dots, X_n) \in \mathbb{Z}[\underline{X}]$, $\underline{x}$ s.t. $f(\underline{x}) = 0$.

Or: $f(\underline{x}) \equiv 0 \bmod p$, or p^2, or $\dots$ p^n.

Local fields: "package" all info, together.

---

§1: Absolute Value.

DEF 1.1 K field. An **absolute value** on K is: $|\cdot| : K \to \mathbb{R}_{\geq 0}$

s.t: ⊛ $|x| = 0 \iff x = 0$

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

⊛ $|x+y| \leq |x| + |y|$ $(\forall x, y \in K)$. $(\Delta\text{-ineq})$

Then: say, $(K, |\cdot|)$ is **valued field**.

Examples. ⊛ $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $|a+ib| = \sqrt{a^2+b^2}$

⊛ **Trivial absolute value.** $|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0. \end{cases}$ (any field k).

In this course: ignore this. (nontrivial abs val)

⊛ $K = \mathbb{Q}$ & p prime.

$\Rightarrow \forall x \in \mathbb{Q}$ $(x \neq 0)$, write: $x = p^n \cdot \frac{a}{b}$ where $\gcd(a,b) = 1$ and $p \nmid a$, $p \nmid b$. Then, define: $|x|_p \equiv \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{if } x \text{ as above.} \end{cases}$

Is an absolute value, because:

1) clear.

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

3) $|x+y|_p = \left| p^n \frac{ad + p^{m-n} bc}{bd} \right|_p$. If WLOG $m \geq n$, then:

this $\leq p^{-n} = \max(|x|_p, |y|_p)$. ✓ ("Ultrametric property")

Facts. An abs val $|\cdot|$ induces: metric $d(x,y) := |x-y|$ on K.
$\Rightarrow$ Induces topology on K.

DEF 1.2 $|\cdot|, |\cdot|'$ abs vals on K. Are: **equivalent** if: induce same topology. Defines equivalence class of abs vals.
& Equiv class of abs vals is a **place**.

Prop 1.3 TFAE:

1) $|\cdot|, |\cdot|'$ equivalent
2) $|x|<1 \iff |x|'<1$
3) $\exists c>0,\ |x|^c = |x|' \ (\forall x \in K.)$

Proof 1) $\Rightarrow$ 2): $|x|<1 \iff x^n \to 0$ (WRT $|\cdot|$)
$\iff x^n \to 0$ (WRT $|\cdot|'$)
$\iff |x|'<1$.

2) $\Rightarrow$ 3): Note: $|x|^c = |x|' \iff c \log|x| = \log|x|'$.
So, need: for fixed $a \in K^*$, $\dfrac{\log|x|}{\log|a|} = \dfrac{\log|x|'}{\log|a|'}$ $\forall x \in K$.
If not: WLOG, $\dfrac{\log|x|}{\log|a|} < \dfrac{\log|x|'}{\log|a|'}$. (WLOG, $|a|>1$, since abs val nontrivial)
$\Rightarrow \exists m, n \in \mathbb{Z}$, s.t. $LHS < \frac{m}{n} < RHS$.
$\Rightarrow n \log|x| < m \log|a|$ & $n \log|x|' > m \log|a|'$
$\Rightarrow \left|\frac{x^n}{a^m}\right| < 1$ & $\left|\frac{x^n}{a^m}\right|' > 1$ ⚡.
So, equality holds.
3) $\Rightarrow$ 1): is obvious. ✓

Remark $|\cdot|_\infty^2$ on $\mathbb{C}$ not an absval, since doesn't satisfy Δ-ineq.
Some authors replace Δ-ineq with: $|x+y|^\beta \leq |x|^\beta + |y|^\beta$ for some $\beta > 0$ fixed.

In this course: interested in:

DEF 1.4 $|\cdot|$ non-Archimedean (on K) if: satisfies ultrametric ineq $|x+y| \leq \max |x|, |y|$.
& $|\cdot|$ archimedean if not non-archimedean.

Examples $|\cdot|_\infty$ on $\mathbb{R}$ is archimedean
$|\cdot|_p$ on $\mathbb{Q}$ is not.

Lemma 1.5 $(K, |\cdot|)$ non-archimedean & $x, y \in K$. Then if $|x| < |y|$, then $|x-y| = |y|$. ("All triangles isosceles")

Proof $|x-y| \leq \max(|x|, |y|) = |y|$ (since: $|-y| = |y|$).
& $|y| \leq \max(|x|, |x-y|)$, so $|y| \leq |x-y|$. So, equal.

Convergence is easier in non-archimedean fields:

Prop 1.6 $(K, |\cdot|)$ non-arch & $(x_n)_{n=1}^\infty \subseteq K$, with $|x_n - x_{n+1}| \to 0$. Then: (x_n) Cauchy.
In addition: if K complete WRT $|\cdot|$, then (x_n) converges.

Proof For $\varepsilon > 0$: find N, $|x_n - x_{n+1}| < \varepsilon$ $\forall n \geq N$.
$\Rightarrow$ For $N < n < m$: $|x_n - x_m| = |(x_n - x_{n+1}) + \cdots + (x_{m-1} - x_m)| < \varepsilon$.

So, is Cauchy. (& In particular part is obvious)

Example) $p=5$, & $(x_n)_{n=1}^{\infty}$ defined by:

(*) $x_n^2+1 \equiv 0 \mod 5^n$

(*) $x_n \equiv x_{n+1} \mod 5^n$.

Construct by induction: $x_1=2$, and: if x_n constructed: then

$x_{n+1} = x_n + b\cdot 5^n$ (b to be determined)

have: $x_{n+1}^2+1 = x_n^2 + 2bx_n 5^n + b^2 5^{2n} + 1$

$= a\cdot 5^n + 2b\cdot x_n 5^n + \underbrace{b^2 5^{2n}}_{\equiv 0 \mod 5^{n+1}}$.

$\Rightarrow$ Choose b: $a+2bx_n \equiv 0 \mod 5$. (since x_n coprime to 5)

Then: $|x_n - x_{n+1}|_5 \to 0$, so Cauchy.

If $x_n \to \ell$ in $\mathbb{Q}$ then $x_n^2 \to \ell^2$ in $\mathbb{Q}$

but: by 1): $x_n^2 \to -1$, so $\ell^2 = -1$ #.

$\Rightarrow (\mathbb{Q}, |\cdot|_5)$ not complete.

DEF 1.7) p-adic numbers $\mathbb{Q}_p \equiv$ completion of $\mathbb{Q}$, WRT $|\cdot|_p$.

$\mathbb{Q} \xrightarrow{|\cdot|_\infty} \mathbb{R}$

$\mathbb{Q} \xrightarrow{|\cdot|_p} \mathbb{Q}_p$

Local Fields. Lecture 2.

Let: $(K, |\cdot|)$ non-Arch field. Define: for $x \in K$ & $r \geq 0$:

$B(x,r) \equiv \{y \in K : |x-y| < r\}$ & $\bar{B}(x,r) \equiv \{y \in K : |x-y| \leq r\}$.

Lemma 1.8 Open & closed balls don't have centres.

i) If $z \in B(x,r)$ then $B(x,r) = B(z,r)$

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

iii) $B(x,r)$ closed

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

Proof i) For $y \in B(x,r)$: $|x-y| < r$.

$\Rightarrow |z-y| = |(z-x)+(x-y)| \leq \max(|z-x|, |x-y|) < r$.

$\Rightarrow B(x,r) \subseteq B(z,r)$ (and $\supseteq$, by symmetry).

ii) Same argument as i).

iii): Let: $y \notin B(x,r)$. Claim: $B(x,r) \cap B(y,r) = \emptyset$.

(This gives open nbhood of y not intersecting $B(x,r)$.)

Proof: if $z \in B(x,r)$, then $B(x,r) = B(z,r) = B(y,r) \Rightarrow y \in B(x,r)$ ↯.

iv): If $z \in \bar{B}(x,r)$, then: $B(z,r) \subseteq \bar{B}(z,r) \underset{(ii)}{=} \bar{B}(x,r)$.

---

§2: Valuation Rings.

DEF 2.1 K field. A valuation is $v : K^* \to \mathbb{R}$ s.t.

i) $v(xy) = v(x) + v(y)$ $\forall x, y \in K^*$

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

Note For $0<\alpha<1$: can define abs val $|x| = \begin{cases} \alpha^{v(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$
& conversely, given $|\cdot|$, get $v(x) \equiv \log_\alpha |x|$.
$\Rightarrow$ Valuations & non-Archimedean abs vals are the same.

Remark Say v_1, v_2 equivalent $\Leftrightarrow \exists c > 0$, $cv_1 = v_2$.

Examples ⊛ $k = \mathbb{Q}$, $v_p(x) = -\log_p(|x|_p)$ (p-adic val.)

⊛ k field & $K \equiv k(t) \equiv FF\, k[t]$.
& $v\left(t^n \frac{f(t)}{g(t)}\right) \equiv n$, where f, g polys with nonzero const term.
"t-adic valuation".

⊛ $K = k((t))$, formal Laurent series. $\equiv FF\, k[[t]]$.
$\equiv \left\{ \sum_{i \geq n} a_i t^i : a_i \in k \text{ & } n \in \mathbb{Z} \right\}$.
& $v\left(\sum_i a_i t^i\right) = \min\{i : a_i \neq 0\}$. Also is valuation.

DEF 2.2 $(K, |\cdot|)$ non-Arch. The valuation ring
$\mathcal{O}_K \equiv \{x \in K : |x| \leq 1\} = \{x \in K : v(x) \geq 0\} \cup \{0\} = \bar{B}(0,1)$.

Prop 2.3 i) $\mathcal{O}_K$ is open subring of K
ii) The sets $\{x \in K : |x| \leq r\}$ & $\{x \in K : |x| < r\}$ (for $r \leq 1$) are open ideals in $\mathcal{O}_K$.
iii) $\mathcal{O}_K^* = \{x \in K : |x| = 1\}$.

Proof i) $|0| = 0$ & $|1| = 1 \Rightarrow 0, 1 \in \mathcal{O}_K$.

If $x \in \mathcal{O}_K$ then $|-x| = |x| \leq 1 \Rightarrow -x \in \mathcal{O}_K$.

If $x, y \in \mathcal{O}_K$ then: $|x+y| \leq \max(|x|, |y|) \leq 1$ & $|xy| = |x||y| \leq 1$, so $x+y$, $xy \in \mathcal{O}_K$. Hence: $\mathcal{O}_K$ is subring, and since it is $\overline{B}(0,1)$, it is open.

ii) Similar to i)

iii) $|x| \cdot |x^{-1}| = |x \cdot x^{-1}| = 1$, so $|x| = 1 \Leftrightarrow |x^{-1}| = 1$

$\Leftrightarrow x, x^{-1} \in \mathcal{O}_K \Leftrightarrow x \in \mathcal{O}_K^*$.

Notation $\mathfrak{m} \equiv \{x \in \mathcal{O}_K : |x| < 1\} = B(0,1)$, maximal ideal of $\mathcal{O}_K$, and: $k \equiv \mathcal{O}_K / \mathfrak{m}$. $\equiv$ Residue field.

Corollary 2.4] $\mathcal{O}_K$ is local ring (has unique max ideal).

Proof If $\mathfrak{m}'$ some other maximal ideal ($\mathfrak{m}' \neq \mathfrak{m}$), then find $x \in \mathfrak{m}' \setminus \mathfrak{m}$. Then, x unit, so $\mathfrak{m}' = R$ ##

Examples $K = \mathbb{Q}$, with $|\cdot|_p$. Then: $\mathcal{O}_K = \mathbb{Z}_{(p)} = \{\frac{a}{b} : p \nmid b\}$. & $\mathfrak{m} = p\mathbb{Z}_{(p)}$ and $k = \mathbb{F}_p$.

DEF 2.5] If $v(K^\times) \cong \mathbb{Z}$ then v is a Discrete valuation & K is discretely valued field.

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

Examples $K = \mathbb{Q}$, with $|\cdot|_p$
$K = k(t)$, with t-adic val.
} $\Rightarrow$ discrete val fields.

& $k = k(t)(t^{\frac{1}{2}}, t^{1/4}, t^{1/8}, \ldots)$ not DVR.

Remark If v is DVR: can scale, s.t. $v(k^\times) = \mathbb{Z}$.

Call this: normalised valuations.

So, in this case, π uniformizer $\iff v(\pi) = 1$.

Lemma 2.6 v valuation on k. TFAE:

i) v discrete

ii) $\mathcal{O}_k$ PID

iii) $\mathcal{O}_k$ Noetherian

iv) m principal.

Proof i) $\Rightarrow$ ii): Integral domain ✓ (since $\mathcal{O}_k \subseteq k$)

Let: $I \subseteq \mathcal{O}_k$ ideal & choose $x \in I$ with minimal positive valuation,

i.e. $v(x) = \min\{v(y) : y \in I \ \& \ y \neq 0\}$.

(Exists, as v discrete)

Then: claim $x\mathcal{O}_k \equiv \{a \in \mathcal{O}_k : v(a) \geq v(x)\}$ is $= I$.

$\subseteq$ obvious, since I ideal

$\supseteq$: for $y \in I$, have $v(x^{-1}y) \geq 0$, so $y = x(x^{-1}y) \in \mathcal{O}_k$.

ii) $\Rightarrow$ iii): obvious.

iii) $\Rightarrow$ iv): Write: $m = x_1\mathcal{O}_k + \cdots + x_n\mathcal{O}_k$ where WLOG

$v(x_1) \leq v(x_2) \leq \ldots \leq v(x_n)$. Then, $x_i \in x_1\mathcal{O}_k$ $\forall i$, so $m = x_1\mathcal{O}_k$.

iv) $\Rightarrow$ i): Let $m = \pi\mathcal{O}_k$, some $\pi \in \mathcal{O}_k$, and $c \equiv v(\pi)$.

If $v(x) > 0$, $x \in m$, then $v(x) \geq c$, so $v(k^\times) \cap (0, c) = \emptyset$.

Since $v(k^\times) \leq (\mathbb{R}, +)$: get $v(k^\times) = c\mathbb{Z}$ ✓ discrete.

Local Fields: Lecture 3

Here: v discrete val on K, & $\pi \in \mathcal{O}_K$ uniformizer.

For $x \in K^*$: $\exists n \in \mathbb{Z}$, $v(x) = n \cdot v(\pi)$. Then, $u \equiv x \cdot \pi^{-n} \in \mathcal{O}_K^*$ is a unit & $x = u \cdot \pi^n$.

$\Rightarrow$ In particular: $K = \mathcal{O}_K\left[\frac{1}{\pi}\right]$, so $K = \mathrm{Frac}(\mathcal{O}_K)$.

DEF 2.7 R ring. Is: discrete valuation ring (DVR) if: R PID & exactly 1 nonzero prime ideal (necessarily maximal).

Lemma 2.8 i) v discrete val. Then: $\mathcal{O}_K$ DVR.

ii) R DVR. $\Rightarrow \exists v$ valuation on $K = FF(R)$ s.t. $R = \mathcal{O}_K$.

Proof i) $\mathcal{O}_K$ is PID, by lemma 2.6, so any nonzero prime ideal is maximal. So, is DVR, since local ring.

ii) R DVR, maximal ideal m. So, $m = (\pi)$, $\pi \in R$.

Since PID $\Rightarrow$ UFD: can write: $\forall x \in R \setminus 0$ uniquely as $\pi^n \cdot u$, $(n \geq 0$ & u unit)

$\Rightarrow$ Any $y \in K^*$ can be written uniquely as: $\pi^n \cdot u$, u unit. $n \in \mathbb{Z}$.

Define: $v(\pi^n \cdot u) \equiv n$. Then, this defines a valuation, and $\mathcal{O}_K = R$ (check!).

Examples (of DVR's). $\mathbb{Z}_{(p)}$, $k[\![t]\!]$ are DVR's. (k field)

§3: p-adic numbers. $\mathbb{Q}_p \equiv$ Completion of $\mathbb{Q}$ WRT $|\cdot|_p$.

From sheet 1: $\mathbb{Q}_p$ is a field. & $|\cdot|_p$ extends to $\mathbb{Q}_p$,

and the associated valuation is discrete.

DEF 3.1 Ring of p-adic integers $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

Facts: $\mathbb{Z}_p$ is DVR. Maximal ideal $p \cdot \mathbb{Z}_p$.

All nonzero ideals are: $p^n \cdot \mathbb{Z}_p$ $(n \geq 1)$.

Prop 3.2 $\mathbb{Z}_p$ = closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$.

In particular: $\mathbb{Z}_p$ is completion of $\mathbb{Z}$, WRT $|\cdot|_p$.

Proof Suffices to show $\mathbb{Z}$ dense in $\mathbb{Z}_p$.

Note: $\mathbb{Q}$ dense in $\mathbb{Q}_p$, & since $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ open: have $\mathbb{Z}_p \cap \mathbb{Q}$ dense in $\mathbb{Z}_p$.

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

So, suffices to show $\mathbb{Z}$ dense in $\mathbb{Z}_{(p)}$.

Select: $\frac{a}{b} \in \mathbb{Z}_{(p)}$. Then: $\forall n \in \mathbb{N}$, choose $y_n \in \mathbb{Z}$, such that: $by_n \equiv a \bmod p^n$. Then $y_n \longrightarrow \frac{a}{b}$ as $n \to \infty$. ✓

In particular: $\mathbb{Z}_p$ complete & $\mathbb{Z} \subseteq \mathbb{Z}_p$ dense.

Inverse Limits.

Let: $(A_n)_{n \in \mathbb{Z}}$ sequence of sets / groups / rings, together with homs $\varphi_n : A_{n+1} \longrightarrow A_n$. Then, the inverse limit is:

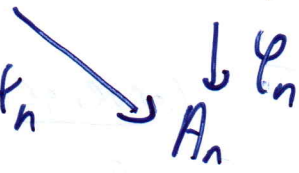
the set / group / ring $\varprojlim_n A_n \equiv \left\{(a_n)_{n \geq 1} \in \prod_{n \geq 1} A_n : \varphi_n(a_{n+1}) = a_n \ \forall n\right\}$

Fact If A_n group / ring then $\varprojlim_n A_n$ is also such.

$\square$

Let: $\theta_m : \varprojlim_n A_n \longrightarrow A_m$ natural projection.

Prop 3.3 (Universal Property). For any set/group/ring B with homs $\psi_n : B \to A_n$ s.t. $B \xrightarrow{\psi_{n+1}} A_{n+1}$ commutes:



then, $\exists!\ \psi : B \to \varprojlim_n A_n$,

with $\theta_n \circ \psi = \psi_n$ $\forall n$.

Proof Define: $\psi : B \to \prod_{n\in\mathbb{N}} A_n$ by $b \mapsto (\psi_n(b))_{n\geq 1}$.

Then: since $\psi_n = \varphi_n \circ \psi_{n+1} \Rightarrow \psi(b) \in \varprojlim_n A_n$

& map is clearly unique, determined by $\psi_n = \varphi_n \circ \psi_{n+1}$.

& is: hom. of sets/group/limits. ✓

DEF 3.4 Let: $I \subseteq R$ ideal. The I-adic completion of R is the ring: $\hat{R} \equiv \varprojlim_n R/I^n$. ($R/I^{n+1} \to R/I^n$ natural proj)

Note: $\exists$ natural map $i : R \to \hat{R}$ by universal prop. (i.e. maps $R \to R/I^n$).

Say: R is I-adically complete, if i is isomorphism.

Fact: $\ker(i) = \bigcap_{n\geq 1} I^n$.

Let: $(K, |\cdot|)$ non-arch. valued field & $\pi \in \mathcal{O}_K$, $|\pi| < 1$.

Prop 3.5 ~~As sequence~~ Assume: k complete WRT $|\cdot|$.

i) $\mathcal{O}_K \xrightarrow{i} \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$. ($\Rightarrow \mathcal{O}_K$ π-adically complete)

ii) $\forall x \in \mathcal{O}_K$: x can be written uniquely as $\sum_{i\geq 0} a_i \pi^i$, for $a_i \in A$, where $A \subseteq \mathcal{O}_K$ is a set of coset reps for $\mathcal{O}_K/\pi\mathcal{O}_K$.

Moreover, $\sum a_i \pi^i$ converges in $\mathcal{O}_K$.

Proof i) K complete & $\mathcal{O}_K$ closed $\Rightarrow \mathcal{O}_K$ complete.

& If $x \in \bigcap_{n\geq 1} \pi^n\mathcal{O}_K$, then: $v(x) \geq n\, v(\pi)$ $\forall n$, so $x = 0$.

Hence: $\mathcal{O}_K \xrightarrow{i} \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ injective ✓

Let: $(x_n)_{n\in\mathbb{N}} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$, and $\forall n$, find $y_n \in \mathcal{O}_K$ lift of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$.

Then: $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$, so (y_n) Cauchy in $\mathcal{O}_K$, hence converges to $y_n \longrightarrow y \in \mathcal{O}_K$.

Then: y maps to $(x_n)_{n\in\mathbb{N}}$ in $\varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ ✓

Corollary 3.6] i) $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

ii) Every $x \in \mathbb{Q}_p$ is uniquely $\sum_{i\geq n} a_i p^i$, $a_i \in \{0, 1, \dots, p-1\}$.

Local Fields: Lecture 4.

Proof i) By Prop 3.5: suffices to show: $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$

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

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

$\Rightarrow$ this is injective.

For $\bar{c} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$: take $c \in \mathbb{Z}_p$ lift. Since $\mathbb{Z}$ dense in $\mathbb{Z}_p$, $\exists x \in \mathbb{Z}$, s.t. $x \in c + p^n\mathbb{Z}_p$. (is: open in $\mathbb{Z}_p$)

$\Rightarrow f_n(x) = \bar{c}$, hence this surjective ✓

ii) Follows from: prop 3.5 ii), applied to $p^{-n}x \in \mathbb{Z}_p$ for some $n \in \mathbb{Z}$.

Example $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \cdots$ in $\mathbb{Q}_p$.

II: Complete Valued Fields.

§4: Hensel's lemma.

Theorem 4.1 (Version 1): $(K, |\cdot|)$ complete discretely valued field, and $f(x) \in \mathcal{O}_K[X]$.

Assume: $\exists a \in \mathcal{O}_K$, s.t. $|f(a)| < |f'(a)|^2$. (Formal derivative)

Then: $\exists!\ x \in \mathcal{O}_K$, with $f(x) = 0$ & $|x - a| < |f'(a)|$.

Proof Find $\pi \in \mathcal{O}_K$ uniformizer & $r \equiv v(f'(a))$.

