Week 1. lec 1.

def: Absolute values:

on a field $|\cdot| \to \mathbb{R}_{\geq 0}$

$$\begin{cases} |x| = 0 \Leftrightarrow x = 0 \\ |xy| = |x||y| \\ |x+y| \leq |x| + |y|. \end{cases}$$

def: P-adic abs value

abs val on $\mathbb{Q}$.

if $x = 0$ $|x|_p = 0$

if $x = p^n \frac{a}{b}$, $\gcd(p, a) = \gcd(p, b) = 1$, then $|x|_p = p^{-n}$

lem. p-adic abs val is an abs val

1) $x = 0 \to |x|_p = 0$

$|x|_p = 0 \to x = 0$

2) $x = p^n \frac{a_1}{b_1}$ $y = p^m \frac{a_2}{b_2}$

$|x||y| = p^{-m} p^{-n}$

$xy = p^{m+n} \frac{a_1 a_2}{b_1 b_2}$ but $\gcd(a_1 a_2, p) = \gcd(b_1 b_2, p) = 0$

so $|xy|_p = p^{-(m+n)}$

3) $x = p^n \frac{a_1}{b_1}$ $y = p^m \frac{a_2}{b_2}$ WLOG $n \geq m$

$x+y = p^m \left(\frac{a_2}{b_2} + p^{n-m} \frac{a_1}{b_1} \right) = p^m \frac{a_2 b_1 + p^{n-m} a_1 b_2}{b_1 b_2}$ but $\gcd(b_1 b_2, p) = 1$

and $v_p(a_2 b_1 + p^{n-m} a_1 b_2) \geq 1$

$\leq p^{-m}$

def. equivalent absolute values

$|\cdot|_1$ is equivalent to $|\cdot|_2$ if they induce the same top.

def place absolute values $/ \sim$

Prop 3 equivalent conditions for equivalent absolute values.

1) $|x|$, $|x|'$ are equivalent.

2) $|x| < 1 \Leftrightarrow |x|' < 1$ $\forall x \in K$. remember $<$ vs $\leq$. It's the weaker one.

3) there exists $s \in \mathbb{R}_{>0}$ st $\forall x \in K$

$|x|^s = |x|'$

Proof.

1) → 2) $|x|<1 \Rightarrow \lim_{n\to\infty} |x|^n = 0$

$\Rightarrow \lim_{n\to\infty} |x|'^n = 0$ (same top)

$\Rightarrow |x|'<1$

$\lim |x|^n \to 0$ w.r.t. $|\cdot|$

$\lim |x|^n - |x|'^n \to 0$

$\lim |x|_1 \to 0 \Rightarrow \lim |x|_2 \to 0$. Proof. let $\epsilon>0$. Consider $B_2(0,\epsilon)$. written as union of $B_1(a_i, r_i)$. One contains 0. Say $B_1(0,r)$. get some $B_1(0,\epsilon_2) \subseteq B_1(0,r) \subseteq B_2(0,\epsilon)$ But $|x_n|_1 \to 0$. $\exists N>0$, $\forall n>N$, $|x_n|_1^n < \epsilon_2$. for this n, $|x_n|_1^n \subseteq B_2(0,\epsilon)$ so $|x_n|_2^n < \epsilon$. $|x_n|_2 \to 0$.

2) → 3)

If 3 true, get

$s \log |x| = \log |x|' \quad \forall x$

$s = \frac{\log |x|'}{\log |x|} \quad \forall x$

get constant s.

We show contradiction. Say 3 false. then get contradiction.

let $a, x \in K$ be elements s.t.

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

so $\frac{\log |a|}{\log |x|} < \frac{\log |a|'}{\log |x|'}$ so exists $\frac{m}{n} \in \mathbb{Q}$, $\frac{\log |a|}{\log |x|} < \frac{m}{n} < \frac{\log |a|'}{\log |x|'}$

so $n \log |a| < m \log |x|$ $\quad m \log |x|' < n \log |a|'$

$|a|^n < |x|^m$ $\quad |x|'^m < |a|'^n$ $\quad \left|\frac{a^n}{x^m}\right|' < 1$

$\frac{1}{|a|'^n} < \frac{1}{|x|'^m}$ $\quad 1 < \left|\frac{a^n}{x^m}\right|'$ $\quad$ ※

3) → 1) they have same open balls ⇒ form same topology.

2)⇒3) proof scheme.

1, 3 true → same log ratio

2, By contradiction, say diff log ratio

3, Squeeze $\frac{m}{n}$ in middle, multiply out

4, back to exponent

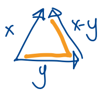
5, get <1 and >1.

def. non-archimedean

An absolute value is non-arch if $|a+b| \le \max(|a|,|b|) \quad \forall a,b$

lem all triangles are isosceles.

(long edges)



WLOG $|y| > |x|$

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

$|-x-y| = |x-y+y-y| \ge \max(|x-y+y|, |y|) = |y|$

lem. Condition to be cauchy

let $x_n \in K$. If $\lim_{n\to\infty} |x_n - x_{n+1}| \to 0$ then it's cauchy

let $\varepsilon > 0$. Pick N st $\forall n > N$, $|x_n - x_{n+1}| < \varepsilon$

then $\forall m_1, m_2 > N$, $|x_{m_1} - x_{m_2}| = |x_{m_1} - x_{m_1+1} + x_{m_1+1} - \cdots + x_{m_2-1} - x_{m_2}|$

$\le \max\left[(x_{m_1} - x_{m_1+1}), \cdots (x_{m_2-1} - x_{m_2})\right]$

$< \varepsilon$.

ex. a cauchy seq $\to -\frac{1}{3}$.

$a_1 = 3$, $a_2 = 33$, $a_3 = 333$, ----

$|a_n - a_{n+1}|_5 \to 0$ so cauchy

$a_i = \frac{10^i - 1}{3}$

$3a_i - 1 = 10^i$ in 5-adic, $|3a_i - 1|_5 \to 0$ $a_i \to \frac{1}{3}$ in 5-adic.

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

make a cauchy seq but not convergent to anything in $\mathbb{Q}$.

1) $a_n^2 + 1 \equiv 0 \pmod{5^n}$

2) $a_n \equiv a_{n+1} \pmod{5^n}$

$a_1 = 2$. Say a_n picked. Write $a_n^2 + 1 = 5^n \cdot c$

want to make a_{n+1} st. $(a_{n+1})^2 + 1 \equiv 5^{n+1}$ Set $a_{n+1} = a_n + b \cdot 5^n$.

so $(a_{n+1}^2 + 1) = (a_n + b5^n)^2 + 1 = \cancel{a_n^2} + b^2 5^{2n} + 2ba_n 5^n \cancel{+1}$

$= 5^n \cdot c + b^2 5^{2n} + 2a_n b 5^n$

$= b^2 5^{2n} + 5^n(\underbrace{c + 2a_n b}_{\text{want this } 0 \bmod 5.})$

$c \equiv 0 \to b \equiv 0$

$c \not\equiv 0$ but $\gcd(2a_n, 5) = 1$ as $a_n^2 + 1 \equiv 0 \bmod 5^n \Rightarrow a_n^2 + 1 \equiv 0 \bmod 5$

can pick a b.

now 1), 2) satisfied. a_n cauchy in 5-adic

But say if $\lim x_n = L \in \mathbb{Q}$ $\lim x_n^2 = L^2$ $-1 = L^2$ $\times$.

$|L^2 + 1| = |a_n^2 + 1| = 0 \Rightarrow L^2 \to -1$

Proof scheme: ① $\begin{cases} a_i \equiv a_{i+1} & (5^n) \\ a_i^2+1 \equiv 0 & (5^n) \end{cases}$

② try to make it. $a_1 = 2$

③ Write $a_i^2+1 = 5^n c$

④ Say $a_{i+1} = a_i + 5^n b$, try to satisfy $(a_i+1)^2+1 \equiv 0 \quad 5^{n+1}$

def. p-adic # $\mathbb{Q}_p$ is completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$.

lecture 2

lemma 1.9. 4 properties of non-arch val fields.