(v normalised, so $v(\pi) = 1$).

Construct: $(x_n)_{n\in\mathbb{N}}$ in $\mathcal{O}_K$ s.t.

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

ii) $x_{n+1} \equiv x_n \bmod \pi^{n+r}$

Take: $x_1 = a$, so $f(a) \equiv 0 \bmod \pi^{1+2r}$.

If constructed $x_1, \dots, x_n$: then let $x_{n+1} \equiv x_n - \dfrac{f(x_n)}{f'(x_n)}$.

Have: $x_n \equiv x_1 \bmod \pi^{r+1} \Rightarrow v(f'(x_n)) = v(f'(x_1)) = r$

$\Rightarrow \dfrac{f(x_n)}{f'(x_n)} \equiv 0 \bmod \pi^{n+r}$, by i).

$\Rightarrow x_{n+1} \equiv x_n \bmod \pi^{n+r}$, so have ii). ✓

For i): If X, Y indeterminates, then $f(X+Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \dots$

where: $f_0(X) = f(X)$, $f_1(X) = f'(X)$.

$\Rightarrow f(x_{n+1}) = f(x_n) + f'(x_n)c + f_2(x_n)c^2 + \dots \quad \left(c = -\dfrac{f(x_n)}{f'(x_n)}\right)$

Since $c \equiv 0 \bmod \pi^{n+r}$ & $v(f_i(x_n)) \geq 0$, have: all terms $f_i(x_n)\,c^i \equiv 0 \bmod \pi^{n+2r+1}$ $\forall i \geq 2$.

$\Rightarrow f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \bmod \pi^{n+2r+1}$

$\equiv 0$ ✓

So, have: $(x_n)_{n\in\mathbb{N}}$. By ii): (x_n) Cauchy, so by completeness, $\exists x \in \mathcal{O}_K$, $x_n \to x$. So $f(x) = \lim_{n\to\infty} f(x_n) = 0$

Moreover: by iii): $a = x_1 \equiv x_n \bmod \pi^{r+1}$ $\forall n$.

$\Rightarrow x \equiv a \bmod \pi^{r+1}$, so: $|x-a| < |f'(a)|$. ✓

Uniqueness: Find x' also satisfying both $f(x') = 0$ & $|x'-a| < |f'(a)|$

$\sqrt{2}$

Set: $\delta \equiv x' - x$. If $\delta \neq 0$: $|x'-a| < |f'(a)|$ & $|x-a| < |f'(a)|$

$\Rightarrow |\delta| = |x'-x| \leq \max(|x'-a|, |x-a|) < |f'(a)| = |f'(x)|$

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

$\Rightarrow |f'(x)| \leq |\delta|$ ⚡

Corollary 4.2 $(k, |\cdot|)$ complete, discretely valued. Let $f(x) \in \mathcal{O}_k[x]$ & $\bar{c} \in k \equiv \mathcal{O}_k/m$ simple root of $\bar{f}(x) \equiv f(x) \bmod m \in k[x]$.

Then: $\exists! x \in \mathcal{O}_k$, with: $f(x) = 0$ and $x \equiv \bar{c} \bmod m$.

Proof Apply Theorem 4.1, to lift c of $\bar{c}$. Then, since c simple root: $|f(c)| < 1 = |f'(c)|^2$. So, gives x.

Example $f(x) = x^2 - 2$. Has: simple root mod 7, so by Hensel's lemma, $\exists$ solution in $\mathbb{Q}_7$. So, $\sqrt{2} \in \mathbb{Q}_7$.

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

Proof for $p > 2$: let $b \in \mathbb{Z}_p^\times$, then by Corollary 4.2 to $f(x) \equiv x^2 - b$: find, $b \in (\mathbb{Z}_p^\times)^2 \iff b \in (\mathbb{F}_p^\times)^2$.

Thus: $\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 \xrightarrow{\cong} \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$. (Since: $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$)

& Note $\exists$ isom. $\mathbb{Z}_p^\times \times \mathbb{Z} \xrightarrow{\cong} \mathbb{Q}_p^\times$

$(u, n) \longmapsto u \cdot p^n$

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

If $p=2$: again, $b \in \mathbb{Q}_2^\times$ & $f(x) = x^2 - b$.

Then: $f'(x) \equiv 0 \mod 2$, so f doesn't have simple root.

So, instead: look at congruences mod 8.

If $b \equiv 1 \mod 8$: $|f(1)|_2 \leq 2^{-3} < |f'(1)|_2^2 = 2^{-2}$.

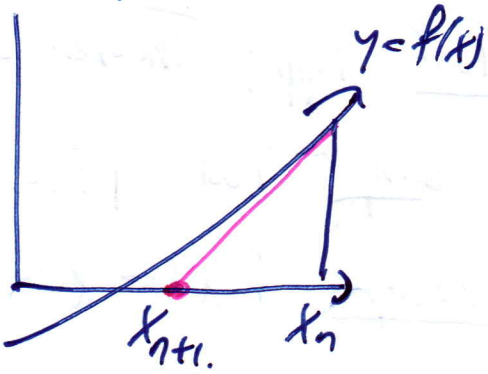
$\Rightarrow$ By Hensel's lemma: $b \in (\mathbb{Q}_2^\times)^2 \Leftrightarrow b \equiv 1 \mod 8$.

$\Rightarrow \mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$

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

Remark Proof uses iteration: $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.

$\Rightarrow$ Hensel's lemma is: non-Archimedean analogue, of the Newton–Rhapson method.



Theorem 4.4 (Hensel, 2nd version).

Let: $(K, |\cdot|)$ complete Discrete val field, and $f(x) \in \mathcal{O}_K[x]$. Suppose $\bar{f}(x) \equiv f(x) \pmod{m} \in k[x]$ factorises as: $\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$ in $k[x]$, for $\bar{g}, \bar{h}$ coprime.

Then: $\exists$ factorisation $f(x) = g(x)h(x)$ (in $\mathcal{O}_K[x]$) & $\deg(g) = \deg(\bar{g})$, and $g \equiv \bar{g}$, $h \equiv \bar{h} \mod m$.

Local Fields: lecture 5.

[corollary 4.5] $f(X) = a_n X^n + \dots + a_0 \in K[X]$, $a_n, a_0 \neq 0$.
If f irred then $|a_i| \leq \max(|a_n|, |a_0|)$ $\forall i$.

[Proof] By scaling: assume $f(X) \in \mathcal{O}_K[X]$ & $\max_{0 \leq i \leq n} |a_i| = 1$.
Need to show: $\max(|a_0|, |a_n|) = 1$.
If not: find r minimal, $|a_r| = 1$. (so: $0 < r < n$ by assumption)
Reduction mod m $\Rightarrow$ $\overline{f}(X) = X^r(a_r + \dots + a_n X^{n-r}) \bmod m$.
By Hensel's lemma: lift to $f(X) = g(X)h(X)$, $\deg(g) = r$.
So, nontrivial factorisation ✗

---

§5: Teichmüller Lifts.

[DEF 5.1] ring R, $\mathrm{char} = p > 0$, is perfect if $x \mapsto x^p$ is a bijection. A field F is perfect field if perfect as ring.

[Remark] Since $\mathrm{char}(R) = p$: $(x+y)^p = x^p + y^p$, so Frobenius map is a ring hom.

[Example] i) $\mathbb{F}_{p^n}$ & $\overline{\mathbb{F}_p}$ are perfect.
ii) $\mathbb{F}_p[t]$ not perfect: since t has no p^{th} root.
iii) $\mathbb{F}_p(t^{\frac{1}{p}}, t^{\frac{1}{p^2}}, \dots) \equiv \mathbb{F}_p(t^{1/p^\infty})$ is perfect.
Is called: perfection of $\mathbb{F}_p(t)$.

Fact: field K, $\mathrm{char}(K) = p > 0$ perfect iff: any finite extension L/K is separable.

Theorem 5.2 $(K, |\cdot|)$ complete, DVF, s.t. $k \equiv \mathcal{O}_K / m$ is perfect field, char p. Then: $\exists!$ map $[\,]: k \to \mathcal{O}_K$:

i) $a \equiv [a] \bmod m \quad \forall a \in k$

ii) $[ab] = [a] \cdot [b] \quad \forall a, b \in k$

Moreover: if $\mathrm{char}(\mathcal{O}_K) = p$ then $[-]$ is ring hom, i.e.

$[a+b] = [a] + [b]$. $\forall a, b \in k$.

DEF 5.3 $[a] \in \mathcal{O}_K$ is Teichmüller Lift. of a.

Lemma 5.4 $(K, |\cdot|)$ as before. & $\pi \in \mathcal{O}_K$ uniformizer.

Let: $x, y \in \mathcal{O}_K$ s.t. $x \equiv y \bmod \pi^k$, $k \geq 1$. Then $x^p \equiv y^p \bmod \pi^{k+1}$.

Proof write: $x = y + u \cdot \pi^k$ $(u \in \mathcal{O}_K)$. Then: $x^p = (y + u\pi^k)^p$

$$= \sum_{i \leq p} \binom{p}{i} y^{p-i} (u \cdot \pi^k)^i$$

Since $\mathcal{O}_K / \pi \mathcal{O}_K$ has char $= p$: have, $p \in \pi \mathcal{O}_K$. So, indeed, get $x^p \equiv y^p \bmod \pi^{k+1}$ ✓

Proof of **Theorem 5.2**

For $a \in k$: for each $i \geq 0$, choose lift $y_i \in \mathcal{O}_K$ of a^{1/p^i}, and define: $x_i = y_i^{p^i}$. Claim that: (x_i) Cauchy, so $x_i \longrightarrow x$, and x indep. of choice of y_i.

Indeed: for Cauchy, have: $y_i \equiv y_{i+1}^p \bmod \pi$.

$\Rightarrow y_i^{p^k} = y_{i+1}^{p^{k+1}} \bmod \pi^{k+1}$. (induction + prev lemma)

$\Rightarrow x_i \equiv x_{i+1} \bmod \pi^{i+1}$. ✓

So, $\exists x$, $x_i \to x \in \mathcal{O}_K$.

Independence: if (x_i') arises from another choice of y_i', and: $x_i' \to x' \in \mathcal{O}_K$.

If $x_i'' = \begin{cases} x_i, & i \text{ even} \\ x_i', & i \text{ odd} \end{cases}$ from: $y_i'' = \begin{cases} y_i, & i \text{ even} \\ y_i', & i \text{ odd.} \end{cases}$

So, x_i'' Cauchy, so $\exists x''$, $x_i'' \to x''$.

But: by uniqueness of limits, $x'' = x$ & $x'' = x'$ ✓

Define: $[a] \equiv x$.

⊛ $x_i \equiv y_i^{p^i} \equiv (a^{\frac{1}{p^i}})^{p^i} \equiv a \mod \pi \Rightarrow x \equiv a \mod \pi$

⊛ If $b \in k$ & $[b] \equiv y$ (by choosing $u_i \in \mathcal{O}_K$ lifts of b^{1/p^i}, and $z_i \equiv u_i^{p^i}$.)

Then: $u_i \cdot y_i$ is lift. of $(ub)^{p^i}$, so $[ab] = \lim_{i\to\infty} x_i z_i$

$= (\lim x_i)(\lim z_i) = [a][b]$ ✓

⊛ If $\mathrm{char}(k) = p$ as well: $u_i + y_i$ is lift. of $a^{\frac{1}{p^i}} + b^{\frac{1}{p^i}}$

$= (a+b)^{1/p^i}$

So: $[a+b] = \lim_{i\to\infty} (y_i + u_i)^{p^i} = \lim_{i\to\infty} (y_i^{p^i} + u_i^{p^i})$

$= [a] + [b]$ ✓

Easy to check: $[0] = 0$, $[1] = 1$, so $[\cdot]$ is ring hom.

Uniqueness: Suppose $\phi: k \to \mathcal{O}_K$ another such map, multiplicative.

Then, $\phi(a^{\frac{1}{p^i}})$ is lift. of $a^{\frac{1}{p^i}}$. So, $[a] = \lim \phi(a^{\frac{1}{p^i}})^{p^i}$

$= \lim \phi(a) = \phi(a)$ ✓ □3

Examples] $K = \mathbb{Q}_p$. $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$.

For $a \in \mathbb{F}_p^\times$: $[a]^{p-1} = [a^{p-1}] = [1] = 1$.

$\Rightarrow$ $[a]$ is $(p-1)^{\text{st}}$ th root of unity.

More generally:

Lemma 5.6] $(K, |\cdot|)$ complete DVF. If $k \subseteq \overline{\mathbb{F}_p}$, then $[a] \in \mathcal{O}_K^\times$ is root of unity. $\forall a \in k^\times$.

Proof] For $a \in k^\times$: have, $a \in \mathbb{F}_{p^n}$, some n. Then:

$[a]^{p^n-1} = [a^{p^n-1}] = 1$, so root of unity.

Theorem 5.7] $(K, |\cdot|)$ complete DVF, $\mathrm{char}(K) = p > 0$.

Assume k perfect. Then $K \cong k((t))$.

Proof] Know: $K = \mathrm{FF}(\mathcal{O}_K)$. So, suffices to show: $\mathcal{O}_K \cong k[\![t]\!]$.

Fix: $\pi \in \mathcal{O}_K$ uniformizer, and $[\cdot] : k \to \mathcal{O}_K$ Teichmuller map

& define $\varphi : k[\![t]\!] \to \mathcal{O}_K$

$$\varphi\left(\sum a_i t^i\right) = \sum [a_i] \pi^i.$$

Since $[\cdot]$ ring hom, have φ ring hom, but also, is a bijection (since elements can be expressed uniquely in this way) ✓

Local Fields. [lecture 6]

§6: Extensions of complete value fields.

Theorem 6.1 $(K, |\cdot|)$ complete DVF & L/K finite ext. of degree $[L:K]=n$.

i) $|\cdot|$ extends uniquely to $|\cdot|_L$ on L, defined by $|y|_L \equiv |N_{L/K}(y)|^{\frac{1}{n}}$

ii) $(L, |\cdot|_L)$ complete.

Recall: L/K finite $\Rightarrow N_{L/K} : L \to K$ defined by $N_{L/K}(y) \equiv \det_K(m_y)$, where $m_y : L \to L$, induced by mult. by y.

Facts: ⊛ $N_{L/K}(xy) = N_{L/K}(x) \cdot N_{L/K}(y)$

⊛ Let: $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ min poly of $y \in L$. Then, $N_{L/K}(y) = \pm a_0^m$, for some $m \geq 1$.

⊛ $N_{L/K}(y) = 0 \Leftrightarrow y = 0$.

DEF 6.2 $(K, |\cdot|)$ non-Archimedean valued field, and V vector space over K. A norm is $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ with:

i) $\|x\| = 0 \Leftrightarrow x = 0$

ii) $\|\lambda x\| = |\lambda| \cdot \|x\|$. $(\forall x \in V, \lambda \in K)$

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

Example (Sup norm): if V f.d. & basis $e_1, \ldots, e_n$ for V:

then $\|\cdot\|_{sup}$ on V defined by $\|\sum x_i e_i\|_{sup} = \max |x_i|$.

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

DEF 6.3 Two norms $\|\cdot\|_1$, $\|\cdot\|_2$ on V are equivalent if
$\exists C, D > 0$ s.t. $C\|x\|_1 \leq \|x\|_2 \leq D\|x\|_1 \quad \forall x \in V$.

Fact: Defines topology on V by $d(x,y) \equiv \|x-y\|$.
& Equivalent norms deduce same topology.

Prop 6.4 $(K, |\cdot|)$ complete non-Arch, & V f.d. VS/K.
Then V is complete WRT topology of sup norm.

Proof let $(v_n)_{n\in\mathbb{N}}$ Cauchy sequence on V, and $\{e_i\}$ basis of V.
Write: $v_i \equiv \sum_{1\leq j\leq n} x_j^i e_j$. Then: $(x_j^i)_{i\in\mathbb{N}}$ is Cauchy, so
$\exists x_j$ with $x_j^i \longrightarrow x_j$ in K.
Then, $v_j \longrightarrow v \equiv \sum x_j e_j$ in V. ✓

Theorem 6.5 $(K, |\cdot|)$ complete, non-Arch & V f.d. VS/K.
Then, any 2 norms on V are equivalent.
In particular: V is complete WRT any norm.

Proof Suffices to show: any norm equivalent to Sup norm.
Fix: basis $\{e_i\}$ of V/K.
(*) Upper bound: set $D \equiv \max \|e_i\|$. Then,

$\|x\| = \|\sum_i x_i e_i\| \le \max \|x_i e_i\| = \max |x_i| \|e_i\| \le D \|x\|_{sup}$.

For lower bound: use induction on n.

- $n=1$: $C = \|e_1\|$, since: $\|x\| = \|x_1 e_1\| = \|x\|_{sup} \|e_1\|$.
- $n>1$: set $V_i \equiv \text{span}(e_1, \dots, \widehat{e_i}, \dots, e_n)$ $\forall i$.

By induction: V_i complete WRT $\|\cdot\|$, hence closed.

$\Rightarrow e_i + V_i$ closed $\forall i$, hence $S \equiv \bigcup e_i + V_i$ closed, and does not contain 0. So, $\exists C>0$, s.t. $S \cap B(0,C) = \emptyset$.

For $x = \sum x_i e_i \neq 0$: if $|x_i| = \max |x_j|$, then $\|x\|_{sup} = |x_i|$ and $\frac{1}{x_i} \cdot x \in S$. So, $\|\frac{1}{x_i} x\| \ge C \Rightarrow \|x\| \le C \|x\|_{sup}$ ✓

For completeness: V complete since complete WRT sup norm.

Proof of Theorem 6.1

Will show: $|\cdot|_L \equiv |N_{L/K}(\cdot)|^{\frac{1}{n}}$ has the 3 props of abs val.

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

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

$= |y_1|_L \cdot |y_2|_L$.

iii) Need to do more work.

DEF 6.6] $R \subseteq S$ rings. Say $s \in S$ integral if $\exists f \in R[X]$ monic, with $f(s) = 0$.

& Integral closure $R^{\text{int}(S)} \equiv \{s \in S : s \text{ integral over } R\}$.

& R integrally closed in $S \iff R^{int(S)} = R$

Prop 6.7] $R^{int(S)}$ is subring of S & integrally closed in S

Lemma 6.8] $(K, |\cdot|)$ non-Arch valued field. Then: $\mathcal{O}_K$ integrally closed in K.

Proof) let $x \in K$ integral over $\mathcal{O}_K$. & assume $x \neq 0$.

Let: $f(X) \equiv X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathcal{O}_K[X]$ with $f(x) = 0$.

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

If $|x| > 1$: then $1 < |x| \leq \max(|a_{n-1}|, \dots, |a_0 \frac{1}{x^{n-1}}|) \leq 1$ ✗

$\Rightarrow$ hence, $|x| \leq 1$, so $x \in \mathcal{O}_K$ ✓

6.1 iii)] set $\mathcal{O}_L \equiv \{y \in L : |y|_L \leq 1\}$.

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

(will prove next time). In particular: $\mathcal{O}_L$ is a subring of L.

If $x, y \in L$: WLOG $|x|_L \leq |y|_L$. Then $|\frac{x}{y}|_L \leq 1$, so $\frac{x}{y} \in \mathcal{O}_L$.

Since $\mathcal{O}_L$ ring: $1 \in \mathcal{O}_L$, & closed under $+$, so $1 + \frac{x}{y} \in \mathcal{O}_L$.

$\Rightarrow |1 + \frac{x}{y}|_L \leq 1$, so $|x+y|_L \leq |y|_L = \max(|x|_L, |y|_L)$ ✓

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

Local Fields: lecture 7

Proof Set $y \in L$, $y \neq 0$ & $f(x) \equiv x^d + a_{d-1}x^{d-1} + \dots + a_0 \in K[x]$ minimal monic poly for y.

Claim y integral / $\mathcal{O}_K \iff f(x) \in \mathcal{O}_K[x]$

$\Leftarrow$: Obvious.

$\Rightarrow$: Find $g(x) \in \mathcal{O}_K[x]$ monic, $g(y)=0$. Then $f \mid g$ in $K(x)$, so every root of f is a root of g.

$\Rightarrow$ Every root of f in $\bar{K}$ is integral over $\mathcal{O}_K$

$\Rightarrow a_i$ integral over $\mathcal{O}_K$, $0 \leq i \leq d$. Hence $a_i \in \mathcal{O}_K$ $\forall i$. ✓

By Corollary ~~4.5~~ : Since f irred: $|a_i| \leq \max(|a_0|, \underbrace{|a_d|}_{=1})$

By properties of $N_{L/K}$: $N_{L/K}(y) = \pm a_0^m \in \mathcal{O}_K$.

So, $y \in \mathcal{O}_L \iff |N_{L/K}(y)| \leq 1 \iff |a_0| \leq 1 \iff |a_i| \leq 1 \ \forall i$
$\iff a_i \in \mathcal{O}_K$. ✓

Hence: $|y|_L$ defines an abs val. on L.

Since $|N_{L/K}(x)| = x^n$ $\forall x \in K$: $|y|_L$ extends $|\cdot|$.

Uniqueness (Theorem 6.1): if $|\cdot|_L, |\cdot|_L'$ are 2 abs vals extending $|\cdot|$, then by Theorem 6.5: they are equivalent.

By Prop 1.3: $\exists c$, $|\cdot|_L^c = |\cdot|_L'$.

Since both extend $|\cdot|$: get $c=1$ (absolute value nontrivial) ✓

Completeness (Theorem 6.1): have L complete WRT $|\cdot|_L$. ✓

Corollary 6.10 $(K, |\cdot|)$ complete non-Arch discretely valued field, & L/K finite ext. Then:

i) L is discretely valued WRT $|\cdot|_L$

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

Proof i) fix valuation v on K, and v_L valuation that extends v. & $n \equiv [L:K]$.

Then for $y \in L^\times$: $|y|_L = |N_{L/K}(y)|^{\frac{1}{n}}$ ~~$\Rightarrow \log|y|_L = \frac{1}{n}\log|N_{L/K}(y)|$~~

$\Rightarrow v_L(y) = \frac{1}{n} v(N_{L/K}(y))$.

$\Rightarrow v_L(L^\times) \subseteq \frac{1}{n} v(K^\times)$, discrete. So, v_L discrete.

ii) Proved in Lemma 6.9.

Corollary 6.11 $\bar{K}/K$ algebraic closure of K. Then, $|\cdot|_K$ extends uniquely to an absolute value $|\cdot|_{\bar{K}}$ on $\bar{K}$.