1) $B(x,r) = B(y,r)$ if $y \in B(x,r)$
2) $\bar{B}(x,r) = \bar{B}(y,r)$ if $y \in B(x,r)$
3) $B(x,r)$ is closed
4) $\overline{B(x,r)}$ is open

1) let $z \in B(x,r)$ then $|y-z| = |y-x+x-z| \le \max(|y-x|, |x-z|) < r$ so $z \in B(y,r)$
2) Same let $z \in \bar{B}(x,r)$, $|y-z| = |y-x+x-z| \le \max(|y-x|, |x-z|) \le r$ so $z \in \bar{B}(y,r)$.
3) $B(x,r)$ is closed

want to show $B(x,r)^c$ is open.

let $z \in B(x,r)^c$

Claim $B(z,r) \subset B(x,r)^c$

Suppose not. then $y \in B(z,r) \cap B(x,r)$

then $|x-z| = |x-y+y-z| \le \max(|x-y|, |y-z|) < r$. ※.

4) want to show $\bar{B}(x,r)$ is open.

let $y \in \bar{B}(x,r)$ claim $B(y,r) \subset \bar{B}(x,r)$

let $z \in B(y,r)$ then $z \in B(y,r) \subseteq B(x,r) \subseteq \bar{B}(x,r)$

Proof scheme: $\bar{B}$ open: Show $\subseteq$

B closed: Show B^c open.

§ valuation rings

<u>def valuation</u>

K field. a valuation on K is $v: K \to \mathbb{R}_{\geq 0}$

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

2) $v(xy) = v(x) + v(y)$

counting powers of p in element.

Valuation $\to$ abs value:

fix $\alpha \in (0,1)$. $|x| = \begin{cases} 0 & \text{if } x=0 \\ \alpha^{v(x)} & \text{o.w.} \end{cases}$

abs val $\to$ valuation:

$v(x) = \begin{cases} \text{undefined} & x=0 \\ \log_\alpha |x| & \text{o.w.} \end{cases}$ why? think: $|p^n|_p = p^{-n}$

$\log_{1/p}(|p^n|) = \log_{1/p}(p^{-n}) = n$

note: v_1, v_2 are equiv if $v_1 = cv_2$. $c \in \mathbb{R}_{\geq 0}$

p-adic valuation $v_p(x) = -\log_p |x|_p$

<u>defn: the t-adic valuation on Formal Laurent series.</u>

<u>defn: the Valuation ring</u>

given K a field. then $\mathcal{O}_K = \{x \in K^\times \mid v_p(x) \geq 0\} \cup \{0\}$.

$= \{x \in K \mid |x| \leq 1\}$

$= \overline{B(0,1)}$

$\mathcal{O}_K$ is a ring!

it has a unique max ideal $\{x \in K \mid |x| = 1\}$. $\mathcal{O}_K / m = k \leftarrow$ residue field.

<u>Prop. properties of $\mathcal{O}_K$.</u> (subring, units, ideals).

1) $\mathcal{O}_K$ is an open subring of K.

2) for $r \leq 1$, $\left.\begin{array}{l} \{x \in K \mid |x| < r\} \\ \{x \in K \mid |x| \leq r\} \end{array}\right\}$ are open ideals of $\mathcal{O}_K$

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

Proof: 1) $\mathcal{O}_K$ is open B/C it's closed.

a) $0, 1 \in \mathcal{O}_K$

b) $a \in \mathcal{O}_K$ $\quad |-a| = |-1||a| = |a| \leq 1$

c) $a, b \in \mathcal{O}_K$, $\quad |ab| = |a||b| \leq 1$

d) $a, b \in \mathcal{O}_K$ $\quad |a+b| \leq \max(|a|, |b|) \leq 1$

2) open close same thing again.

let $a \in \mathcal{O}_K$, $x \in I$ then $|ax| = |a||x| < r$

3) $\mathcal{O}_K^\times = \{1 \cdot 1 = 1\}$.

$\subseteq$ let $x \in \mathcal{O}_K^\times$. then $x^{-1} \in \mathcal{O}_K^\times$. $\quad |x||x^{-1}| = 1$ $\quad \Rightarrow |x| = 1$

$|x| \leq 1$, $|x^{-1}| \leq 1$

$\supseteq$ $|x| = 1$, $|x^{-1}| = 1$, so $x, x^{-1} \in \mathcal{O}_K \Rightarrow x \in \mathcal{O}_K^\times$.