Proof For $x \in \bar{K}$, $\exists L/K$ finite ext, s.t. $x \in L$. Then, define $|x|_{\bar{K}} \equiv |x|_L$.

By uniqueness of extension (Theorem 6.9): $|\cdot|_{\bar{K}}$ well-defd & Axioms for absolute value hold at finite level.

Uniqueness is obvious.

Remark $|\cdot|_{\bar{K}}$ never discrete. on $\bar{K}$. (In contrast of finite case)

E.g. can check in roots of uniformizer.

When $K = \mathbb{Q}_p$: $\sqrt[n]{p} \in \mathbb{Q}_p$ $\forall n$, and $v_p(\sqrt[n]{p}) = \frac{1}{n}$

$\square$

Also: $\overline{\mathbb{Q}}_p$ not complete WRT $|\cdot|_{\overline{\mathbb{Q}}_p}$.
The completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}}_p$ WRT this abs value is algebraically closed.

Prop 6.12) L/K finite ext, of discretely valued fields.
Assume: $\mathcal{O}_K$ (1) compact & k_L/k extension of residue fields is finite & separable. (2)
Then: $\exists \alpha \in \mathcal{O}_L$ with $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.
(Later: (1) $\Rightarrow$ (2).)

Proof Choose $\alpha \in \mathcal{O}_L$ with:
* $\exists \beta \in \mathcal{O}_K[\alpha]$, uniformizer for $\mathcal{O}_L$
* The map $\mathcal{O}_K[\alpha] \longrightarrow k_L$ surjective.

Since k_L/k separable: $\exists \bar{\alpha} \in k_L$ with $k_L = k(\bar{\alpha})$ (primitive element)
Let: $\alpha \in \mathcal{O}_L$ any lift of $\bar{\alpha}$, and $g(x) \in \mathcal{O}_K(x)$ some monic lift of min poly of $\bar{\alpha}$.
& $\pi_L \in \mathcal{O}_L$ some uniformizer.
Then: $\bar{g}(x) \in k[x]$ irred & separable (min poly of $\bar{\alpha}$)
$\Rightarrow \bar{\alpha}$ is simple root of $\bar{g}$
$\Rightarrow g(\alpha) \equiv 0 \bmod \pi_L$ & $g'(\alpha) \not\equiv 0 \bmod \pi_L$.
If $g(\alpha) \equiv 0 \bmod \pi_L^2$ then $g(\alpha + \pi_L) \equiv g(\alpha) + \pi_L g'(\alpha) \not\equiv 0 \bmod \pi_L^2$
~~$\Rightarrow$ Either α or $\alpha + \pi_L$~~ ~~###~~.
$\Rightarrow$ Either $v_L(g(\alpha)) = 1$ or $v_L(g(\alpha + \pi_L)) = 1$.

So, by replacing, WLOG assume $v_L(g(\alpha)) = 1$.

Set: $\beta \equiv g(\alpha) \in \mathcal{O}_K[\alpha]$, uniformizer. ↗

Then: $\mathcal{O}_K[\alpha] \subseteq L$ is image of the continuous map

$$\mathcal{O}_K^n \longrightarrow L, \quad (x_0, \dots, x_{n-1}) \longmapsto \sum x_i \cdot \alpha^i$$

Since $\mathcal{O}_K$ compact: $\mathcal{O}_K[\alpha]$ also compact $\Rightarrow$ closed.

Since $k_L = k(\bar{\alpha})$: $\mathcal{O}_K[\alpha]$ contains set of coset reps for $k_L \equiv \mathcal{O}_L / \beta \mathcal{O}_L$.

For $y \in \mathcal{O}_L$: by prop 3.5: $y = \sum_{i \in \mathbb{N}} \lambda_i \beta^i$, for $\lambda_i \in \mathcal{O}_K[\bar{\alpha}]$

$\Rightarrow \forall m \; y_m \equiv \sum_{i \leq m} \lambda_i \beta^i \in \mathcal{O}_K[\alpha]$.

$\Rightarrow y \in \mathcal{O}_K[\alpha]$, since $\mathcal{O}_K[\alpha]$ closed ✓

III: Local Fields.

DEF 7.1] $(K, |\cdot|)$ valued field. Say K local field if complete & locally compact (any pt has compact nbhood).

Prop 7.2]: $(K, |\cdot|)$ non-Arch, complete valued field. TFAE:

i) K ~~compact~~ locally compact

ii) $\mathcal{O}_K$ compact

iii) v discrete & $k \equiv \mathcal{O}_K / m$ finite.

Local Fields: lecture 8

Proof of Prop 7.2 i) $\Rightarrow$ ii): Find compact nbhood $U \ni 0$.
(i.e. $0 \in U \subseteq K$ compact).
$\Rightarrow \exists x \in \mathcal{O}_K$ s.t. $x\mathcal{O}_K \subseteq U$ (choose $|x|$ small enough)
Since $x\mathcal{O}_K$ closed $\Rightarrow x\mathcal{O}_K$ compact $\Rightarrow \mathcal{O}_K$ compact
(since $\mathcal{O}_K \xrightarrow[\text{homeo}]{\cong} x\mathcal{O}_K$ (homeo) by mult. by x map).

ii) $\Rightarrow$ i): $\mathcal{O}_K$ compact $\Rightarrow a + \mathcal{O}_K$ compact. $\forall a \in K$.
So, K locally compact ✓

ii) $\Rightarrow$ iii): let $x \in m$ & $A_x \subseteq \mathcal{O}_K$ coset reps, of $\mathcal{O}_K / x\mathcal{O}_K$. Then: $\mathcal{O}_K = \bigcup_{y \in A_x} y + x\mathcal{O}_K$, and is disjoint open cover.

So, by compactness: finite subcover $\Rightarrow A_x$ finite.
$\Rightarrow \mathcal{O}_K / x\mathcal{O}_K$ finite, and so $\mathcal{O}_K / m\mathcal{O}_K$ finite.

If v not discrete: pick $X = x_1, x_2, \ldots$ such that $v(x_i) > 0$ & strictly decreasing. $v(x_1) > v(x_2) > \ldots$
Then: $x\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq \ldots \subsetneq \mathcal{O}_K$.
But: $\forall x_i$, $\mathcal{O}_K / x\mathcal{O}_K$ finite, so only finitely many subgroups. #

iii) $\Rightarrow$ ii): Will prove $\mathcal{O}_K$ sequentially compact (since metric space).
Pick $(x_n)_{n \in \mathbb{N}}$ sequence in $\mathcal{O}_K$. & $\pi \in \mathcal{O}_K$ uniformizer.
Know: $\pi^i \mathcal{O}_K / \pi^{i+1} \mathcal{O}_K \cong k$: get $\mathcal{O}_K / \pi^i \mathcal{O}_K$ finite $\forall i$.

Since $\mathcal{O}_K/\pi\mathcal{O}_K$ finite: $\exists a_1 \in \mathcal{O}_K/\pi\mathcal{O}_K$ and subsequence $(x_{1n})_{n\in\mathbb{N}} \subseteq (x_n)_{n\in\mathbb{N}}$ s.t. $x_{1n} \equiv a_1 \bmod \pi$.

Since $\mathcal{O}_K/\pi^2\mathcal{O}_K$ finite: $\exists a_2 \in \mathcal{O}_K/\pi^2\mathcal{O}_K$ & subseq $(x_{2n})_{n\in\mathbb{N}} \subseteq (x_{1n})_{n\in\mathbb{N}}$ s.t. $x_{2n} \equiv a_2 \bmod \pi^2$

So, get (x_{in}) sequences, $i=1,2,\dots$ with:

- $(x_{in}) \supseteq (x_{i+1,n})$ $\forall i$
- $x_{in} \equiv a_i \bmod \pi^i$

So: $a_{i+1} \equiv a_i \bmod \pi^i$, and so $\exists a \in \mathcal{O}_K$, $a_i \to a$.

If $y_i \equiv x_{ii}$: then $(y_i) \subseteq (x_i)$ & $y_i \equiv a_i \bmod \pi^i$, hence $y_i \to a$ ✓

Examples of Local Fields

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

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

More on Inverse Limits.

Let $(A_n)_{n\in\mathbb{N}}$ sets, ~~finite~~ and homs $\varphi_n : A_{n+1} \to A_n$.

DEF 7.3] If A_n finite $\forall n$, then Profinite Topology on $\varprojlim_n A_n$ is defined as weakest topology s.t. $\theta_n : A \to A_n$ continuous $\forall n$.

(where: A_n discrete topology $\forall n$).

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

Prop 7.4 K non-Arch, Local field. Under the isom. $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$, ($\pi \in \mathcal{O}_K$ uniformizer):

the topology on $\mathcal{O}_K$ coincides with profinite topology.

Proof Let: $\mathcal{B} \equiv \{a + \pi^n\mathcal{O}_K : n \geq 1 \;\&\; a \in \mathcal{O}_K\}$.

Check: $\mathcal{B}$ is a basis of open sets, in both topologies.

⊛ For 1-1: obvious.

⊕ For profinite: have; $\mathcal{O}_K \longrightarrow \mathcal{O}_K/\pi^n\mathcal{O}_K$ continuous iff $a + \pi^n\mathcal{O}_K$ open $\forall a \in \mathcal{O}_K$ ✓ (by pre-image.)

Lemma 7.5 K non-Arch Local Field & L/K finite.

Then: L local field.

Proof By Theorem 6.1: L complete & discretely valued.

Suffices to show: $k_L = \mathcal{O}_L/\mathfrak{m}_L$ finite.

Let: $\alpha_1, \ldots, \alpha_n$ basis for L/K (as vector space). Since $\|\cdot\|_{sup}$ equiv to $\|\cdot\|_L$: $\exists r > 0$, $\mathcal{O}_L \subseteq \{x \in L : \|x\|_{sup} \leq r\}$.

Then $\forall a \in K$ with $|a| \geq r$: then $\mathcal{O}_L \subseteq \bigoplus_{1 \leq i \leq n} a\alpha_i\mathcal{O}_K \subseteq L$.

$\Rightarrow \mathcal{O}_L$ fin-gen as module over $\mathcal{O}_K$

$\Rightarrow k_L$ fin-gen over k ✓

DEF 7.7 $(K, |\cdot|)$ non-Arch, Local field. Has: equal characteristic if $\mathrm{Char}(K) = \mathrm{char}(k)$. Otherwise: mixed characteristic.

E.g. $\mathbb{Q}_p$ has mixed char.

Theorem 7.8 K non-Arch local field, equal char $= p > 0$.
Then: $K \cong \mathbb{F}_{p^n}((t))$, for some $n \geq 1$.

Proof K is: complete & discretely valued, and $\mathrm{char}(k) > 0$.
Moreover: $k \cong \mathbb{F}_{p^n}$ finite $\Rightarrow$ hence perfect.
By Theorem 5.7: $K \cong \mathbb{F}_{p^n}((t))$.

Theorem 7.9 An absolute value $|\cdot|$ on a field K is non-Archimedean iff $|n|$ bounded ($n \in \mathbb{Z}$).

Proof $\Rightarrow$: $|n| = |1 + \cdots + 1| \leq |1| \ \forall n \geq 1$, and $|-n| = |n| \leq |1|$.
$\Leftarrow$: Say $|n| \leq \beta \ \forall n \in \mathbb{Z}$.
For $x, y \in K$, with $|x| \leq |y|$, $|x+y|^m = \left|\sum \binom{m}{i} x^i y^{m-i}\right|$
$\leq \sum_{i=0}^{m} \left|\binom{m}{i}\right| |x|^i |y|^{m-i} \leq \beta(m+1)\,|y|^m$.
$\Rightarrow |x+y| \leq |y| \cdot (\beta(m+1))^{\frac{1}{m}} \ \forall m \in \mathbb{N}$.
$\Rightarrow |x+y| \leq |y| = \max(|x|, |y|)$. ✓

Local Fields: Lecture 9

Theorem 7.10 (Ostrowski's Theorem)
Any (nontrivial) abs val on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ or $|\cdot|_p$, p prime.

Proof Case 1: $|\cdot|$ Archimedean.
Fix: $b > 1$ integer, s.t. $|b| > 1$ (by lemma 7.9)
& $a > 1$ integer, and write: $b^n = c_m a^m + c_{m-1} a^{m-1} + \cdots + c_0$,
for $0 \le c_i < a$ & $c_m \neq 0$.
& $B \equiv \max_{0 \le c \le a} (|c|)$.

$\Rightarrow |b^n| \le (m+1) B \max(|a|^m, 1)$

$\Rightarrow |b| \le \underbrace{\left[B(n \log_a(b) + 1)\right]^{\frac{1}{n}}}_{\to 1} \max(e |a|^{\log_a(b)}, 1)$

$\Rightarrow |b| \le \max(|a|^{\log_a(b)}, 1)$.

Then: if $|a| > 1$, then $|b| \le |a|^{\log_a(b)}$.] $\Rightarrow \frac{\log|a|}{\log a} = \frac{\log|b|}{\log b}$

Switch a, b $\Rightarrow$ get: $|a| \le |b|^{\log_b(a)}$.

$\Rightarrow \exists \lambda > 0$, s.t. $|a| = a^\lambda \ \forall a \in \mathbb{Z}_{>1}$.

$\Rightarrow |x| = x^\lambda \ \forall x \in \mathbb{Q}$, so $|\cdot|$ equivalent to $|\cdot|_\infty$.

Case 2: $|\cdot|$ non-Archimedean.
By lemma 7.9: $|n| \le 1 \ \forall n \in \mathbb{Z}$, & since $|\cdot|$ non-trivial, $\exists n > 1$, with $|n| < 1$.

□

So, if $n = \pi p_i^{e_i} \Rightarrow \exists p \in \{p_i\}$ s.t. $|p| < 1$

If $\exists q \neq p$, $|q| < 1$, then $\exists r, s \in \mathbb{Z}$, $1 = rp + sq$.

$\Rightarrow 1 = |rp + sq| \leq \max(|rp|, |sq|) < 1$ #.

So, $|p| = \alpha < 1$ & $|q| = 1$ $\forall q \neq p$ prime.

$\Rightarrow |\cdot|$ equivalent to $|\cdot|_p$.

Theorem 7.11 $(K, |\cdot|)$ non-Arch local field, mixed char.

Then: K finite ext of $\mathbb{Q}_p$.

Proof Mixed char $\Rightarrow$ Char $(K) = 0$. $\Rightarrow \mathbb{Q} \subseteq K$.

K non-Arch $\Rightarrow |\cdot|_{\mathbb{Q}} \sim |\cdot|_p$, some p

K complete $\Rightarrow \mathbb{Q}_p \subseteq K$.

Suffices to show: $\mathcal{O}_K$ finite as $\mathbb{Z}_p$-module.

Find: $\pi \in \mathcal{O}_K$ uniformizer, and v normalized val. on K.

$\Rightarrow$ If $v(p) = e$, then $\mathcal{O}_K / p\mathcal{O}_K \cong \mathcal{O}_K / \pi^e \mathcal{O}_K$,

finite (since $\pi^i \mathcal{O}_K / \pi^{i+1} \mathcal{O}_K \cong k$ finite)

Since $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K / p\mathcal{O}_K$, see: $\mathcal{O}_K / p\mathcal{O}_K$ is a finite-dimensional $\mathbb{F}_p$-vector space.

Let: $x_1, \ldots, x_n \in \mathcal{O}_K$ coset reps. for $\mathbb{F}_p$-basis of $\mathcal{O}_K / p\mathcal{O}_K$ (lift of a basis)

$\Rightarrow \left\{ \sum a_j x_j : a_j \in \{0, \ldots, p-1\} \right\}$ is: set of coset reps, for quotient $\mathcal{O}_K / p\mathcal{O}_K$.

$\square$

Let: $y \in \mathcal{O}_K$, then by prop 3.5: $y = \sum_{i \in \mathbb{N}_0} \left(\sum_{j \le n} a_{ij} x_j \right) p^i$

$= \sum_{j \le n} \left(\underbrace{\sum_i a_{ij} p^i}_{\in \mathbb{Z}_p} \right) x_j$ is linear comb. of elements of $\mathbb{Z}_p$.

$\Rightarrow \mathcal{O}_K$ finite / $\mathbb{Z}_p$ ✓

From sheet 2: if K complete Archimedean, then $K \cong \mathbb{R}, \mathbb{C}$.

Summary: if K local field, either:

- $K \cong \mathbb{R}, \mathbb{C}$ (Archimedean)
- $K \cong \mathbb{F}_{p^n}((t))$ (non-Arch) + equal char.
- K finite ext. of $\mathbb{Q}_p$ (non-Arch & mixed char)

§8: Global Fields.

DEF 8.1 Global field is either:

1) Algebraic number field
2) Global function field. (finite ext. of $\mathbb{F}_p(t)$)

Lemma 8.2 $(K, |\cdot|)$ Complete, Discretely valued field, L/K finite ext. (Galois ext) with abs val $|\cdot|_L$.

Then: $\forall x \in L, \sigma \in \mathrm{Gal}(L/K)$: $|\sigma(x)|_L = |x|_L$.

Proof $x \mapsto |\sigma(x)|_L$ is an abs val on L extending $|\cdot|$, so result follows by uniqueness of extension.

Lemma 8.3 (Krasner's Lemma)

$(K, |\cdot|)$ complete ~~discretely~~ valued field (Non-Arch)
& $f(X) \in K[X]$ separable irred poly, roots $\alpha_1, \dots, \alpha_n \in \bar{K}$.
Suppose $\beta \in \bar{K}$, $|\beta - \alpha_1| < |\beta - \alpha_i| \ \forall i \geq 2$.
Then: $\alpha_1 \in K(\beta)$.

Proof let $L = K(\beta)$ & $L' = L(\alpha_1, \dots, \alpha_n)$ splitting field,
so L'/L is Galois. If $\sigma \in \mathrm{Gal}(L'/L)$:
$|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1|$. (lemma above)
$\Rightarrow$ must have $\sigma(\alpha_1) = \alpha_1$. (since ineq) so $\alpha_1 \in K(\beta)$.

Prop 8.4) $(K, |\cdot|)$ complete, Discretely valued.
$f(X) = \sum_{i=0}^{n} a_i X^i \in \mathcal{O}_K[X]$ separable, irred monic poly.
& $\alpha \in \bar{K}$, root of f.
Then: $\exists \varepsilon > 0$: $\forall g(X) = \sum_{i=0}^{n} b_i X^i \in \mathcal{O}_K[X]$, monic and
$|\alpha_i - \beta_i| < \varepsilon \ \forall i$, $\exists \beta$ root of g s.t. $K(\alpha) = K(\beta)$.
("Nearby polys define same ext.")

Proof $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n \in \bar{K}$ roots of f, distinct.
Choose ε small s.t. $|g(\alpha_1)| < |f'(\alpha_1)|^2$ & $|f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha_1)|$
$\Rightarrow |g(\alpha_1)| < |f'(\alpha_1)|^2 = |g'(\alpha_1)|^2$.
Hensel's lemma to field $K(\alpha_1)$: $\exists \beta \in K(\alpha_1)$, s.t. β
root of g & $|\beta - \alpha_1| < |g'(\alpha_1)| = |f'(\alpha_1)| = \prod_{i=2}^{n} |\alpha_1 - \alpha_i| \leq |\alpha_i - \alpha_i| = |\beta - \alpha_i|$
$\Rightarrow \alpha \in K(\beta)$ (Kronecker), so $K(\alpha) = K(\beta)$.

Local Fields: lecture 10

Theorem 8.5 | K local field $\Rightarrow$ K is completion of some global field.

Proof

* 1-1 Archimedean: $\mathbb{R}, \mathbb{C}$ completion of $\mathbb{Q}$, $\mathbb{Q}(i)$ WRT $|\cdot|_\infty$
* 1-1 non-Archimedean, equal char: $\Rightarrow K \cong \mathbb{F}_q((t))$, and is completion of $\mathbb{F}_q(t)$ WRT t-adic abs val.
* 1-1 non-Arch, mixed char: $K = \mathbb{Q}_p(\alpha)$, α root of monic irred $f(X) \in \mathbb{Z}_p[X]$.

Since $\mathbb{Z} \subseteq \mathbb{Z}_p$ dense: choose: $g(X) \in \mathbb{Z}[X]$ as in Prop 8.4.

$\Rightarrow K = \mathbb{Q}_p(\beta)$, β root of $g(X)$.

Then: $\mathbb{Q}(\beta) \subseteq \mathbb{Q}_p(\beta)$ dense (since consider as vector space.)

$\Rightarrow K$ completion of $\mathbb{Q}(\beta)$ ✓

IV: Dedekind Domains.)

DEF 9.1 | Dedekind domain is ring R s.t.

* Noetherian, integral domain
* R integrally closed in $FF(R)$: $\forall$
* Every nonzero prime ideal is maximal

Examples Ring of integers of number field is Dedekind.

& Any PID (hence DVR) is Dedekind.

Theorem 9.2 | R ring. Then: R DVR $\Leftrightarrow$ Dedekind + exactly 1 nonzero prime ideal.

Lemma 9.3 | R Noeth, $I \subseteq R$ nonzero.

Then: $\exists$ nonzero prime $P_1, \dots, P_r \in R$ s.t. $P_1 \cdots P_r \subseteq I$.

Proof If not: since R Noeth, choose I maximal with this property. Then: I not prime $\Rightarrow \exists x,y \in R\setminus I$, $xy \in I$.
$\Rightarrow$ If $I_1 \equiv I + (x)$ & $I_2 \equiv I + (y)$, then by maximality of I, have $\exists p_1, \dots, p_r, q_1, \dots, q_s$ prime s.t. $p_1 \cdots p_r \subseteq I_1$, $q_1 \cdots q_s \subseteq I_2$
$\Rightarrow p_1 \cdots p_r q_1 \cdots q_s \subseteq I_1 I_2 \subseteq I$ ↯

lemma 9.4] R integral, integrally closed in $FF(R)$.
Then: if $0 \neq I \subseteq R$ ideal, fin-gen, and $x \in k$ with $xI \subseteq I$, then $x \in R$.

Proof Let $I_n \equiv (c_1, \dots, c_n)$ & $xc_i = \sum_j a_{ij} c_j$. ($a_{ij} \in R$)
& Let $A = (a_{ij})_{1 \le i,j \le n}$ matrix, and $B \equiv x\,Id_n - A$.
$\Rightarrow B \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$ in K^n.
$\Rightarrow \det(B) = 0$ (since: $\det(B) \cdot Id_n \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$)
But, $\det(B)$ is monic poly in x, with coeffs in R.
$\Rightarrow x$ integral over R, so $x \in R$ by integral closure.

Proof of Theorem 9.2

$\Rightarrow$: clear

$\Leftarrow$: Need R is PID.
By assumption: R local ring, unique maximal ideal m.

Step 1] m principal.
Let $0 \neq x \in m$. By lemma 9.3: $\exists n$, $m^n \subseteq (x)$.

Choose n minimal with this prop.

Then: pick $y \in m^{n-1} - (x)$.

Set $\pi \equiv x/y$. $\Rightarrow y m \subseteq m^n \subseteq (x) \Rightarrow \pi^{-1} m \subseteq R$.

If $\subsetneq$: then by maximality: $\pi^{-1} m \subseteq m$, so $\pi^{-1} \in R$ (lemma 9.4)

so $y \in (x)$ ##.

Hence: $\pi^{-1} m = R \Rightarrow m = \pi R = (\pi)$ principal.

Step 2: R is PID.

Let $I \subseteq R$ nonzero ideal & consider $I \subseteq \pi^{-1} I \subseteq \pi^{-2} I \subseteq \ldots$ in K.

Since $\pi^{-1} \notin R$: $\pi^{-k} I \neq \pi^{-k+1} I$ $\forall k$. (by lemma 9.4)

R noeth $\Rightarrow$ choose n maximal, s.t. $\pi^{-n} I \subseteq R$.

If $\pi^{-n} I \subseteq m = (\pi)$, then $\pi^{-(k+1)} I \subseteq R$ #

$\Rightarrow \pi^{-n} I = R$, hence $I = (\pi^n)$. ✓

Let R integral domain & $S \subseteq R$ multiplicatively closed subset (i.e. $\forall x, y \in S: xy \in S$). The localisation $S^{-1}R$ of R WRT S is: $S^{-1}R \equiv \left\{ \frac{r}{s} : r \in R, s \in S \right\} \subseteq FF(R)$.

& lies

Examples p prime ideal in $R \Rightarrow R \setminus p$ multiplicatively closed,

& $R_{(p)} \equiv$ localisation WRT $S \equiv R \setminus p$.

$p = 0$: $\Rightarrow R_{(0)} = Frac(R)$.

⊛ $R = \mathbb{Z}$, $p = (p)$: $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \not\equiv 0 \bmod p \right\}$.

Facts: ⊛ R noeth $\Rightarrow S^{-1}R$ noeth

⊛ $\exists$ bijection $\{\text{prime ideals in } S^{-1}R\} \longleftrightarrow \{\text{prime ideals } p \subseteq R, \text{ with } p \cap S = \emptyset\}$

$pS^{-1}R \longmapsto p$

Corollary 9.5 R Dedekind domain & $p \subseteq R$ nonzero prime ideal. Then $R_{(p)}$ is a DVR.

Proof By properties of Localisation: $R_{(p)}$ Noetherian integral domain. & has: unique nonzero prime ideal $pR_{(p)}$.

$\Rightarrow$ Suffices to show: $R_{(p)}$ integrally closed in $FF(R_{(p)}) = FF(R)$.

(since then, $R_{(p)}$ Dedekind $\overset{9.2}{\Rightarrow}$ DVR).

Let $x \in \text{Frac}(R)$ integral over $R_{(p)}$. Multiply denoms. of some poly satisfied by x.

$sx^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \quad (a_i \in R, s \in S)$.

Multiply s^{n-1}: $\Rightarrow xs$ integral over R.

$\Rightarrow xs \in R$. (R integrally closed)

$\Rightarrow x \in R_{(p)}$ ✓

Local Fields: lecture 11

DEF 9.6 R Dedekind domain & $p \subseteq R$ nonzero prime ideal.
Write: $v_p \equiv$ normalised valuation on $\mathrm{Frac}(R) \equiv \mathrm{Frac}(R_{(p)})$ corresponding to DVR $R_{(p)}$.

Examples $R = \mathbb{Z}$, $p = (p) \Rightarrow \mathbb{Z}_{(p)}$ & $v_p \equiv p$-adic val.

Theorem 9.7 R Dedekind, Then any $0 \neq I \subseteq R$ ideal is a unique product of prime ideals.

Remark Clear for PID's

Proof Quote following properties of localisation: (I, J ideals)

i) $IR_{(p)} = JR_{(p)}$ $\forall p$ prime ideal $\Rightarrow I = J$

ii) R Dedekind, $p_1 \neq p_2$ nonzero prime ideals. Then:

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

Let $I \subseteq R$ nonzero ideal. By lemma 9.3: $\exists$ distinct prime ideals $p_1, \dots, p_r$, with $p_1^{\beta_1} \cdots p_r^{\beta_r} \subset I$ ($\beta_i > 0$)

For $0 \neq p \subset R$, $p \notin \{p_i\}$ prime ideal: ii) $\Rightarrow p_i R_{(p)} = R_{(p)}$

$\Rightarrow I R_{(p)} = R_{(p)}$. ← DVR, max ideal.

By Corollary 9.5: $IR_{(p_i)} = (p_i R_{(p_i)})^{\alpha_i} = p_i^{\alpha_i} R_{(p_i)}$

for some $\alpha_i \in \mathbb{N}_0$ (in fact, $0 \leq \alpha_i \leq \beta_i$)

$\Rightarrow$ By i): $I = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

Uniqueness If $I = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_r^{\beta_r}$.

$\Rightarrow p_i^{\alpha_i} R_{(p_i)} = p_i^{\beta_i} R_{(p_i)}$ $\forall i \Rightarrow \alpha_i = \beta_i$ (by unique fact. in DUR's.)

---

§10: Dedekind Domains & Extensions.

Let: L/k finite ext. For $x \in L$: $Tr_{L/k}(x) \equiv$ trace of k-linear map $L \to L$, $y \mapsto xy$. (so $Tr_{L/k}(x) \in k$).

If L/k separable & degree n: & $\sigma_1, \dots, \sigma_n : L \to \bar{k}$ are set of embeddings: then, $Tr_{L/k}(x) \equiv \sum_{i \le n} \sigma_i(x)$.

Lemma 10.1 L/k finite separable ext. The symmetric bilinear form $(\cdot,\cdot) : L^2 \to k$, $(x,y) \mapsto Tr_{L/k}(xy)$, is non-degenerate. (Converse true too)

Proof L/k separable $\Rightarrow L = k(\alpha)$, some $\alpha \in L$.

Consider matrix A for $(\cdot,\cdot)$ in k-basis $\{1, \alpha, \dots, \alpha^{n-1}\}$.

Then: $A_{ij} = Tr_{L/k}(\alpha^{i+j}) = [BB^T]_{ij}$, where

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

$\Rightarrow \det(A) = \det(B)^2 = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$ (Vandermonde) $\neq 0$.

(by separability: $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ $\forall i \neq j$) ✓

Converse on Example sheet 3.

Theorem (0.2) $\mathcal{O}_K$ Dedekind & L/K $(K = FF(\mathcal{O}_K))$ is finite separable ext. Then: integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L is a Dedekind domain.

Proof Check the conditions:

* $\mathcal{O}_L \subseteq L \Rightarrow$ Integral domain.
* Noetherian: let $e_1, \dots, e_n \in L$ basis of L/K, and by scaling by k, assume $e_i \in \mathcal{O}_L$.

Let: $\{f_i\}$ dual basis of $\{e_i\}$ WRT $(\cdot,\cdot)$

Let: $x \in \mathcal{O}_L$, $x = \sum_{1 \le i \le n} \lambda_i f_i$ $(\lambda_i \in k)$. Then: $\lambda_i = Tr(x e_i) \in \mathcal{O}_K$.

[Because: $\forall z \in \mathcal{O}_L$, $Tr_{L/K}(z)$ is sum of elements of $\overline{K}$, which are integral over $\mathcal{O}_K$, so $Tr_{L/K}(z)$ integral over $\mathcal{O}_K$ and hence $Tr_{L/K}(z) \in \mathcal{O}_K$)

Thus: $\mathcal{O}_L \subseteq \mathcal{O}_K f_1 + \cdots + \mathcal{O}_K f_n \Rightarrow \mathcal{O}_L$ fin-gen as $\mathcal{O}_K$-module,

Since $\mathcal{O}_K$ noeth $\Rightarrow \mathcal{O}_L$ noeth (satisfies ACC)

* $\mathcal{O}_L$ integrally closed in L: ex sheet 2
* Every nonzero Prime $\mathfrak{p} \subseteq \mathcal{O}_L$ maximal:

Let $\mathfrak{P}$ nonzero prime ideal of $\mathcal{O}_L$, and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ prime ideal of $\mathcal{O}_K$.

For $0 \neq x \in \mathfrak{P}$: x integral $/\mathcal{O}_K \Rightarrow x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for some $a_i \in \mathcal{O}_K$.

WLOG: $a_0 \neq 0$. Then: $a_0 \in \mathfrak{P} \cap \mathcal{O}_K \Rightarrow \mathfrak{P} \neq \phi \Rightarrow \mathfrak{P}$ max.

Know: $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$, ~~both fields~~, & $\mathcal{O}_L$ finite / $\mathcal{O}_K$.

& $\mathcal{O}_L/\mathfrak{P}$ is fin-dim VS over $\mathcal{O}_K/\mathfrak{p}$

Since $\mathcal{O}_L/\mathfrak{P}$ is integral domain: is a field (e.g. by applying rank-nullity to $y \mapsto a_0 y$)

$\Rightarrow \mathfrak{P}$ maximal ✓

Remark Theorem 10.2 holds for L/K not separable.

[Only used separable for: $\mathcal{O}_L$ Noetherian.]

Corollary 10.3 Ring of integers of a number field is a Dedekind domain.

Convention $\mathcal{O}_K \equiv$ ring of integers of number field K

- $\mathfrak{p} \subseteq \mathcal{O}_K$ nonzero prime ideal.

Normalize $|\cdot|_{\mathfrak{p}}$ (abs val associated with $\mathfrak{p}$) by:

$|x|_{\mathfrak{p}} = N_{\mathfrak{p}}^{-v_{\mathfrak{p}}(x)}$, where $N_{\mathfrak{p}} \equiv |\mathcal{O}_K/\mathfrak{p}|$.

Number Fields: lecture 12

Setup: $\mathcal{O}_K$ Dedekind, $K = FF(\mathcal{O}_K)$.
L/K finite, $\mathcal{O}_L$ = integral closure of $\mathcal{O}_K$ in L.
$\Rightarrow \mathcal{O}_L$ Dedekind (by Theorem 10.4)

Lemma 10.4 $0 \neq x \in \mathcal{O}_K \Rightarrow (x) = \prod_{\substack{p \neq 0 \\ \text{prime ideal}}} p^{v_p(x)}$

Proof $x\mathcal{O}_{K,(p)} = (p\mathcal{O}_{K,(p)})^{v_p(x)}$ (by def.)
$\Rightarrow \{p \neq 0 : v_p(x) \neq 0\}$ finite
& lemma follows from $I = J \Leftrightarrow I\mathcal{O}_{K,(p)} = J\mathcal{O}_{K,(p)}$ $\forall p$.

Notation: $P \in \mathcal{O}_L$, $\mathfrak{p} \in \mathcal{O}_K$ nonzero prime ideals.
Write: $P \mid \mathfrak{p}$ if $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$ & $\exists i$, $P_i = P$.

Theorem 10.5 $\mathcal{O}_K$, $\mathcal{O}_L$, K, L as above.
For $\mathfrak{p}$ nonzero prime ideal of $\mathcal{O}_K$: abs vals on L extending $|\cdot|_{\mathfrak{p}}$ (up to equivalence) are precisely $|\cdot|_{P_1}, \ldots, |\cdot|_{P_r}$,
where $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$.

Proof By Lemma 10.4: $\forall 0 \neq x \in \mathcal{O}_K$, $\forall P_i$, $v_{P_i}(x) = e_i v_{\mathfrak{p}}(x)$
$\Rightarrow$ up to equivalence, $|\cdot|_{P_i}$ extends $|\cdot|_{\mathfrak{p}}$

Now: suppose $|\cdot|$ abs val on L, extending $|\cdot|_{\mathfrak{p}}$.
$\Rightarrow |\cdot|$ bounded on $\mathbb{Z}$ (since $|\cdot|_{\mathfrak{p}}$ is), so $|\cdot|$ non-Arch.
Let $R = \{x \in L : |x| \leq 1\} \subseteq L$. Valuation ring of L.
Claim: R arises as localisation of some prime ideal $\square$

Have: $\mathcal{O}_K \subseteq R$, and since R integrally closed in L: (lemma 6.8) have $\mathcal{O}_L \subseteq R$.

Set: $P \equiv \{x \in \mathcal{O}_L : |x| < 1\} \equiv m_R \cap \mathcal{O}_L$. ($m_R$ = max ideal in R)

$\Rightarrow P$ prime ideal, nonzero (contains p)

Then: $\mathcal{O}_{L,(P)} \subseteq R$, since: $S \in \mathcal{O}_L - P \Rightarrow |S| = 1$

& $\mathcal{O}_{L,(P)}$ is DVR, hence, is maximal subring of L,

$\Rightarrow \mathcal{O}_{L,(P)} = R$.

$\Rightarrow |\cdot|$ equivalent to $|\cdot|_P$.

Since $|\cdot|_\mathfrak{P}$ extends $|\cdot|_P$: have $\mathfrak{P} \cap \mathcal{O}_K = p$, so:

$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{P} \Rightarrow \mathfrak{P} = \mathfrak{P}_i$, some i.

Let: K number field. & $\sigma : K \to \mathbb{R}$ or $\mathbb{C}$ real or complex embed. Then: $x \mapsto |\sigma(x)|_\infty$ defines abs val. on K.

(sheet 2) Denote this $|\cdot|_\sigma$.

Corollary 10.6 | K NF, ring of ints $\mathcal{O}_K$. Then: any abs val on K is equivalent to either:

(i) $|\cdot|_P$, some $0 \neq p \subseteq \mathcal{O}_K$ prime ideal (non-Arch)

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

Proof Non-archimedean: then $|\cdot|_\mathbb{Q}$ equivalent to $|\cdot|_{\frac{1}{p}}$, some prime $p \in \mathbb{Z}$. (Ostrowski's theorem)

Theorem 10.5 $\Rightarrow |\cdot|$ equiv. to $|\cdot|_P$, some prime ideal $p \subseteq \mathcal{O}_K$. $\square$

Archimedean example sheet 2

Completions.

let: $\mathcal{O}_K$ Dedekind, L/K finite separable.
let: $\mathfrak{p} \subseteq \mathcal{O}_K$, $P \neq \mathcal{O}_L$ non-0 prime ideals, $P \mid \mathfrak{p}$.
write: $K_{\mathfrak{p}}$ & L_P completions of K, L WRT $|\cdot|_{\mathfrak{p}}, |\cdot|_P$.

Lemma 10.7 i) $\pi_P : L \otimes_K K_{\mathfrak{p}} \to L_P$ surjective
ii) $[L_P : K_{\mathfrak{p}}] \leq [L : K]$.

Proof let $M = \mathrm{Im}(\pi_P) = LK_{\mathfrak{p}} \subseteq L_P$.
write: $L = K(\alpha)$, $M = K_{\mathfrak{p}}(\alpha) \Rightarrow M$ finite ext of $K_{\mathfrak{p}}$
& $[M : K_{\mathfrak{p}}] \leq [L : K]$.
Moreover: (Theorem 6.1) M complete & $L \subseteq M \subseteq L_P$,
hence $M = L_P$. ✓

Lemma 10.8 (CRT) R ring, $I_1, \dots, I_n \subseteq R$ coprime ideals ($I_i + I_j = R \ \forall (i \neq j)$). Then:
(i) $\bigcap_{i \leq n} I_i = \prod_{i \leq n} I_i \equiv I$
(ii) $R/I \cong \prod_{i \leq n} R/I_i$.

Theorem 10.9 The natural map $L \otimes_K K_{\mathfrak{p}} \to \prod_{P \mid \mathfrak{p}} L_P$ is $\cong$.

Proof write $L = K(\alpha)$ & let: $f(x) \in K[x]$ the min poly of α.

Then: $f(x) = f_1(x) \cdots f_r(x)$ in $k_p[x]$, f_i distinct and irreducible (separable, since L separable)

Since $L \cong k[x]/(f(x))$: by CRT:

$$L \otimes_k k_p \cong \frac{k_p[x]}{(f(x))} \underset{CRT}{\cong} \prod \left[\frac{k_p[x]}{(f_i(x))} \right] \leftarrow L_i$$

L_i is finite ext / k_p, contains L and k_p.

(Since: $L = \frac{k(x)}{(f(x))} \hookrightarrow \frac{k_p[x]}{(f_i(x))}$ injective, since field morphisms)

Moreover: $L \subseteq L_i$ dense, since for an element of $\frac{k_p(x)}{(f_i(x))}$, can approximate coeffs with element of $\frac{k(x)}{(f(x))}$)

Theorem now follows from the following claims:

(i) $L_i \cong L_p$ for some $P \subseteq \mathcal{O}_L$, $P \mid p$

(ii) Each P appears at most once

(iii) Each P appears at least once.

(i) $[L_i : k_p] < \infty \Rightarrow \exists$ $|\cdot|$ abs val on L_i extending $|\cdot|_p$.

Theorem 10.5 $\Rightarrow$ $|\cdot|_L$ equiv to some $|\cdot|_p$, $P \mid p$.

Since L dense in L_i: & L_i complete: $\Rightarrow L_i = L_p$.

(ii) If P appears 2x: find isom. $\varphi : L_i \xrightarrow{\cong} L_j$ preserving L & k_p.

$\Rightarrow \varphi : \frac{k_p[x]}{(f_i(x))} \xrightarrow{\sim} \frac{k_p[x]}{(f_j(x))}$ takes: $x \mapsto x$ (preserves L, k_p)

$\Rightarrow f_i(x) = f_j(x)$, hence $i = j$.

(iii) By lemma 10.7: natural map $\pi_p : L \otimes_k k_p \to L_p$ surj $\forall P \mid p$.

Since L_p field: π_p factors through L_i, some i. So, $L_i \cong L_p$. ✓ (by surj) $\square$ 4

Local Fields: (lecture 13)

Let: $\mathcal{O}_K$ Dedekind, L/K finite separable.

From last time: $L \otimes_K K_\mathfrak{p} \cong \prod_{P \mid \mathfrak{p}} L_P$.

Example $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $f(x) = x^2 + 1$. By Hensel: $i \in \mathbb{Q}_5$, so (5) splits in $\mathbb{Q}(i)$ as $5\mathcal{O}_L = P_1 P_2$.

Corollary 10.10) $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal. Then: $\forall x \in L$:

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

Proof) Let: $B_1, \dots, B_r$ bases of $L_{P_1}, \dots, L_{P_r}$ $\left(\mathfrak{p}\mathcal{O}_L = \prod P_i^{e_i}\right)$

$\Rightarrow B = \bigcup_{i \leq r} B_i$ is basis for $L \otimes_K K_\mathfrak{p}$ over $K_\mathfrak{p}$ (by isomorphism).

Let: $[\text{mult}(x)]_B \equiv$ matrix for $\text{mult}(x) : L \otimes_K K_\mathfrak{p} \to L \otimes_K K_\mathfrak{p}$.

& $[\text{mult}(x)]_{B_i} \equiv$ matrix for $\text{mult}(x) : L_{P_i} \to L_{P_i}$

$$\Rightarrow [\text{mult}(x)]_B = \begin{pmatrix} [\text{mult}(x)]_{B_1} & & 0 \\ & \ddots & \\ 0 & & [\text{mult}(x)]_{B_r} \end{pmatrix}$$

$$\Rightarrow \text{Det}([\text{mult}(x)]_B) = \prod_{i \leq r} \text{Det}([\text{mult}(x)]_{B_i})$$

$$\Rightarrow N_{L/K}(x) = \prod_{i \leq r} N_{L_{P_i}/K_{P_i}}(x) \quad \checkmark$$

Decomposition Groups.

$0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal $\Rightarrow \mathfrak{p}\mathcal{O}_L = \prod P_i^{e_i}$. $(e_i > 0)$

Note $\forall i$: $P_i \cap \mathcal{O}_K \supseteq \mathfrak{p}$ (proper) prime ideal of $\mathcal{O}_K$.

$\Rightarrow \mathfrak{p} = P_i \cap \mathcal{O}_K$.

DEF 11.1 i) $e_i \equiv$ Ramification Indices of P_i over p.

ii) Say p ramifies in $L \iff \exists i,\ e_i > 1$.

Example $\mathcal{O}_K = \mathbb{C}[t]$, $\mathcal{O}_L = \mathbb{C}[T]$. & $\mathcal{O}_K \longrightarrow \mathcal{O}_L$, $t \longmapsto T^n$.

$\Rightarrow t\mathcal{O}_L = T^n\mathcal{O}_L$, so ram idx of (T) over (t) is n.

Corresponds (geometrically) to deg n covering of RS $\mathbb{C} \longrightarrow \mathbb{C}$, by $x \longmapsto x^n$. Is ramified at 0, ram idx n.

DEF 11.2 $f_i \equiv [\mathcal{O}_L/P_i : \mathcal{O}_K/p]$ Residue class degree, of P_i over p.

Theorem 11.3 $\sum e_i f_i = [L:K]$.

Proof let $S \equiv \mathcal{O}_K - p$. Quote following:

* $S^{-1}\mathcal{O}_L$ is integral closure of $S^{-1}\mathcal{O}_K$, in L
* $S^{-1}p\,S^{-1}\mathcal{O}_L \cong S^{-1}P_1^{e_1} \cdots S^{-1}P_r^{e_r}$ ($S^{-1}p$: ideal)
* $S^{-1}\mathcal{O}_L / S^{-1}P_i \cong \mathcal{O}_L/P_i$ & $S^{-1}\mathcal{O}_K / S^{-1}p \cong \mathcal{O}_K/p$.

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

$\Rightarrow$ can WLOG: $\mathcal{O}_K$ is DVR (hence PID).

By CRT: $\mathcal{O}_L/p\mathcal{O}_L \cong \prod_{i \le r} \mathcal{O}_L/P_i^{e_i}$ & count dim. of both sides, as $k \equiv \mathcal{O}_K/p$ – vector spaces:

* RHS: $\forall i$: $\exists$ decreasing sequences of k–subspaces:
  $0 \subseteq P_i^{e_i-1}/P_i^{e_i} \subseteq \cdots \subseteq P_i/P_i^{e_i} \subseteq \mathcal{O}_L/P_i^{e_i}$.

Note: $\mathfrak{P}_i^j / \mathfrak{P}_i^{j+1}$ is an $\mathcal{O}_L/\mathfrak{p}_i$ — module, generated by some $x \in \mathfrak{P}_i^j - \mathfrak{P}_i^{j+1}$ (e.g. can prove this via localisation at $\mathfrak{P}_i$)

$\Rightarrow \dim_k (\mathfrak{P}_i^j / \mathfrak{P}_i^{j+1}) = f_i \ \forall j$

$\Rightarrow \dim_k (\mathcal{O}_L / \mathfrak{P}_i^{e_i}) = e_i f_i$.

RHS $= \sum_{i \le r} e_i f_i$.

For LHS: by Structure Theorem (for f.g. modules over PID): since $\mathcal{O}_L$ is torsion-free $\mathcal{O}_K$-module: $\Rightarrow$ Free module / $\mathcal{O}_K$, and rank $= [L:K] = n$.

$\Rightarrow \mathcal{O}_L / \mathfrak{p}\mathcal{O}_L$, as an $\mathcal{O}_K$-module, is $\cong (\mathcal{O}_K/\mathfrak{p})^n$

$\Rightarrow \dim_k (\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = n$. ✓

Geometric Analogue: say $X \xrightarrow{f} Y$ is degree n cover of compact RS's. Then: $\forall y \in Y$: $n = \sum_{x \in f^{-1}(y)} e_x$ (ram idx)

~~Corollary~~ Now: assume L/K Galois.

Then: $\forall \sigma \in \mathrm{Gal}(L/K)$: $\sigma(\mathfrak{P}_i)$ is another prime ideal of $\mathcal{O}_L$, and $\sigma(\mathfrak{P}_i) \cap \mathcal{O}_K = \mathfrak{p}$. $\Rightarrow \sigma(\mathfrak{P}_i) \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$.

$\Rightarrow \sigma$ acts on $\{\mathfrak{P}_i\}$. ← of $\mathrm{Gal}(L/K)$ on $\{\mathfrak{P}_i\}$

Prop 11.4] This action is transitive.

Proof If not: find $i \neq j$ s.t. $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_j$. $\forall \sigma \in \mathrm{Gal}(L/K)$.

By CRT: can choose $x \in \mathcal{O}_L$ s.t. $x \equiv 0 \bmod \mathfrak{P}_i$, and $x \equiv 1 \bmod \sigma(\mathfrak{P}_j)$ $\forall \sigma \in \mathrm{Gal}(L/K)$.

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

Since P_j prime: $\exists\, \tau \in Gal(L/K)$, $\tau(x) \in P_j$.

$\Rightarrow x \in \tau^{-1}(P_j)$, so $x \equiv 0 \bmod \tau^{-1}(P_j)$ ⚡

Corollary 11.5 Suppose L/K Galois. Then e_i equal $\forall i$, f_i equal $\forall i$, and $n = efr$.

Proof $\forall \sigma \in Gal(L/K)$: have:

i) $p = \sigma(p) = \sigma(P_1)^{e_1} \cdots \sigma(P_r)^{e_r}$ $\Rightarrow e_1 = \cdots = e_r$ (transitivity)

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

If instead L/K extension of complete discretely valued fields, & normalised valuations v_L & v_K: & uniformizers π_L, π_K:

Ramification index is $e \equiv e_{L/K} = v_L(\pi_K)$.

(i.e. $\pi_K \mathcal{O}_L = \pi_L^e \mathcal{O}_L$.)

Residue class degree is: $f \equiv f_{L/K} = [k_L : k]$.

Corollary 11.6 L/K finite, separable. Then $[L:K] = ef$.

Remark Can also hold without separable assumption.

Back to $\mathcal{O}_K$ Dedekind domain.

DEF 11.7 L/K finite, Galois. Then, the decomposition group at prime P of $\mathcal{O}_L$ is: $G_P \equiv \{\sigma \in Gal(L/K) : \sigma(P) = P\} \leq Gal(L/K)$

Local Fields: lecture 14

From last time: $\mathcal{O}_K$ Dedekind, L/K finite Galois, and $0 \subsetneq P \subseteq \mathcal{O}_L$ prime. $G_P \equiv \{\sigma \in Gal(L/K) : \sigma(P) = P\}$.

Prop 11.4] $\forall P, P'$ lying over p, G_P & $G_{P'}$ are conjugate. & have size ef (Orbit-Stabiliser)

Prop 11.8] Suppose $P \mid p \subseteq \mathcal{O}_K$.

(i) L_P/K_p Galois

(ii) There is natural map $res: Gal(L_P/K_p) \to Gal(L/K)$ injective & image G_P.

Proof] (i) L/K Galois $\Rightarrow$ L splitting field of separable poly, $f(x) \in K[x]$.

$\Rightarrow$ L_P is splitting field of $f(x) \in K_p[x]$

$\Rightarrow$ L_P/K_p Galois.

(ii) Let $\sigma \in Gal(L_P/K_p)$, then $\sigma(L_P) = L_P$ (since L/K normal)

$\Rightarrow \exists$ map $res: Gal(L_P/K_p) \to Gal(L/K)$

$$\sigma \longmapsto \sigma|_L$$

Since L dense in L_P: res injective

& By lemma 8.2: $|\sigma(x)|_P = |x|_P \quad \forall \sigma \in Gal(L_P/K_p)$, $x \in L_P$.

$\Rightarrow \sigma(P) = P \quad \forall \sigma \in Gal(L_P/K_p)$

$\Rightarrow res(\sigma) \in G_P \quad \forall \sigma \in Gal(L_P/K_p)$.

For surj: suffices to show: $[L_P/K_p] = |G_P| = ef$.

- $|G_p| = ef$ ✓ by prop 11.4 & corollary 11.5
- $[L_p^\phi : K_p] = ef$: ✓ by corollary 11.6 + noting that e, f don't change when taking completions.

V: Ramification Theory.

§12.1: Different & Discriminant.

let: L/K ext. of algebraic NF's & $[L:K] = n$.

Notation: for $x_1, \dots, x_n \in L$: $\Delta(x_1, \dots, x_n) \equiv \det(\mathrm{Tr}_{L/K}(x_i x_j)) \in K$
$= \det(\sigma_i(x_j))^2$ for $\sigma_i : L \to \bar{K}$ different embeddings.

& If $y_i = \sum_j a_{ij} x_j$ $(a_{ij} \in K)$ then $\Delta(y_1, \dots, y_n) = (\det A)^2 \times \Delta(x_1, \dots, x_n)$

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

Lemma 12.1 k perfect field & R some k-algebra which is fin-dim k-VS.

Then: trace form $(\cdot,\cdot) : R \times R \to k$

$$(x, y) \equiv \mathrm{Tr}_{R/k}(xy) \equiv \mathrm{Tr}_k(\mathrm{mult}(xy))$$

is non-degenerate iff $R = k_1 \times \dots \times k_r$, where k_i/k is a finite (hence separable) extension of k.

[Proof: example sheet 3]

Theorem 12.2 $0 \subsetneq \mathfrak{p} \subseteq \mathcal{O}_K$ prime.

(i) If $\mathfrak{p}$ ramifies in L: then $\forall x_1, \dots, x_n \in \mathcal{O}_L$: $\Delta(x_1, \dots, x_n) \equiv 0 \mod \mathfrak{p}$

(ii) If $\mathfrak{p}$ unramified in L: $\exists x_1, \dots, x_n \in \mathcal{O}_L$, $\Delta(x_1, \dots, x_n) \not\equiv 0 \mod \mathfrak{p}$

Proof i) Let $p\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where $0 \subsetneq \mathfrak{P}_i \subseteq \mathcal{O}_L$ distinct prime ideals & $e_i > 0$.

By CRT: $R = \mathcal{O}_L/p\mathcal{O}_L \cong \prod_{i \le r} \mathcal{O}_L/\mathfrak{P}_i^{e_i}$.

$\Rightarrow$ If p ramifies in L: $\Rightarrow$ $\mathcal{O}_L/p\mathcal{O}_L$ has nilpotents.

$\Rightarrow$ $Tr_{R/k}$ degenerate (lemma 12.1)

$\Rightarrow \Delta(\overline{x}_1, \dots, \overline{x}_n) = 0 \ \forall \ \overline{x}_i \in \mathcal{O}_L/p\mathcal{O}_L$

$\Rightarrow \Delta(x_1, \dots, x_n) \equiv 0 \bmod \mathfrak{P} \ \forall \ x_i \in \mathcal{O}_L$.

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & R \\ \downarrow & & \downarrow \\ \mathcal{O}_K & \longrightarrow & k \equiv \mathcal{O}_K/\mathfrak{p} \end{array}$$

ii) p unramified in L $\Rightarrow$ $\mathcal{O}_L/p\mathcal{O}_L$ is product of finite extensions of k.

$\Rightarrow$ Trace form non-degenerate (lemma 12.1)

$\Rightarrow$ If $\overline{x}_1, \dots, \overline{x}_n$ basis of $\mathcal{O}_L/p\mathcal{O}_L$ as k-VS, then:

$\Delta(\overline{x}_1, \dots, \overline{x}_n) \neq 0$, so $\exists x_i \in \mathcal{O}_L$ s.t. $\Delta(x_1, \dots, x_n) \neq 0$ ✓

DEF 12.3 Discriminant $\equiv$ ideal $d_{L/K} \subseteq \mathcal{O}_K$ generated by $\Delta(x_1, \dots, x_n)$ for any choices $x_1, \dots, x_n \in \mathcal{O}_L$.

Corollary 12.4 $\mathfrak{p}$ ramifies in $L \Leftrightarrow \mathfrak{p} \mid d_{L/K}$.

In particular: since only finitely $\mathfrak{p}$ divide $d_{L/K}$, only finitely many primes ramify in L.

DEF 12.5 Inverse Different $\mathfrak{D}_{L/K}^{-1} = \{y \in L : Tr_{L/K}(xy) \in \mathcal{O}_K \ \forall x \in \mathcal{O}_L\}$.

Then this is an $\mathcal{O}_L$-submodule of L.

lemma 12.6 $\mathfrak{D}_{L/K}^{-1}$ is a fractional ideal in L, containing $\mathcal{O}_L$.

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

Set: $d \equiv \Delta(x_1, \dots, x_n) \equiv \det(Tr(x_i x_j)) \neq 0$. (non-degen.)

For $X \in D_{L/K}^{-1}$: write $X = \sum_i \lambda_i x_i$, where $\lambda_i \in K$.

$\Rightarrow Tr(X \cdot x_j) = \sum_i \lambda_i Tr(x_i x_j) \in \mathcal{O}_K$.

Set: $A \equiv Tr_{L/K}(x_i x_j)$. Then: multiply by $adj(A) \in M_n(\mathcal{O}_K)$:

$$\Rightarrow d \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = Adj(A) \cdot \begin{pmatrix} Tr_{L/K}(X x_1) \\ \vdots \\ Tr_{L/K}(X x_n) \end{pmatrix}$$

$\Rightarrow \lambda_i \in \frac{1}{d}\mathcal{O}_K$, so $X \in \frac{1}{d}\mathcal{O}_L$, so $D_{L/K}^{-1} \subseteq \frac{1}{d}\mathcal{O}_L$.

Hence it is a fractional ideal.

Contains $\mathcal{O}_L$: know, $Tr(x) \in \mathcal{O}_K \ \forall x \in \mathcal{O}_L \Rightarrow \mathcal{O}_L \subseteq D_{L/K}^{-1}$.

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

Local Fields: lecture 15.

Let: L/K degree n ext. of NF's.

& I_L, I_K the group of fractional ideals of L, K.

By Prop 9.7 $\Rightarrow I_L \cong \bigoplus_{0 \neq P \subseteq \mathcal{O}_L \text{ prime ideal}} \mathbb{Z}$ & $I_K \cong \bigoplus_{0 \subseteq p \subseteq \mathcal{O}_K \text{ prime ideal}} \mathbb{Z}$.

Define $N_{L/K}: I_L \to I_K$ induced by $P \longmapsto p^f$, where $p = P \cap \mathcal{O}_K$ & $f = f(P/p)$. ($f = [\mathcal{O}_L/P : \mathcal{O}_K/p]$)

Fact: $L^\times \longrightarrow I_L$ commutes.

$\downarrow N_{L/K}$ $\quad$ $\downarrow N_{L/K}$

$K^\times \longrightarrow I_K$

[Use fact Cor 10.10 & $v_p(N_{L_P/K_p}(x)) = f_{P/p}\, v_p(x)$, for $x \in L_P$ & v_P, v_p are normalised val's on L_P, K_p.]

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

Proof] Assume: (First) $\mathcal{O}_K, \mathcal{O}_L$ PID's

Choose $x_1, \dots, x_n \in \mathcal{O}_L$ an $\mathcal{O}_K$-basis for $\mathcal{O}_L$

& $y_1, \dots, y_n$ dual basis WRT the trace form.

$\Rightarrow y_1, \dots, y_n$ is basis for $D_{L/K}^{-1}$ (by def)

Let $\sigma_1, \dots, \sigma_n : L \longrightarrow \bar{K}$ distinct embeds.

$\Rightarrow \sum \sigma_i(x_j)\sigma_i(y_k) = Tr_{L/K}(x_j y_k) = \delta_{jk}$.

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

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

Write: $D_{L/K}^{-1} = \beta \cdot \mathcal{O}_L$, some $\beta \in L$ (since PID)

$\Rightarrow d_{L/K}^{-1} = (\Delta(x_1, \dots, x_n))^{-1} = (\Delta(y_1, \dots, y_n)) = (\Delta(\beta x_1, \dots, \beta x_n))$

(since change of basis matrix $\{y_i\} \mapsto \{\beta x_i\}$ is invertible in $\mathcal{O}_K$)

$= N_{L/K}(\beta)^2 (\Delta(x_1, \dots, x_n))$ (since: change of basis matrix is mult. by β)

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

$\Rightarrow N_{L/K}(D_{L/K}) = d_{L/K}$. ✓

In general (not PID): localise at $S \equiv \mathcal{O}_K - P$.

$$\left.\begin{aligned} &\therefore S^{-1} D_{L/K} = D_{S^{-1}\mathcal{O}_L / S^{-1}\mathcal{O}_K} \\ &\therefore S^{-1} d_{L/K} = d_{S^{-1}\mathcal{O}_L / S^{-1}\mathcal{O}_K} \end{aligned}\right]$$

Theorem 12.8 If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ some α with min poly $g(x) \in \mathcal{O}_K[X]$, then: $D_{L/K} = (g'(\alpha))$.

Proof Let $\alpha_1, \dots, \alpha_n$ roots of g ($\alpha = \alpha_1$).

Write $\frac{g(x)}{x-\alpha} = \beta_{n-1} x^{n-1} + \dots + \beta_0$, where $\beta_i \in \mathcal{O}_L$ & $\beta_{n-1} = 1$.

Then: $\sum \frac{g(\alpha)}{x-\alpha_i} \frac{\alpha_i^r}{g'(\alpha_i)} = x^r \quad (0 \le r \le n-1)$

[since: both sides are polys of degree $< n$, and equality holds for $X = \alpha_i$ $\forall i$]

$\Rightarrow \delta_{rs} = Tr_{L/K}\left(\frac{\alpha_i^r \beta_s}{g'(\alpha)}\right) \quad \forall s \le r$

Since $\mathcal{O}_L$ has $\mathcal{O}_K$-basis $\{1, \alpha, \dots, \alpha^{n-1}\}$: means,

□

$D_{L/K}^{-1}$ has $\mathcal{O}_K$-basis $\frac{\beta_0}{g'(\alpha)}, \dots, \frac{\beta_{n-1}}{g'(\alpha)} = \frac{1}{g'(\alpha)}$.

$\Rightarrow D_{L/K}^{-1} = (g'(\alpha))$, hence $D_{L/K} = (g'(\alpha))$.

~~Theorem 12.~~

Let: $0 \subsetneq P \subseteq \mathcal{O}_L$ prime & $p = \mathcal{O}_K \cap P$. Define local different D_{L_P/K_p}, using $\mathcal{O}_{L_P}$ & $\mathcal{O}_{K_p}$.

& Identify: D_{L_P/K_p} with a power of P.

Theorem 12.9 $D_{L/K} = \prod_P D_{L_P/K_p}$ (finite product).

Proof (assuming product finite):

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

a) $\mathrm{Tr}_{L/K}(x) = \sum_{P \mid p} \mathrm{Tr}_{L_P/K_p}(x)$ (similarly: Corollary 10.10)

Let: $r(P) \equiv v_P(D_{L/K})$ & $s(P) = v_P(D_{L_P/K_p})$.

"$\subseteq$": (i.e. $r(P) \geq s(P)$): find $x \in L$, with $v_P(x) \geq -s(P)\ \forall P$.

$\Rightarrow \mathrm{Tr}_{L_P/K_p}(xy) \in \mathcal{O}_{K_p}\ \forall y \in \mathcal{O}_L$ & $\forall P$.

By (a): $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_{K_p}\ \forall y \in \mathcal{O}_L$ & $\forall p$.

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

"$\supseteq$": (i.e. $r(P) \leq s(P)$): Fix P, and let $x \in P^{-r(P)} - P^{-r(P)+1}$.

$\Rightarrow v_P(x) = -r(P)$ & $v_{P'}(x) \geq 0\ \forall P' \neq P$.

By (a): $\mathrm{Tr}_{L_P/K_P}(xy) = \mathrm{Tr}_{L/K}(xy) - \sum_{\substack{P' \neq P \\ P' \mid p}} \mathrm{Tr}_{L_{P'}/K_p}(xy)$ $(\forall y \in \mathcal{O}_L)$

$\Rightarrow Tr_{L/K}(xy) \in \mathcal{O}_{K_p}$ $\forall y \in \mathcal{O}_L$, hence for $y \in \mathcal{O}_{L_p}$
(by continuity). So, $x \in \mathcal{D}^{-1}_{L_p/K_p}$, i.e. $-v_p(x) = r(p) \leq s(p)$.

Corollary 12.10 $d_{L/K} = \prod_{p|p} d_{L_p/K_p}$.

Proof Apply $N_{L/K}$ to previous result

§13: Unramified + Totally Ramified extensions of local fields

Let: L/K finite separable ext. of non-Arch local fields.

By Corollary 11.6: $[L:K] = e_{L/K} f_{L/K}$ (*)

Lemma 13.1 $M/L/K$ finite separable ext. of local fields.

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

Proof i) $f_{M/K} = [k_M : k]$, so follows by Tower Law.

ii) Follows from i) + (*).

DEF 13.2 The extension L/K is:

{Unramified, ramified, totally ramified} $\Leftrightarrow$ {$e_{L/K} = 1 \Leftrightarrow f_{L/K} = [L:K]$; $e_{L/K} > 1 \Leftrightarrow f_{L/K} < [L:K]$; $e_{L/K} = [L:K] \Leftrightarrow f_{L/K} = 1$}

Local Fields: Lecture 16.

Let: L/K finite separable ext. of local fields.

Theorem 13.3] $\exists K_0$ field: $K \subseteq K_0 \subseteq L$, with:

i) K_0/K unramified
$=$
ii) L/K_0 totally ramified.

Moreover: $[K_0 : K] = f_{L/K}$ & $[L : K_0] = e_{L/K}$,

and K_0/K is Galois.

Proof] Let $K = \mathbb{F}_q$, so: $K_L = \mathbb{F}_{q^f}$, $f \equiv f_{L/K}$.

Set $m \equiv q^f - 1$ & $[\cdot] : \mathbb{F}_{q^f} \to L$ Teichmuller map (for L).

Let: $\zeta_m \equiv [\alpha]$, for generator $\alpha \in \mathbb{F}_{q^f}^\times$. Then, ζ_m is a primitive m^{th} root of unity.

Set: $K_0 \equiv K(\zeta_m) \subseteq L$. Then: K_0/K Galois, and K_0 has residue field $k_0 \equiv \mathbb{F}_q(\alpha) = k_L$.

$\Rightarrow f_{L/K_0} = 1$, so L/K_0 totally ramified. ✓

For K_0/K: let res : $\mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_0/k)$ natural map given by restriction.

For $\sigma \in \mathrm{Gal}(K_0/K)$: have $\sigma(\zeta_m) = \zeta_m \iff \sigma(\zeta_m) \equiv \zeta_m \bmod m_0$

[since: by Hensel's lemma, $\mu_m(K_0) = \mu_m(k_0)$]

$\Rightarrow$ res map injective

$\Rightarrow |\mathrm{Gal}(K_0/K)| \leq |\mathrm{Gal}(k_0/k)| = f_{K_0/K}$.

But, also: $|\mathrm{Gal}(K_0/K)| = e_{K/K} f_{K_0/K} \Rightarrow$ have reverse ineq.

So, $[k_0 : k] = f_{k_0/k}$ & $e_{k_0/k} = 1$

$\Rightarrow$ res is $\cong$ & k_0/k unramified. ✓

Theorem 13.4 $k = \mathbb{F}_q$. Then $\forall n \geq 1$, $\exists!$ L/k unramified ext, of degree n. Moreover: L/k Galois, and the natural map $Gal(L/k) \to Gal(k_L/k)$ is $\cong$.

In particular, $Gal(L/k) \cong \langle Frob_{L/k} \rangle$ cyclic, where $Frob_{L/k}(x) \equiv x^q \bmod m_L \ \forall x \in \mathcal{O}_L$.

Proof For $n \geq 1$: take $L = k(\zeta_m)$, $m = q^n - 1$.

$\Rightarrow$ Similar to prev theorem: res: $Gal(L/k) \to Gal(k_L/k)$ is isomorphism $(\cong \mathbb{F}_{q^n}/\mathbb{F}_q)$

$\Rightarrow$ $Gal(L/k)$ is cyclic, and generated by lift of $x \mapsto x^q$.

Uniqueness: know: L/k is degree n & is unramified.

$\Rightarrow$ By Teichmuller: L contains ζ_m, so $L = k(\zeta_m)$.

[since: $k_L \cong \mathbb{F}_{q^m}$, so lift a generator of $\mathbb{F}_{q^m}^\times$.]

Corollary 13.5 L/k finite Galois. Then: the map:

res: $Gal(L/k) \to Gal(k_L/k)$ is surjective.

Proof $Gal(L/k) \twoheadrightarrow Gal(k_0/k) \xrightarrow{\sim} Gal(k_L/k)$

(L/k Galois.)

DEF 13.6 Inertia subgroup $I_{L/k} \equiv \ker\left(Gal(L/k) \xrightarrow{res} Gal(k_L/k)\right)$

✱ Since $[L:k] = e_{L/k} f_{L/k}$: get $|I_{L/k}| = e_{L/k}$.

✱ $I_{L/k} = Gal(L/k_0)$ (k_0 as in Theorem 13.3)

$\square$

DEF 13.7 $f(x) \equiv x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$.

f <u>eisenstein</u> $\iff v_K(a_i) \geq 1 \ \forall i$ & $v_K(a_0) = 1$.

($v_K \equiv$ normalised valuation)

<u>Fact</u>: $f(x)$ Eisenstein $\Rightarrow$ $f(x)$ irreducible.

Theorem 13.8 (i) L/K finite totally ramified ext, $\pi \in \mathcal{O}_L$ unif.

Then: min poly of π_L is Eisenstein, and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

(so, in particular $L = K(\pi_L)$.)

ii) Conversely: if $f(x) \in \mathcal{O}_K[x]$ Eisenstein & α root of f, then $K(\alpha)/K$ totally ramified & α unif. of $\mathcal{O}_L$.

Proof (i) $[L:K] = e = e_{L/K}$ (totally ramified)

let: $f(x) \equiv x^m + \cdots + a_0 \in \mathcal{O}_K[x]$ min poly of π_L.

$\Rightarrow m \leq e$.

$a_i \in \mathcal{O}_K$, so $v_L(a_i) \equiv 0 \bmod e$

<u>Know</u>: $v_L(K^\times) = e\mathbb{Z}$, so $v_L(a_i \pi_L^i) \equiv i \bmod e$ $(i \leq m)$

$\Rightarrow a_i \cdot \pi_L^i$ have <u>distinct</u> valuations (for $i \leq m$)

Since $\pi_L^m = -\sum_{i \leq m-1} a_i \pi_L^i$:

$\Rightarrow m = \min_{0 \leq i \leq m-1} (i + e \cdot v_K(a_i))$.

$\Rightarrow$ must have $v_K(a_i) \geq 1 \ \forall i$, and $v_K(a_0) = 1$, & $m = e$.

$\Rightarrow f(x)$ <u>eisenstein</u> & $[L:K] = [K(\pi_L):K]$, so <u>$L = K(\pi_L)$</u>.

For $y \in L$: write $y = \sum_{0 \leq i < e} \pi_L^i b_i$ $(b_i \in K)$

$\Rightarrow v_L(y) = \min_{0 \le i < e} (i + e \cdot v_k(b_i))$, so:

$y \in \mathcal{O}_L \Leftrightarrow v_L(y) \geq 0 \Leftrightarrow i + e \cdot v_k(b_i) \geq 0 \ \forall i \Leftrightarrow v_k(b_i) \geq 0$
$\Leftrightarrow y \in \mathcal{O}_K(\pi_L)$

ii) Let: $f(x) = x^n + \cdots + a_0 \in \mathcal{O}_K[x]$ Eisenstein. $e = e_{L|K}$. $L = K(\alpha)$.

$\Rightarrow v_L(a_i) \geq e$ (by def. of Eisenstein poly) & $v_L(a_0) = e$.

If $v_L(\alpha) < 0$: then $v_L(\alpha^n) < v_L(\sum_{0 \le i < n} a_i \alpha^i)$ ✗ since $f(\alpha) = 0$.

$\Rightarrow v_L(\alpha) \geq 0$.

$v_L(a_i \cdot \alpha^i) > e = v_L(a_0) \ \forall i > 0$.

$\Rightarrow v_L(\alpha^n) = v_L(\sum_{0 \le i < n} a_i \alpha^i) = v_L(a_0)$, so $n v_L(\alpha) = e$

But: $n = (L:K) \geq e$, hence $n = e$ & $v_L(\alpha) = 1$ ✓

---

§: Structure of units.

Let: $[K: \mathbb{Q}_p] < \infty$ finite ext & $e \equiv e_{K|\mathbb{Q}_p}$, π unif. of K.

Prop 13.8 Suppose $r > \frac{e}{p-1}$. Then: $\exp(x) \equiv \sum_{n \geq 0} \frac{x^n}{n!}$ converges on $\pi^r \mathcal{O}_K$, and induces $\cong$: $(\pi^r \mathcal{O}_K, +) \xrightarrow{\sim} (1 + \pi^r \mathcal{O}_K, \times)$.

Proof Convergence: $v_K(n!) = e \cdot v_p(n!) = e \cdot \frac{n - s_p(n)}{p-1} \leq e \cdot \frac{n-1}{p-1}$.

For $x \in \pi^r \mathcal{O}_K$: $v_K\left(\frac{x^n}{n!}\right) \geq nr - e\frac{n-1}{p-1} = nr + (n-1)\underbrace{\left(r - \frac{e}{p-1}\right)}_{>0}$.

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

$\Rightarrow \exp(x)$ converges on $\pi^r \mathcal{O}_K$, and: since $v_K\left(\frac{x^n}{n!}\right) \geq r \ \forall n$,

get $\exp(x) \in 1 + \pi^r \mathcal{O}_K \ \forall x$.

Similarly: consider $\log(x): 1 + \pi^r \mathcal{O}_K \to \pi^r \mathcal{O}_K$, where

$\log(1+x) \equiv \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} x^n$. Check convergence as before.

& have: $\exp(x)\exp(y) = \exp(x+y)$ & $\exp(\log(1+x)) = x$, so follows.

Local Fields: lecture 17

From last time: if $K/\mathbb{Q}_p$ finite, $e \equiv e_{K/\mathbb{Q}_p}$: if $r > \frac{e}{p-1}$ then $(\pi^r \mathcal{O}_K, +) \underset{exp}{\cong} (1+\pi^r \mathcal{O}_K, \times)$.

Now: let K local field & $U_K \equiv \mathcal{O}_K^\times$, $\pi \in \mathcal{O}_K$ unif.

DEF 13.10] For $s \in \mathbb{Z}_{\geq 1}$: $U_K^{(s)} \equiv (1+\pi^s \mathcal{O}_K, \times)$ s'th unit group. & $U_K^{(0)} \equiv U_K$. Then: $\cdots \subseteq U_K^{(s)} \subseteq \cdots \subseteq U_K^{(1)} \subseteq U_K^{(0)} = U_K$.

Prop 13.11] (i) $U_K^{(0)}/U_K^{(1)} \cong (k^\times, \times)$ $(k \equiv \mathcal{O}_K/\pi)$

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

Proof] (i) Consider reduction mod π: $\mathcal{O}_K^\times \longrightarrow k^\times$ surjective, with kernel $1+\pi\mathcal{O}_K = U_K^{(1)}$.

(ii) consider $f: U_K^{(s)} \longrightarrow k$,
$1+\pi^s x \mapsto x \bmod \pi$.

$\Rightarrow (1+\pi^s x)(1+\pi^s y) = 1+\pi^s(x+y+\pi^s xy)$, and $x+y+\pi^s xy \equiv x+y \bmod \pi$. So, f is group hom. & f surjective, and $\ker(f) = U_K^{(s+1)}$. ✓

Corollary 13.12] Let $K/\mathbb{Q}_p$, $[K:\mathbb{Q}_p] < \infty$. Then: $\exists$ finite index subgroup of $\mathcal{O}_K^\times$, isomorphic to $(\mathcal{O}_K, +)$.

Proof] For $r > \frac{e}{p-1}$: $U_K^{(r)} \cong (\mathcal{O}_K, +)$

& by prop 13.11: $U_K^{(r)} \subseteq U_K$ has finite index. ✓

Remark Not true, for equal charistic K. Because: exp is not defined in this setting.

Examples. $\mathbb{Z}_p^\times$ $(p>2)$. $e=1$. Can take: $r=1$, so:

$\mathbb{Z}_p^\times \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p) \cong \mathbb{F}_p^\times \times \mathbb{Z}_p$.

$x \longmapsto \left(x \bmod p,\ x \cdot \overline{[x \bmod p]}^{\,x}\right)$

$p=2$: take $r=2$, so: $\mathbb{Z}_2^\times \xrightarrow{\cong} (\mathbb{Z}/4\mathbb{Z})^\times \times (1+4\mathbb{Z}_p)$

$x \longmapsto \left(x \bmod 4,\ \frac{x}{\varepsilon(x)}\right)$

$\left(\varepsilon(x) \equiv \begin{cases} +1 \text{ if } x \equiv 1 \bmod 4 \\ -1 \text{ if } x \not\equiv 1 \bmod 4. \end{cases}\right)$

$\Rightarrow$ Another proof of $\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 \cong \begin{cases} \mathbb{Z}/p\mathbb{Z}, & p>2 \\ (\mathbb{Z}/2\mathbb{Z})^2, & p=2. \end{cases}$

§14: Higher Ramification Groups.

From now to end of course: local fields non-Arch.

Let: L/K finite Galois ext. of local fields & $\pi_L \in \mathcal{O}_L$ unif.

DEF 14.1 v_L normalised val. on L. For $s \in \mathbb{R}_{\geq -1}$:

s^{th} ramification group $G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \forall x \in \mathcal{O}_L,\ v_L(\sigma(x)-x) \geq s+1\}$

Remark G_s only changes at integers.

But: $\{G_s : s \geq -1\}$ is used to define upper numbering.

Examples $G_{-1}(L/K) = \mathrm{Gal}(L/K)$, $G_0(L/K) =$

$G_0(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) \equiv x \bmod \pi_L\ \forall x \in \mathcal{O}_L\}$

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

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

$\Rightarrow$ G_s normal in $\mathrm{Gal}(L/K)$. & $\{1\} \subseteq G_s \subseteq G_{s-1} \subseteq \cdots \subseteq G_{-1}$.

Theorem 14.2 i) $\forall s \geq 1$: $G_s = \{\sigma \in G_0 : v_L(\sigma(\pi_L)-\pi_L) \geq s+1\}$

ii) $\bigcap_{n\geq 0} G_n = \{1\}$

iii) $\forall s \in \mathbb{Z}_{\geq 0}$: $\exists$ injective group hom $G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$ induced by: $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$.

Proof] Let $K_0 \subseteq L$ max. unramified ext of K in L. Note that by replacing K with K_0: can WLOG assume L/K totally ramified.

(i) By Theorem 13.8: $\mathcal{O}_L = \mathcal{O}_K[\pi_K]$.

If $v_L(\sigma(\pi_L) - \pi_L) \geq s+1$, then $\forall x \in \mathcal{O}_L$: $x = f(\pi_L)$, $f \in \mathcal{O}_K[X]$

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

$= (\sigma(\pi_L) - \pi_L)\, g(\pi_L)$ for $g \in \mathcal{O}_K[X]$.

~~$\Rightarrow 0 \bmod \pi$~~

Hence: $v_L\left(\sigma\left(\frac{x}{\pi_L}\right) - \frac{x}{\pi_L}\right) \geq v_L(\sigma(\pi_L) - \pi_L) \geq s+1$ ✓

(ii) Suppose $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \neq 1$. Then: $\sigma(\pi_L) \neq \pi_L$

(because: $L = K(\pi_L)$, so cannot fix π_L)

$\Rightarrow v_L(\sigma(\pi_L) - \pi_L) < \infty$, so $\sigma \notin G_s$ for s big enough.

(iii) For $\sigma \in G_s$ $(s \in \mathbb{Z}_{\geq 0})$: $\sigma(\pi_L) \in \pi_L + \pi_L^{s+1}\mathcal{O}_L$.

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

Claim: $\varphi : G_s \longrightarrow U_L^{(s)}/U_L^{(s+1)}$, $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$, is a group hom, with kernel G_{s+1}.

Group hom] $\forall \sigma, \tau \in G_s$: write $\tau(\pi_L) = u \cdot \pi_L$ for $u \in \mathcal{O}_L^\times$. (since both uniformisers).

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

Need to show: $\frac{\sigma(u)}{u} \in U_L^{(s+1)}$.

But: $\sigma(u) \in u + \pi_L^{s+1} \mathcal{O}_L$, so $\frac{\sigma(u)}{u} \in 1 + \pi_L^{s+1} \mathcal{O}_L = U_L^{(s+1)}$ ✓

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

$\Rightarrow \varphi$ is group hom.

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

For independence: if $\pi_L' = a \cdot \pi_L$ for $a \in \mathcal{O}_L^\times$, then:

$$\frac{\sigma(\pi_L')}{\pi_L'} = \frac{\sigma(a)}{a} \frac{\sigma(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \mod U_L^{(s+1)}. \quad ✓$$

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

Proof By prop 13.11 + thm 14.2 + thm 13.4: for $s \in \mathbb{Z}_{\geq -1}$,

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

& All groups here solvable (since: abelian). So, G_s/G_{s+1} solvable $\forall s \geq -1$.

& since $\bigcap G_s = \{1\}$: $\mathrm{Gal}(L/K)$ solvable ✓

Let $\mathrm{char}(k) = p$. Then: $|G_0/G_1|$ is coprime to p, and $|G_1| = p^n$, some $n \geq 0$. So, G_1 is unique (since normal) Sylow p-subgroup of $I_{L/K}$.

DEF 14.4 $G_1 \equiv$ wild inertia group & $G_0/G_1 \equiv$ tame quotient.

Local Fields: lecture 18.

Let: L/K finite separable ext. of local fields. Say:

* L/K tamely ramified, if: $\mathrm{char}(k) \nmid e_{L/K}$
* L/K wildly ramified otherwise.

Theorem 14.5 $K/\mathbb{Q}_p$ finite ext & L/K finite ext. Note: $\exists\, \delta(L/K) \in \mathbb{Z}_{\geq 1}$ s.t. $D_{L/K} = (\pi_L^{\delta(L/K)})$.

Then: $\delta(L/K) \geq e_{L/K} - 1$ & equality $\Leftrightarrow$ L/K tamely ramified.

In particular, L/K unramified $\Leftrightarrow$ $D_{L/K} = \mathcal{O}_L$.

Proof From sheet 3: $D_{L/K} = D_{L/K_0} D_{K_0/K}$ where K_0 is maximal unramified ext. of K.

So, suffices to prove for both unramified + totally ramified cases.

(i) L/K Unramified: By Prop 6.12: $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ where $\alpha \in \mathcal{O}_L$, and also $k_L = k(\bar{\alpha})$.

Let $g(x) \in \mathcal{O}_K[X]$ min poly of α. Then: since unramified, $[k_L : k] = [L:K] \Rightarrow \bar{g}(x) \in k[X]$ min poly of $\bar{\alpha}$.

$\Rightarrow \bar{g}$ separable (field perfect), so $\bar{g}'(\alpha) \not\equiv 0 \bmod \pi_L$.

By Theorem 12.8: $D_{L/K} = (g'(\alpha)) = \mathcal{O}_L$. ✓

(ii) L/K Totally ramified: denote $e = [L:K]$, and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ where π_L root of Eisenstein poly $g(x)$

$$g(x) = 1 \cdot X^e + \sum_{0 \leq i < e} a_i \cdot X^i \in \mathcal{O}_K[X].$$

$\Rightarrow g'(\pi_L) = e \cdot \pi_L^{e-1} + \underbrace{\sum i \cdot a_i \cdot \pi_L^{i-1}}_{\text{if } i \neq e} \quad v_L \geq e$

$\Rightarrow v_L(g'(\pi_L)) \geq e-1$, and equality $\Leftrightarrow$ p$\nmid$e.

$\Leftrightarrow \mathrm{char}(k) \nmid e$. ✓

Corollary 14.6 L/K ext. of NF's & $P \subseteq \mathcal{O}_L$ prime ideal, $p = P \cap \mathcal{O}_K$. Then: $e(P/p) \geq 1 \Leftrightarrow P \mid \mathfrak{D}_{L/K}$.

Proof By Theorem 12.9: $\mathfrak{D}_{L/K} = \prod_P \mathfrak{D}_{L_P/K_p}$

& use fact: $e(P/p) = e_{L_P/K_p}$, and Theorem 14.5.

Example $K = \mathbb{Q}_p$, ζ_{p^n} primitive (p^n)-th root of unity

$L \equiv \mathbb{Q}_p(\zeta_{p^n})$. Then: (p^n)'th Cyclotomic poly is:

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

From Sheet 3:

- $\Phi_{p^n}(X)$ irreducible & min poly of ζ_{p^n}
- $L/\mathbb{Q}_p$ Galois, totally ramified & degree $p^{n-1}(p-1)$
- $\pi \equiv \zeta_{p^n} - 1$ is a uniformizer of $\mathcal{O}_L \Rightarrow \mathcal{O}_L = \mathbb{Z}_p[\pi] = \mathbb{Z}_p[\zeta_{p^n}]$
- $\mathrm{Gal}(L/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ (abelian)

  $\sigma_m \longmapsto m$, where $\sigma_m(\zeta_{p^n}) = \zeta_{p^n}^m$.

Hence: ~~$L/\mathbb{Q}_p$~~ $L/\mathbb{Q}_p$ totally ramified, and:

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

Find: largest k, with $p^k \mid m-1$. Then, $\zeta_{p^n}^{m-1}$ is a primitive $(p^{n-k})^{\text{th}}$ root of unity.

$\Rightarrow (\zeta_{p^n}^{m-1} - 1)$ is a unif. in π' in $L' = \mathbb{Q}_p(\zeta_p^{m-1})$.

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

So, by theorem 14.2 (i):

$p \in G_i \iff p^k \geq i+1$.

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

VI: Local Class Field Theory

§16: Infinite Galois Theory.

Let: L/K algebraic ext. of fields (not necessarily finite).

DEF 16.1] L/K Separable $\iff \forall \alpha \in L$, min poly $f_\alpha \in K[x]$ is separable.

L/K normal $\iff f_\alpha(x)$ splits in L $\forall \alpha \in L$

L/K Galois $\iff$ normal + separable.

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

If L/K finite: have Galois correspondence:

$$\left\{ \begin{array}{c} \text{Subextensions} \\ K \subseteq K' \subseteq L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Subgroups} \\ \text{of } \mathrm{Gal}(L/K) \end{array} \right\}.$$

$$K' \longmapsto \mathrm{Gal}(L/K').$$

Let $(I, \leq)$ poset. Say I directed if $\forall i,j \in I: \exists k \in I$, with $i \leq k$ & $j \leq k$.

Example • Any total order
• $\mathbb{N}_{\geq 1}$ ordered by divisibility.

DEF 16.2] $(I, \leq)$ directed. & $\{G_i\}_{i \in I}$ collection of groups with maps (group homs) $\varphi_{ij}: G_j \to G_i$, with:
⊙ $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$, ⊛ $\varphi_{ii} = id$ & $(\forall\, i \leq j \leq k)$
The $((G_i)_{i \in I}, \varphi_{ij})$ is an inverse system.
& $\varprojlim_{i \in I} G_i \equiv \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \varphi_{ij}(g_j) = g_i \right\}$.

Remark] • $(\mathbb{N}, \leq)$ recovers previous construction of inverse limit.
• $\exists$ Projections $\psi_j: \varprojlim_{i \in I} G_i \to G_j$
• $\varprojlim_{i \in I} G_i$ satisfies universal property.
If G_i finite $\forall i$: profinite topology on $\varprojlim_{i \in I} G_i$ is the weakest topology s.t. ψ_i continuous $\forall i$.

Prop 16.3] L/K Galois.
(i) $I \equiv \{ F/K : F \subseteq L$ & F/K finite Galois$\}$ directed under $\subseteq$
(ii) $\forall F \subseteq F' \in I: \exists\, \mathrm{res}_{F,F'}: \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$, is $\twoheadrightarrow$.
and the natural map $\mathrm{Gal}(L/K) \to \varprojlim_{F \in I} \mathrm{Gal}(F/K)$ is $\cong$.
(Proof: Sheet 4)

Local Fields: lecture 19

Theorem 16.4 (Fundamental Theorem of Galois Theory)
L/k Galois. Endow $\mathrm{Gal}(L/k)$ with profinite topology. (discrete top. if L/k finite.) Then: $\exists$ bijection

$$\left\{ \begin{array}{c} F/k \text{ subext.} \\ \text{of } L/k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Closed subgroups} \\ \text{of } \mathrm{Gal}(L/k) \end{array} \right\}$$

$$F \longmapsto \mathrm{Gal}(L/F)$$

$$L^H \longmapsto H$$

Moreover: F/k finite $\Leftrightarrow$ $\mathrm{Gal}(L/F)$ open

F/k Galois $\Leftrightarrow$ $\mathrm{Gal}(F/k) \subseteq \mathrm{Gal}(L/k)$ normal.

Example $k = \mathbb{F}_q$ & $L = \overline{\mathbb{F}}_q$. Then L/k Galois ($\mathbb{F}_q$ perfect)

Then: $\left\{ F/k \text{ finite Galois} \right\} \longleftrightarrow \mathbb{N}_{\geq 1}$

$$\mathbb{F}_{q^n} \longleftrightarrow n.$$

& $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n} \Leftrightarrow m \mid n$.

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \\ \| & & \| \\ \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z}. \end{array}$$

$\Rightarrow \exists$ Commutative diagram:

$$\Rightarrow \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \varprojlim_{n \in (\mathbb{N}_{\geq 1}, \,\mid)} \mathbb{Z}/n\mathbb{Z}$$

$$\cong \widehat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p. \quad \text{(example sheet 3)}$$

& $\mathrm{Fr}_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ corresponds to $1 \in \widehat{\mathbb{Z}}$.

If $\langle \mathrm{Fr}_q \rangle \subseteq \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, this corresponds to $\mathbb{Z} \subseteq \widehat{\mathbb{Z}}$.

§Weil Groups.

Let: L/K local field & L/K separable algebraic ext.

DEF 16.5 (i) L/K unramified $\Leftrightarrow$ F/K unramified $\forall$ F/K finite ext.

(ii) L/K totally ramified $\Leftrightarrow$ F/K totally ramified $\forall$ F/K finite.

Prop 16.6 L/K unramified. Then: L/K Galois, and:

$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$.

Proof Any finite subext F/K unram, so Galois, so F/K normal + separable $\Rightarrow$ L/K Galois.

Moreover: $\exists$ commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\text{res}} & \mathrm{Gal}(k_L/k) \\ \| \text{ (16.3)} & & \| \text{ (16.3)} \\ \varprojlim_{F/K \text{ finite}, F \subseteq L} \mathrm{Gal}(F/K) & \longrightarrow & \varprojlim_{k'/k \text{ finite}, k' \subseteq k_L} \mathrm{Gal}(k'/k) \\ \| \text{ (3.4)} & & \| \\ \varprojlim_{F/K \text{ finite}, F \subseteq L} \mathrm{Gal}(k_F/k) & & \end{array}$$

$\Leftarrow$ since: $\exists$ bijection $\{F/K \text{ finite}, F \subseteq L\} \leftrightarrow \{k'/k \text{ finite}, k' \subseteq L\}$

$\Rightarrow$ res is an isomorphism ✓

Let: L_1/K & L_2/K finite unram ext. By ex. sheet 3: L_1L_2/K is unram.

$\Rightarrow \forall\, L/k$: $\exists$ maximal unram subext k_0/k.

If L/k Galois: $\exists$ surjection $res: Gal(L/k) \twoheadrightarrow Gal(k_0/k) \cong Gal(k_L/k)$.

Set $I_{L/k} \equiv \ker(res)$ inertia subgroup

& let $Fr_{k_L/k} \in Gal(k_L/k)$ Frobenius $x \mapsto x^q$.

& $\langle Fr_{k_L/k} \rangle \subseteq Gal(k_L/k)$ subgroup.

DEF 16.7 L/k Galois. The Weil Group $W(L/k) \subseteq Gal(L/k)$

$W(L/k) \equiv res^{-1}(\langle Fr_{k_L/k} \rangle)$.

Remark If k_L/k finite: $W(L/k) = Gal(L/k)$, else $\subsetneq$.

& $\exists$ Commutative diagram: (exact rows)

$$\begin{array}{ccccccc} 0 & \longrightarrow & I_{L/k} & \longrightarrow & W(L/k) & \xrightarrow{res} & \langle Fr_{k_L/k} \rangle \longrightarrow 0 \\ & & \| & & \downarrow & & \downarrow \\ 0 & \longrightarrow & I_{L/k} & \longrightarrow & Gal(L/k) & \xrightarrow{res} & Gal(k_L/k) \longrightarrow 0 \end{array}$$

Topology on $W(L/k)$: endow topology on $W(L/k)$ as the weakest topology s.t.

1) $W(L/k)$ topological group (cont mult & inv)

2) $I_{L/k} \subseteq W(L/k)$ open subgroup ($I_{L/k}$ endowed with profinite topology).

i.e. a basis of open sets of $W(L/k)$ are translates of open sets in $I_{L/k}$, by elements in $W(L/k)$.

Warning: If k_L/k infinite, NOT subspace topology by $Gal(L/k)$.

E.g. $I_{L/K} \subseteq W(L/K)$ not open, in subspace topology.

Prop 16.8 L/K Galois.

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

(ii) If F/K finite subext of $L/K \Rightarrow W(L/F) = W(L/K) \cap \mathrm{Gal}(L/F)$.

(iii) F/K finite Galois subext $\Rightarrow \dfrac{W(L/K)}{W(L/F)} \cong \mathrm{Gal}(F/K)$.

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

$\Leftrightarrow \forall F/K$ finite Galois subext, $W(L/K)$ intersects all cosets of $\mathrm{Gal}(F/K)$

$\Leftrightarrow \forall F/K$ finite Galois subext, $W(L/K) \twoheadrightarrow \mathrm{Gal}(F/K)$.

Have diagram:

$$\begin{array}{ccccccccc} 0 & \to & I_{L/K} & \to & W(L/K) & \to & \langle Fr_{k_L/K} \rangle & \to & 0 \\ & & \downarrow a & & \downarrow b & & \downarrow c & & \\ 0 & \to & I_{F/K} & \to & \mathrm{Gal}(F/K) & \to & \mathrm{Gal}(k_F/k) & \to & 0 \end{array}$$

Let: K_0/K maximal unram ext of L/K. Then:

$K_0 \cap F$ = maximal unram ext contained in F

$$\Rightarrow I_{L/K} = \mathrm{Gal}(L/K_0) \twoheadrightarrow \mathrm{Gal}(FK_0/K_0) \cong \mathrm{Gal}(F/K_0 \cap F) \cong I_{F/K}$$

$\Rightarrow a$ surj.

& have: $\mathrm{Gal}(k_F/k)$ generated by $Fr_{k_F/k}$

& $\exists$ element in $\langle Fr_{k_L/K} \rangle$ restricting to this $\Rightarrow c$ surj

By diagram chase: b surj ✓

(ii) Let F/K finite subext. Consider:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \twoheadrightarrow & \mathrm{Gal}(k_L/k) \supseteq \langle Fr_{k_L/k} \rangle \\ \uparrow & & \uparrow \\ \mathrm{Gal}(L/F) & \twoheadrightarrow & \mathrm{Gal}(k_L/k) \supseteq \langle Fr_{k_L/k_F} \rangle \end{array}$$

So: $\sigma \in W(L/F) \Leftrightarrow \sigma|_{k_L} \in \langle Fr_{k_L/k_F} \rangle$

(for $\sigma \in Gal(L/F)$:) $\Leftrightarrow \sigma|_{k_L} \in \langle Fr_{k_L/k} \rangle$

(since: $Gal(k_L/k_F) \cap \langle Fr_{k_L/k} \rangle = \langle Fr_{k_L/k_F} \rangle$)

$\Leftrightarrow \sigma \in W(L/K)$.

(iii) $\dfrac{W(L/K)}{W(L/F)}$ (ii) $\dfrac{W(L/K)}{W(L/K) \cap Gal(L/F)}$

$\cong \dfrac{W(L/K)\, Gal(L/F)}{Gal(L/F)}$

(i) $\dfrac{Gal(L/K)}{Gal(L/F)}$ (since dense subgroup)

$= Gal(F/K)$. ✓

Local Fields: lecture 20.

Statements of Local Class Field Theory.

K local field.

DEF 17.1 L/K extension **abelian** $\Leftrightarrow$ L/K Galois + Abelian Galois group $Gal(L/K)$.

Facts: if L_1/K & L_2/K abelian:

(i) L_1L_2/K abelian

(ii) If $L_1 \cap L_2 = K$ then $\exists$ canonical iso. ~~$Gal(L_1L_2/K)$~~

$$Gal(L_1L_2/K) \xrightarrow{\cong} Gal(L_1/K) \times Gal(L_2/K).$$

By Fact (i) $\Rightarrow \exists$ maximal abelian ext K^{ab} of K.
(given by: composite of all finite abelian ext's of K.)

Let: $K^{ur} \equiv$ max. unramified ext of K (exists by last time) inside K^{sep}.

$$\Rightarrow K^{ur} = \bigcup_{m \geq 1} K(\zeta_{q^m-1}), \quad q = |k|$$

& $k_{K^{ur}} \cong \overline{\mathbb{F}_q}$.

& $Gal(K^{ur}/K) \cong Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ is abelian

$$Fr_{K^{ur}/K} \longrightarrow Fr_{\overline{\mathbb{F}_q}/\mathbb{F}_q}$$

Hence: K^{ur}/K abelian, so $K^{ur} \subseteq K^{ab}$, & $\exists$ exact sequence

$$0 \longrightarrow I_{K^{ab}/K} \longrightarrow W(K^{ab}/K) \twoheadrightarrow \underset{=\langle Fr_{K^{ur}/K} \rangle}{\mathbb{Z}} \longrightarrow 0.$$

Theorem 17.2 (1) (local Artin reciprocity):

$\exists!$ topological isomorphism (group iso + homeo):

$Art_K : K^\times \to W(K^{ab}/K)$, satisfying:

(i) $Art_K(\pi)\big|_{K^{ur}} = Fr_{K^{ur}/K}$ $\quad \forall \pi \in K$ uniformizer.

(ii) $\forall L/K$ finite subext in K^{ab}/K: $Art_K(N_{L/K}(L^\times))\big|_L = \{1\}$.

The map Art_K is Artin map / Artin reciprocity map.

(2) L/K finite Abelian. Then Art_K induces isomorphism:

$$K^\times / N_{L/K}(L^\times) \cong \frac{W(K^{ab}/K)}{W(K^{ab}/L)} \cong Gal(L/K).$$

Properties of Artin map.

- (Existence Theorem): $\forall H \subseteq K^\times$ open & finite index subgroup: $\exists L/K$ finite Abelian ext, with $N_{L/K}(\text{有}L^\times) = H$.

In particular: Art_K induces (inclusion reversing) iso. of posets:

$$\left\{\begin{array}{c}\text{Open finite index} \\ H \subseteq K^\times\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{finite abelian exts} \\ L/K\end{array}\right\}$$

$$H \longmapsto (K^{ab})^{Art_K(H)}$$

$$N_{L/K}(L^\times) \longmapsto L/K$$

- (Norm functoriality) If L/K finite + sep. exts, then:

$$\begin{array}{ccc} L^\times & \xrightarrow{Art_L} & W(L^{ab}/L) \\ \Big\downarrow N_{L/K} & & \Big\downarrow \text{res.} \\ K^\times & \xrightarrow[Art_K]{} & W(K^{ab}/K) \end{array}$$

commuting diagram.

Prop 17.3 L/K finite + Abelian (deg n). Then:

$$e_{L/K} = [O_K^\times : N_{L/K}(O_L^\times)].$$

Proof $\forall x \in L^\times$: ~~$f_{L/K}$~~ $v_K(N_{L/K}(x)) = f_{L/K} v_L(x)$.

$\Rightarrow \exists$ surjection $\dfrac{K^\times}{N_{L/K}(L^\times)} \xrightarrow{v_K} \dfrac{\mathbb{Z}}{f_{L/K}\mathbb{Z}}$ ~~kernel~~

& has kernel: $\dfrac{O_K^\times N_{L/K}(L^\times)}{N_{L/K}(L^\times)} \cong \dfrac{O_K^\times}{O_K^\times \cap N_{L/K}(L^\times)} \cong \dfrac{O_K^\times}{N_{L/K}(O_L^\times)}$.

By Theorem 17.2 ii): $[K^\times : N_{L/K}(L^\times)] = n$.

$\Rightarrow f_{L/K}[O_K^\times : N_{L/K}(O_L^\times)] = n$, so use $n = e_{L/K} f_{L/K}$ ✓

Corollary 17.4 L/K finite + Abelian. Is unram $\Leftrightarrow N_{L/K}(O_L^\times) = O_K^\times$.

§ **Construction of Artin map.** (of $\mathbb{Q}_p$)

Recall: $\mathbb{Q}_p^{ur} = \bigcup_{m \geq 1} \mathbb{Q}_p(\zeta_{p^m-1}) = \bigcup_{p \nmid m} \mathbb{Q}_p(\zeta_m)$.

& $\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p$ is Totally ramified, degree $p^{m-1}(p-1)$, with

$\theta_n : Gal(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \xrightarrow{\cong} (\mathbb{Z}/p^n\mathbb{Z})^\times$.

& $\forall n \geq m \geq 1$: $\exists$ comm diag: ~~$Gal(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)$~~

$$\begin{array}{ccc} Gal(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) & \twoheadrightarrow & Gal(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) \\ \theta_n \downarrow \cong & & \theta_m \downarrow \cong \\ (\mathbb{Z}/p^n\mathbb{Z})^\times & \xrightarrow[\text{(canonical proj.)}]{} & (\mathbb{Z}/p^m\mathbb{Z})^\times \end{array}$$

Set: $\mathbb{Q}_p(\zeta_{p^\infty}) \equiv \bigcup_{n \geq 1} \mathbb{Q}_p(\zeta_{p^m})$, then $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$ Galois ⊐3

and hence: $\theta : Gal(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$.
(Sheet 4)

Have: $\mathbb{Q}_p(\zeta_{p^\infty}) \cap \mathbb{Q}_p^{ur} = \mathbb{Q}_p$
(totally ram; unram)

$\Rightarrow \exists$ iso. $Gal(\mathbb{Q}_p(\zeta_{p^\infty})\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$.

Theorem 17.5 (local Kronecker-Weber): $\mathbb{Q}_p^{ab} = \mathbb{Q}_p^{ur}\mathbb{Q}_p(\zeta_{p^\infty})$.

Construct: $Art_{\mathbb{Q}_p}$ by: note: $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$
$p^n u \mapsto (n, u)$.

Then $Art_{\mathbb{Q}_p}(p^n u) = ((Fr_{\mathbb{Q}_p^{ur}/\mathbb{Q}_p})^n, \theta^{-1}(u^{-1}))$
$\in Gal(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \times Gal(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong Gal(\mathbb{Q}_p^{ab}/\mathbb{Q})$
(by: Kronecker-Weber)

$\Rightarrow$ Image lies in: $W(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ (because: integral power of Frob.)

§ Construction of Art_K (general K)

K local field. For $\pi \in K$ unif: $\forall n \geq 1$, construct fields $K_{\pi,n}$ totally ramified over K, & Galois, s.t.

(i) $K \subseteq \dots \subseteq K_{\pi,n} \subseteq K_{\pi,n+1} \subseteq \dots$

(ii) $\forall m, n \geq 1$: $\exists$ comm diag:

$$\begin{array}{ccc} Gal(K_{\pi,n}/K) & \twoheadrightarrow & Gal(K_{\pi,m}/K) \\ \downarrow \cong (\Psi_n) & & \downarrow \cong (\Psi_m) \\ \mathcal{O}_K^\times / U_K^{(n)} & \xrightarrow{proj} & \mathcal{O}_K^\times / U_K^{(m)} \end{array}$$

(iii) Setting $K_{\pi,\infty} \equiv \bigcup_{n \geq 1} K_{\pi,n}$: then, $K^{ab} = K^{ur} K_{\pi,\infty}$.

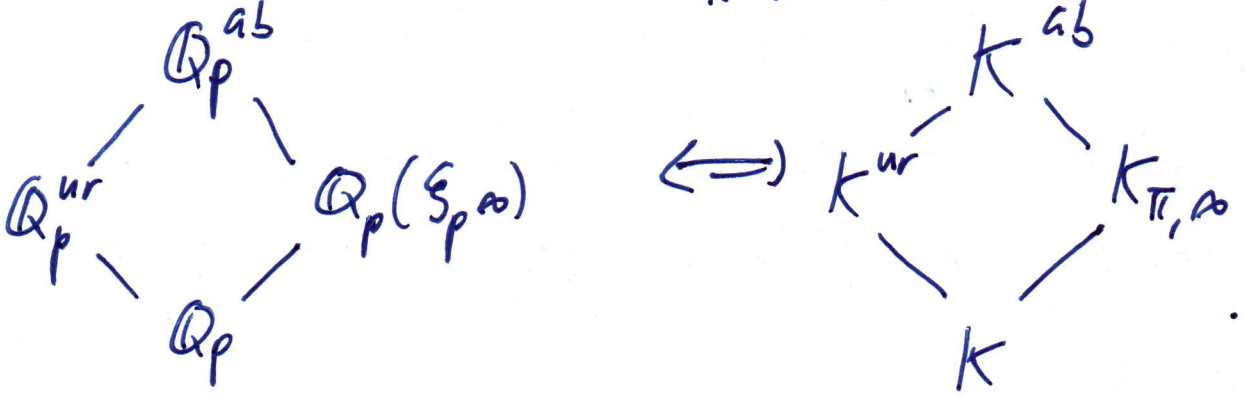
Local Fields: lecture 21

Construction continued

By Sheet 4 (Q1): $\exists$ iso. $\Psi: Gal(K_{\pi,\infty}/K) \xrightarrow{\cong} \varprojlim_n O_K/U_K^{(n)} \cong O_K^\times$

Define Art_K by:

$$K^\times \cong \mathbb{Z} \times O_K^\times \longrightarrow Gal(K^{ur}/K) \times Gal(K_{\pi,\infty}/K)$$
$$\pi^n u \longmapsto (n, u) \longmapsto \left((Fr_{K^{ur}/K})^n,\ \Psi^{-1}(u^{-1})\right)$$



Remark] No "maximal" totally ramified ext. of K.
Art_K depends on choice of $K_{\pi,\infty}$, and iso $K^\times \cong \mathbb{Z} \times O_K^\times$.
These choices are related: both depends on π, and "cancel out",
i.e. Art_K is canonical.

Goal: Construct $K_{\pi,n}$ $\forall n$.

VII: Lubin-Tate theory.

§18: Formal Group Laws.

R ring. $R[[X_1, \dots, X_n]] \equiv \left\{ \sum_{k_1,\dots,k_n \geq 0} a_{k_1,\dots,k_n} X_1^{k_1} \cdots X_n^{k_n} \right\}$, $a_{k_1,\dots,k_n} \in R$

DEF 18.1] A (1-dim) (commutative) formal group law (over R) is power series $F(X,Y) \in R[[X,Y]]$ s.t.

(i) $F(X,Y) \equiv X+Y \bmod$ (deg 2)

(ii) Assoc: $F(F(X,Y),Z) = F(X,F(Y,Z))$

(iii) Comm: $F(X,Y) = F(Y,X)$.

Examples: $\hat{\mathbb{G}}_a(X,Y) = X+Y$ (formal additive group)

$\hat{\mathbb{G}}_m(X,Y) = X+Y+XY$ (formal mult group)

Lemma 18.2: F formal group law $/R$.

(i) $F(X,0) = F(0,X) = X$

(ii) $\exists$ "inverses": $i(X) \in XR[[X]]$ s.t. $F(X, i(X)) = 0$

Point: If K complete + non-Arch local field, and F formal group laws over $\mathcal{O}_K$, then $F(X,Y)$ converges $\forall X,Y \in \mathfrak{m}_K$, to an element in $\mathfrak{m}_K$.

$\Rightarrow$ Defining $X \dot{+}_F Y \equiv F(X,Y)$ turns $(\mathfrak{m}_K, \dot{+})$ into comm group.

Example: $\hat{\mathbb{G}}_m / \mathbb{Z}_p$: $x \cdot y \equiv x+y+xy$. $\mathfrak{m} = p\mathbb{Z}_p$.

$\Rightarrow (p\mathbb{Z}_p, \cdot) \cong (1+p\mathbb{Z}_p, \times)$

$x \longmapsto 1+x$

DEF 18.3: Let F, G formal group laws $/R$.

A homomorphism $f: F \to G$ is element $f(X) \in XR[[X]]$, s.t.

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

f is isomorphism if $\exists g: G \to F$ hom, s.t. $f(g(X)) = X$ & $g(f(X)) = X$.

Define: $\mathrm{End}_R(F) \equiv \{\text{homs } F \to F\}$.

Prop 18.4: R is $\mathbb{Q}$-algebra. Then: $\exists$ iso. of formal group laws $\hat{\mathbb{G}}_a \longmapsto \hat{\mathbb{G}}_m$. (given by exp)

$\exp(X) = \sum_{n \geq 1} X^n/n!$ (No const term!)

Proof Define $\log(X) \equiv \sum_{n \geq 1} (-1)^{n-1} \frac{X^n}{n}$. Then $\exists$ equality of formal power series: $\log(\exp(X)) = X$ & $\exp(\log(X)) = X$.

& $\exp(\hat{\mathbb{G}}_a(X,Y)) = \hat{\mathbb{G}}_m(\exp(X), \exp(Y))$. ✓

[need $\mathbb{Q}$-algebra, since need divisible by $n!$ thing]

Lemma 18.5 $\mathrm{End}_R(F)$ is ring, with $f +_F g \equiv F(f(X), g(X))$ and mult $\equiv$ composition.

Proof $\forall f, g \in \mathrm{End}_R(F)$:

$$(f +_F g) \circ F(X,Y) = F(f(F(X,Y)), g(F(X,Y)))$$
$$= F(F(f(X), f(Y)), F(g(X), g(Y)))$$
$$= F(F(f(X), g(X)), F(f(Y), g(Y))) \quad (\text{comm + assoc})$$
$$= F(f +_F g(X), f +_F g(Y)). \quad \in \mathrm{End}(F)$$

$\Rightarrow f +_F g \in \mathrm{End}_R(F)$ ✓ (& $f \circ g \circ F = f \circ F \circ g = F \circ f \circ g$)

$\Rightarrow f \circ g \in \mathrm{End}_R(F)$

~~Theorem 19.~~ **§ Lubin-Tate Formal groups.**

Let: K local field & $|k| = q$.

DEF 19.1 A formal $\mathcal{O}_K$-module over $\mathcal{O}_K$ is a formal group law $F(X,Y) \in \mathcal{O}_K[[X,Y]]$, together with ring hom $[\cdot]_F : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$, s.t. $\forall a \in \mathcal{O}_K$, $[a]_F(X) \equiv aX \bmod X^2$

A hom/iso of formal ~~group laws~~ $\mathcal{O}_K$-modules $f : F \to G$ is hom/iso of

formal group laws s.t. $f \circ [a]_F = [a]_G \circ f \quad \forall a \in \mathcal{O}_K$.

DEF 19.2] $\pi \in \mathcal{O}_K$ unif. A ~~Rubber~~ Luben–Tate series for π is power series $f(X) \in \mathcal{O}_K[[X]]$ s.t.

a) $f(X) \equiv \pi X \bmod X^2$; b) $f(X) \equiv X^q \bmod \pi$

(Example: $\pi X + X^q$)

Theorem 19.3] $f \in \mathcal{O}_K[[X]]$ ~~Re~~ Luben–Tate for π.

(i) $\exists!$ F_f formal group law / $\mathcal{O}_K$, s.t. $f \in \mathrm{End}_{\mathcal{O}_K}(F_f)$

(ii) $\exists\, [\cdot]_{F_f} : \mathcal{O}_K \longrightarrow \mathrm{End}_R(F_f)$ ring hom s.t.

$\boxed{[\pi]_{F_f}(X) = f(X).}$ (Makes F_f into formal $\mathcal{O}_K$-module / $\mathcal{O}_K$)

(iii) If $g(X)$ another Luben–Tate series for π: then $F_f \cong F_g$ as formal $\mathcal{O}_K$-modules.

The F_f is: Luben–Tate formal group law, for π

(only depends on π, up to isomorphism.)

Local Fields: lecture 22.

Examples (of Theorem 19.3): $K = \mathbb{Q}_p$, $f(X) = (X+1)^p - 1$ is a LT-series for unif p.
& LT-formal group law is: $F_f = \hat{\mathbb{G}}_m$.
Since: $f(\hat{\mathbb{G}}_m(X,Y)) = (1+X)^p(1+Y)^p - 1 = \hat{\mathbb{G}}_m(f(X), f(Y))$.

lemma 19.4 (key lemma)
$f(X)$, $g(X)$ LT-series for π, & $L \equiv \sum_{i \le n} a_i X_i$ linear form, $a_i \in \mathcal{O}_K$.
Then: $\exists!\ F(X_1, \dots, X_n) \in \mathcal{O}_K[X_1, \dots, X_n]$ s.t.
(i) $F \equiv L \bmod$ (deg 2 terms)
(ii) $f(F(X_1, \dots, X_n)) = F(g(X_1), \dots, g(X_n))$.

Proof Idea: proof by approximation. Will show: by induction,
$\exists!\ F_m \in \mathcal{O}_K[X_1, \dots, X_m]$ total degree $\le m$, s.t.
(a) $f(F_m(X_1, \dots, X_n)) \equiv F_m(g(X_1), \dots, g(X_n)) \bmod$ deg $m+1$ terms
(b) $F_m \equiv L \bmod$ deg-2 terms
(c) $F_m \equiv F_{m+1} \bmod$ deg-$(m+1)$-terms.
Then, can get F by taking limit of these polynomials.
For $m=1$, take $f_1 = L$ ✓ (satisfies (b) trivially, and
$f(L(X_1, \dots, X_n)) \equiv \pi L(X_1, \dots, X_n) \bmod X^2$ ($f(X) \equiv \pi X \bmod X^2$)
$\equiv L(g(X_1), \dots, g(X_n))$ ✓)
Suppose $\{F_i\}_{i \le m}$ already constructed. Let: $F_{m+1} = F_m + h$,

For $h \in \mathcal{O}_K[X_1, \dots, X_n]$ homog & $\deg = m+1$.

Since $f(X+Y) = f(X) + f'(X)\cdot Y + Y^2(\dots)$:

& $f'(X) \equiv \pi \bmod X$ (due to $L-T$)

$\Rightarrow f \circ (F_m + h) \equiv f \circ F_m + \pi h \bmod \deg -(m+2)$

$(F_m + h) \circ g = F_m \circ g + h(\pi X_1, \dots, \pi X_n) \bmod \deg -(m+2)$

(using fact: $g(X) \equiv \pi X \bmod X^2$)

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

$\Rightarrow$ Satisfy (a), (b), (c) $\Leftrightarrow f \circ F_m - F_m \circ g \equiv (\pi - \pi^{m+1}) h \bmod \deg (m+2)$

But: $f \circ F_m - F_m \circ g \equiv F_m(X_1, \dots, X_n)^q - F_m(X_1^q, \dots, X_n^q) \bmod \pi$

(since $f, g \equiv X^q \bmod \pi$) $\equiv 0 \bmod \pi$.

So, set $h = \frac{1}{\pi(1-\pi^m)} r(X_1, \dots, X_n)$, where $r(X_1, \dots, X_n)$

is the $\deg -(m+1)$ terms of $f \circ F_m - F_m \circ g$.

$\Rightarrow F_{m+1}$ satisfies (a), (b), (c) ✓

Uniqueness: note h uniquely determined by (a) ✓

So, $F(X_1, \dots, X_n) \equiv \lim_{m \to \infty} F_m \in \mathcal{O}_K[[X_1, \dots, X_n]]$ satisfies (i)+(ii).

Uniqueness of F follows from uniqueness of F_m, since truncating the $\deg \le m+1$ terms of F recovers F_m ✓

Proof of Theorem 19.3)

(i) Lemma 19.4 $\Rightarrow \exists!\ F_f \in \mathcal{O}_K[[X,Y]]$ s.t.

$F_f(X,Y) \equiv X+Y \bmod \deg 2$ & $f(F_f(X,Y)) = F_f(f(X), f(Y))$.

$\square 2$

Then: F_f is a formal group law.

- Assoc: $F_f(X, F_f(Y,Z)) \equiv X+Y+Z \equiv F_f(F_f(X,Y),Z) \pmod{\deg 2}$.
- & $f \circ F_f(X, F_f(Y,Z)) = F_f(f(X), f \circ F_f(Y,Z))$
$= F_f(f(X), F_f(f(Y), f(Z)))$

& similarly, $f \circ F_f(F_f(X,Y),Z) = F_f(F_f(f(X), f(Y)), f(Z))$

$\Rightarrow$ By uniqueness of Lemma 19.4: have equality.

- Commutative: Similar to above.

(ii) By Lemma 19.4: $\forall a \in \mathcal{O}_K$, $\exists! [a]_{F_f} \in \mathcal{O}_K[[X]]$, s.t.

$[a]_{F_f} \equiv aX \pmod{X^2}$ & $f \circ [a]_{F_f} = [a]_{F_f} \circ f$.

Then: $[a]_{F_f} \circ F_f = F_f \circ [a]_{F_f}$ by uniqueness (show they have same linear terms + satisfy compatibility with LT.)

$\Rightarrow [a]_{F_f} \in \mathrm{End}_{\mathcal{O}_K}(F_f)$.

To show ring hom of $[\cdot]_{F_f}$: use uniqueness again.

$\Rightarrow F_f$ is formal $\mathcal{O}_K$-module / $\mathcal{O}_K$.

& $[\pi]_{F_f} = f$, since f has linear term πX.

(iii) If $g(X)$ another LT series for π: then find $\theta(X)$ in $\mathcal{O}_K[[X]]$ s.t. $\theta(X) \equiv X \pmod{X^2}$ & $\theta \circ f = g \circ \theta$

$\Rightarrow \theta \circ F_f = F_g \circ \theta$ (by uniqueness), so $\theta \in \mathrm{Hom}(F_f, F_g)$

Reversing role of f, g: find series $\theta^{-1} \in \mathcal{O}_K[[X]]$, $\theta^{-1} \in \mathrm{Hom}(F_g, F_f)$

and $\theta^{-1} \circ \theta(x) = X$ & $\theta \circ \theta^{-1}(x) = X$ by uniqueness ✓

To show $F_f \cong F_g$ as formal $\mathcal{O}_K$-modules:

$\theta \circ [a]_{F_f} = [a]_{F_g} \circ \theta \quad \forall a \in \mathcal{O}_K$ ✓

---

§20: Luben-Tate Extensions.

Let: $\overline{K}$ alg closure of K & $\mathfrak{m} \subseteq \mathcal{O}_{\overline{K}}$ maximal ideal.

Lemma 20.1 F formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. Then: $\overline{\mathfrak{m}}$ becomes (genuine) $\mathcal{O}_K$-module, with ops:

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

Proof (note: $\overline{K}$ not complete!)

$\forall x \in \overline{\mathfrak{m}}$: ~~$x \in \mathcal{O}_{\overline{K}}$~~ $x \in \mathfrak{m}_L$, some L/K finite.

$\Rightarrow$ Since $[a]_F \in \mathcal{O}_K[\![X]\!]$: $[a]_F(x)$ converges in L, and since $\mathfrak{m}_L$ closed, $[a]_F(x) \in \mathfrak{m}_L \subseteq \overline{\mathfrak{m}}$.

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

Module structure follows from def of formal $\mathcal{O}_K$-modules.

Local Fields: lecture 23

DEF 20.2] $F(X)$ LT-series for π. From last time: if $\bar{K}$ sep closure and $\mathfrak{m}_{\bar{K}} \in \mathcal{O}_{\bar{K}}$ max ideal, then $\mathfrak{m}_{\bar{K}}$ has structure of a $\mathcal{O}_K$-module.

Define: π^n-torsion group $\mu_{f,n} = \{x \in \mathfrak{m}_{\bar{K}} : \pi^n \cdot_{F_f} x = 0\}$

$= \{x \in \mathfrak{m}_{\bar{K}} : f_\bullet^{(n)}(x) = \underbrace{f_0 - \cdots \circ f}_{n}(x) = 0\}$.

Facts: $\mu_{f,n}$ is $\mathcal{O}_K$-module & nested. $\mu_{f,n} \subseteq \mu_{f,n+1}$.

Examples] $K = \mathbb{Q}_p$, $f(X) = (X+1)^p - 1$.

$\Rightarrow [p^n]_{F_f} = \underbrace{f_0 - \cdots \circ f}_{n} = (X+1)^{p^n} - 1$.

$\Rightarrow \mu_{f,n} = \{\zeta_{p^n}^i - 1 : 0 \le i \le p^n - 1\}$.

For $f(X) \equiv \pi X + X^q$ (LT for π): $f_n(X) = f_0 f_{n-1}(X)$

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

Set: $h_n(X) = \dfrac{f_n(X)}{f_{n-1}(X)} = \pi + f_{n-1}(X)^{q-1}$ ($\& f_0(X) = X$)

Prop 20.3] $h_n(X)$ separable & Eisenstein poly, deg $q^{n-1}(q-1)$.

Proof] Degree is clear (by induction)

Know: $f(X) \equiv X^q \bmod \pi$, so $h_n(X) \equiv f_{n-1}(X)^{q-1} \equiv X^{q^{n-1}(q-1)} \bmod \pi$

Since $f_{n-1}(X)$ has 0 const term: $h_n(X) = \pi + f_{n-1}(X)^{q-1}$ has constant term π, hence is Eisenstein ✓

For separable: since $h_n(X)$ irred: is separable if $\mathrm{char}(K) = 0$

or if $\mathrm{char}(K) = p$ & $h_n'(X) \neq 0$.

In 2nd case: induction on n.

- $n=1$: $h_1(X) = \pi + X^{q-1}$ is separable ✓
- If $h_1, \dots, h_{n-1}$ separable: $f_{n-1} = h_{n-1}(X) \circ_{f_1} h_1(X)$ separable, since product of irred separable polys of different degrees separable.

$\Rightarrow h_n(X) = \pi + f_{n-1}(X)^{q-1}$, so $h_n'(X) = (q-1) f_{n-1}'(X) f_{n-1}^{q-2}(X) \neq 0$ ✓

Next: need to understand module structure on $\mu_{f,n}$.

Prop 2.4 (i) $\mu_{f,n}$ free $(\mathcal{O}_K/\pi^n\mathcal{O}_K)$-module, rank 1

(ii) If g another LT-series for π then $\mu_{f,n} \cong \mu_{g,n}$ as $\mathcal{O}_K$-modules, and $K(\mu_{f,n}) = K(\mu_{g,n})$.

Proof (i) Take α root of $h_n(X)$. Since $h_n(X)$ & $f_{n-1}(X)$ coprime: α not root of f_{n-1}, so $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$.

Consider map $\tilde{\varphi}: \mathcal{O}_K \longrightarrow \mu_{f,n}$

$a \longmapsto a \circ_{F_f} \alpha$

Is: $\mathcal{O}_K$-module hom, with $\pi^n \mathcal{O}_K \subseteq \ker(\tilde{\varphi})$ (since α π^n-torsion)

& $\pi^{n-1} \circ_{F_f} \alpha \neq 0$ ($\alpha \notin \mu_{f,n-1}$)

$\Rightarrow \ker(\tilde{\varphi}) = \pi^n \mathcal{O}_K$, so $\tilde{\varphi}$ induces injection

$\mathcal{O}_K/\pi^n\mathcal{O}_K \xrightarrow{\varphi} \mu_{f,n}$.

Since f_{n-1} separable: $|\mu_{f,n}| = \deg(f_n) = q^n = |\mathcal{O}_K/\pi^n\mathcal{O}_K|$.

$\Rightarrow$ Rank 1.

(ii) Let $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(F_f, F_g)$ iso. of formal $\mathcal{O}_K$-modules.

$\Rightarrow$ θ induces: iso. $\theta : (m_{\bar{K}}, \overset{+}{F}_f) \longrightarrow (m_{\bar{K}}, \overset{+}{F}_g)$ of $\mathcal{O}_K$-modules. (using lemma 20.1)

$\Rightarrow$ θ induces iso. $\mu_{f,n} \cong \mu_{g,n}$.

Since $\mu_{f,n}$ algebraic: $K(\mu_{f,n})$ finite $/K$ $\Rightarrow$ complete, and $\theta(X) \in \mathcal{O}_K[\![X]\!]$.

$\Rightarrow \forall x \in \mu_{f,n}$: $\theta(x) \in K(\mu_{f,n})$, so $\mu_{g,n} \subseteq K(\mu_{f,n})$.

Applying opposite directions give $K(\mu_{g,n}) = K(\overset{+}{F}_f \mu_{f,n})$ ✓

(since now know $\mu_{g,n}$ algebraic)

DEF 20.5 $\boxed{K_{\pi,n} = K(\mu_{f,n})}$ (called: LT-extensions.

Remarks (i) $K_{\pi,n}$ depend only on π (not on f) (prop 20.4)

(ii) $K_{\pi,n} \subseteq K_{\pi,n+1}$ $\forall n$. $(\mu_{f,n} \subseteq \mu_{f,n+1})$

Prop 20.6 (i) $K_{\pi,n}/K$ totally ramified, Galois, degree $q^{n-1}(q-1)$

(ii) $\exists$ isoms $\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\cong} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times/U_K^{(n)}$

and ψ_n characterised by: $\psi_n(\sigma) \overset{+}{F}_f (x) = \sigma(x)$, $x \in \mu_{f,n}$.

Proof (i) Galois, since $K_{\pi,n}$ splitting field of $f_n(X)$ separable. $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$

For totally ramified: let α root of $h_n(X) = \dfrac{f_n(X)}{f_{n-1}(X)}$.

Suffices to show: $K(\alpha) = K(\mu_{f,n}) = K_{\pi,n}$. (since α root of Eisenstein poly, of correct degree $q^{n-1}(q-1)$)

$\subseteq$: clear, since $\alpha \in \mu_{f,n}$

$\supseteq$: By Prop 20.4: any $\chi \in \mu_{f,n}$ is of form $a \cdot_{F_f} \alpha$ for some $a \in \mathcal{O}_K$. (since rank 1 module) ($\alpha \in \mu_{f,n} - \mu_{f,n-1} \Rightarrow$ Generates)

So, $K(\alpha)$ complete & $[a]_{F_f} \in \mathcal{O}_K[[X]]$

$\Rightarrow \chi = [a]_{F_f}(\alpha) \in K(\alpha)$, so $\mu_{f,n} \subseteq K(\alpha)$ ✓

For characterisation: let $\sigma \in Gal(K_{\pi,n}/K)$. Then: σ preserves $\mu_{f,n}$ & acts continuously on $K_{\pi,n} = K(\mu_{f,n})$.

Since $F_f(X,Y) \in \mathcal{O}_K[[X]]$ & $[a]_{F_f} \in \mathcal{O}_K[[X]]$: ($\forall a \in \mathcal{O}_K$)

$\sigma(X +_{F_f} Y) = \sigma(X) +_{F_f} \sigma(Y)$

$\sigma([a]_{F_f} Y) = a \cdot_{F_f} \sigma(Y)$

} $\forall X,Y \in \mu_{f,n}$

$\forall X \in \mu_{f,n}$, $a \in \mathcal{O}_K$

(by continuity of σ)

$\Rightarrow \sigma \in Aut_{\mathcal{O}_K}(\mu_{f,n})$ (Aut as $\mathcal{O}_K$-module)

$\Rightarrow$ Induces group hom: $Gal(K_{\pi,n}/K) \xrightarrow{\Psi_n} Aut_{\mathcal{O}_K}(\mu_{f,n})$.

(Injective, since $K_{\pi,n} = K(\mu_{f,n})$)

Since $\mu_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$ as modules: Canonical

$\Rightarrow Aut_{\mathcal{O}_K}(\mu_{f,n}) \cong Aut_{\mathcal{O}_K/\pi^n\mathcal{O}_K}(\mu_{f,n}) \cong (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$

[using fact: $Aut_R(M) \cong R^\times$ $\forall M$ free rank-1 module / R]

$\Rightarrow$ Obtain Ψ_n: $Gal(K_{\pi,n}/K) \hookrightarrow (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ defined by:

$\Psi_n(\sigma) \in (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$ unique element, s.t. $\Psi_n(\sigma) \cdot_{F_f} x = \sigma(x)$.

($\forall x \in \mu_{f,n}$)

Local Fields: Lecture 24

Proof (continued).

Have: $[K_{\pi,n} : K] = q^{n-1}(q-1) = |(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times|$

$\Rightarrow \psi_n$ surjective (by counting), hence $\cong$.

Let: g another LT-series.

$\Rightarrow$ By similar argument: get $\psi_n' : Gal(K_{\pi,n}/K) \xrightarrow{\cong} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$

Find: $\theta : F_f \to F_g$ iso. of formal $\mathcal{O}_K$-modules.

$\Rightarrow$ Induces $\theta : \mu_{f,n} \xrightarrow{\cong} \mu_{g,n}$ of $\mathcal{O}_K$-modules

$\Rightarrow \forall x \in \mu_{f,n}$: $\theta(\psi_n(\sigma) \dot{}_{F_f} x) = \psi_n(\sigma) \dot{}_{F_g} \theta(x)$ (1)

But: $\theta \in \mathcal{O}_K[[X]]$ has coeffs in $\mathcal{O}_K$.

$\Rightarrow \theta(\sigma(x)) = \sigma(\theta(x))$ (σ continuous) $\forall x \in \mu_{f,n}$ & $\sigma \in Gal(K_{\pi,n}/K)$

$\Rightarrow \theta(\psi_n(\sigma) \dot{}_{F_f} x) = \theta(\sigma(x)) = \sigma(\theta(x)) = \psi_n'(\sigma) \dot{}_{F_g} \theta(x)$ (2)

(1)+(2) $\Rightarrow \psi_n(\sigma) \dot{}_{F_g} \theta(x) = \psi_n'(\sigma) \dot{}_{F_g} \theta(x)$

$\Rightarrow \psi_n(\sigma) = \psi_n'(\sigma)$ ✓

Set: $K_{\pi,\infty} \equiv \bigcup_{n \geq 1} K_{\pi,n}$.

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

Theorem 20.7 (Generalised local Kronecker–Weber)

$K^{ab} = K^{ur} \cdot K_{\pi,\infty}$. (proof omitted)

$K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times \longrightarrow Gal(K^{ab}/K) \times Gal(K_{\pi,\infty}/K) \cong Gal(K^{ab}/K)$

$\pi^n u \longrightarrow (n, u) \longmapsto \left(Fr^n_{K^{ur}/K},\ \psi^{-1}(u^{-1}) \right)$

Indep of choice of π.

§ Upper Numbering of ram groups

Let: L/K finite, Galois, & define $\phi \equiv \phi_{L/K} : \mathbb{R}_{\geq -1} \to \mathbb{R}$

$$\phi(s) = \int_0^s \frac{dt}{[G_0 : G_t]}.$$

Convention: for $t \in [-1, 0]$, $\dfrac{*\,1}{[G_0 : G_t]} = [G_t : G_0]$.

For $m \leq s \leq m+1$: $(m \in \mathbb{Z}_{\geq -1})$

$$\phi(s) = \begin{cases} s & m = -1 \\ \frac{1}{|G_0|}\left(|G_1| + \cdots + |G_m| + (s-m)|G_{m+1}|\right), & m \geq 0. \end{cases}$$

$\Rightarrow$ ϕ continuous & piecewise linear & strictly increasing.

$\Rightarrow$ Can define: $\psi_{L/K} \equiv \phi^{-1}_{L/K}$.

DEF 21.1 (Upper numbering)

Higher ram groups in upper numbering defined by:

$$G^s(L/K) \equiv G_{\psi_{L/K}(s)} \quad (L/K) \subseteq Gal(L/K).$$

Key point: $G_s(L/K)$ behave well WRT subgroups

$G^s(L/K)$ behave well WRT quotients.

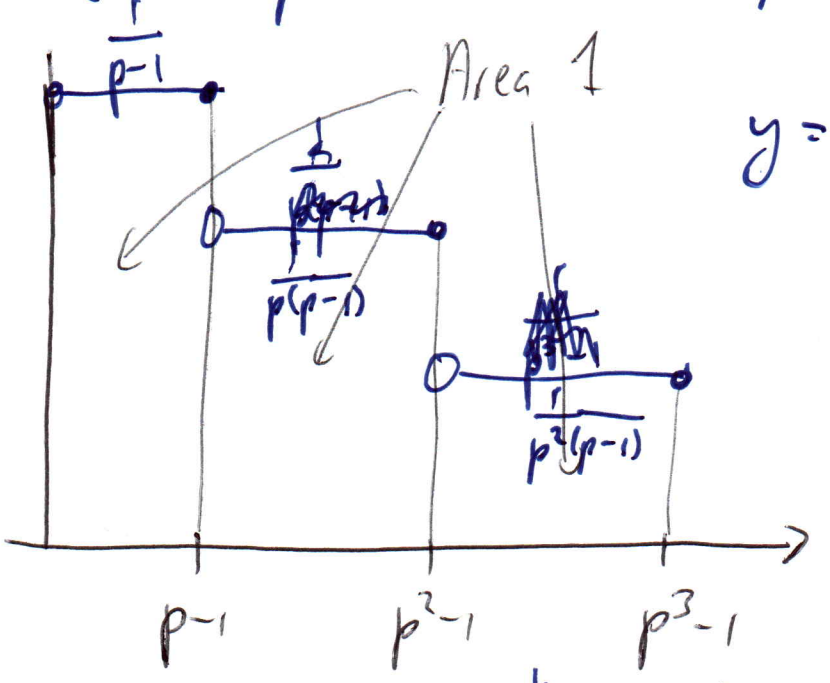
If $L/F/K$ exts & L/K finite & Galois: then

- $G_s(L/F) = G_s(L/K) \cap Gal(L/F)$
- If F/K Galois, then $G^t(L/K) \dfrac{Gal(L/F)}{Gal(L/K)} = G^t(F/K)$.

Example $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\zeta_{p^n})$.

For $1 \le k \le n-1$: & $p^{k-1} - 1 < s \le p^k - 1$:

$G_s = \{ m \in (\mathbb{Z}/p^n\mathbb{Z})^\times : m \equiv 1 \bmod p^k \} = U_{\mathbb{Q}_p}^{(k)} / U_{\mathbb{Q}_p}^{(n)}$.



$$y = \frac{\text{Area } 1}{[G_0 : G_1]}$$

Since G_s jumps at $p^k - 1$: $\phi_{L|K}$ linear on $[p^{k-1} - 1, p^k - 1]$

$\Rightarrow$ To compute $\phi_{L|K}$: suffices to compute $\phi_{L|K}(p^k - 1)$

$$\phi_{L|K}(p^k - 1) = \frac{p-1}{p-1} + \frac{p^2 - 1 - (p-1)}{p(p-1)} + \cdots = 1 + \cdots + 1 = k \quad (1 \le k \le n-1)$$

$$\Rightarrow G^s(L|K) \cong \begin{cases} (\mathbb{Z}/p^n\mathbb{Z})^\times & \text{if } s \le 0 \\ 1 + p^k\mathbb{Z}/p^n\mathbb{Z} & \text{if } k-1 < s \le k \\ \{1\} & \text{if } s > k-1 \end{cases}$$

$\Rightarrow G^{sk} \cong U_{\mathbb{Q}_p}^{(k)} / U_{\mathbb{Q}_p}^{(n)}$ (in particular)

(*) Seems more natural

(*) Jumps at integers (Hasse-Art)