Prop $\underline{m = \{x \in K \mid |x| < 1\}}$ is the max ideal and let $k = \mathcal{O}_K/m$ be the res field. $\quad (k \hookleftarrow \mathcal{O}_K \hookrightarrow K)$

Cor $\mathcal{O}_K$'s unique max ideal is m, hence $\mathcal{O}_K$ is a local ring

proof

why m is max ideal: if some element in m with $|x| \geq 1$, $|x||x^{-1}| = 1$. get whole thing.

let $m' \neq m$ be another max ideal.

let $x = m' \setminus m$ so its abs ≥ 1 $\times$.

example p-adic integers:

$K = \mathbb{Q}$. with $|\cdot|_p$. $\quad \mathcal{O}_K = \{x \in \mathbb{Q}, |x| \leq 1\}$ $\quad \mathbb{F}_p \hookleftarrow \mathbb{Z}_{(p)} \hookrightarrow \mathbb{Q}$

$= \{p^n \frac{a}{b}, n \geq 0\}$

$= \mathbb{Z}_{(p)} = \{\frac{a}{b} \mid p \nmid b\}$.

$m = \{x \in \mathbb{Q}, |x| < 1\} = p\mathbb{Z}_{(p)}$

$k = \mathcal{O}_K/m = \mathbb{F}_p$

defn: discrete valuation

let $v: K^\times \to \mathbb{R}_{\geq 0}$ be a valuation. Then v is discrete if

$v(K^\times) \cong \mathbb{Z}$

defn: uniformizer

$\pi \in \mathcal{O}_K$ is unif if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$

for any discrete valued ring, can always replace the valuation s.t. $v(K^\times) \cong \mathbb{Z}$.

lemma : 4 equivalent conditions of v discrete (v dis, $\mathcal{O}_K$ PID, Noe, m prin).

1) v is discrete
2) $\mathcal{O}_K$ is a PID
3) $\mathcal{O}_K$ is a Noetherian ring
4) m is principal

1)⇒2) $\mathcal{O}_K$ is ID. ✓

$\mathcal{O}_K$ is PID: let $I \subseteq \mathcal{O}_K$ be an ideal.

let $x \in I$ s.t. $v(x) = \min \{v(a) \mid a \in I\}$. existence b/c unique.

claim $x\mathcal{O}_K = I$.

$\subseteq$ $x \in I$, I is an ideal, so any $y \in \mathcal{O}_K$, $xy \in I$.

$\supseteq$. let $y \in I$. claim $x^{-1}y \in \mathcal{O}_K$. why? $v(x^{-1}y)$

so $y = x(x^{-1}y) \in x\mathcal{O}_K$ $= v(x^{-1}) + v(y)$

2)⇒3) By ring theory $= v(y) - v(x) \geq 0$

3)⇒4) $\mathcal{O}_K$ Noetherian ⇒ all ideals finitely generated, so $m = (x_1, \cdots x_n)$.

WLOG say $v(x_1) = \min_i v(x_i)$. Claim $m = x_1\mathcal{O}_K$. This is true as $x_i \in x_1\mathcal{O}_K$.

4)⇒1) Say $m = \pi\mathcal{O}_K$

let $c = v(\pi)$ $v(\pi^{-1}x) = v(x) - v(\pi)$ $\left\{ \begin{array}{l} \text{if } v(\pi) > v(x) \\ \text{then } x \notin \underbrace{\pi\mathcal{O}_K}_{\text{valuation} \geq c} \end{array} \right.$

if $v(x) > 0$, $x \in m$. $v(x) = v(\pi\pi^{-1}x) = c + v(\pi^{-1}x) \geq c$.

so $v(K^\times) \cap (0, c) = \phi$.

$v(K^\times) \subsetneq (\mathbb{R}, +)$ ⇒ $v(K^\times) = c\mathbb{Z}$.

rewrite 4) ⇒ 1)

$m = \pi\mathcal{O}_K$. claim $v(K^\times) \cap (0, c) = \phi$. if $v(x) > 0$, $x \in m$. then $x \in \pi\mathcal{O}_K$ ⇒

$v(x) \geq v(\pi) = c$. so claim proc.

hence $v(K^\times) \subsetneq (\mathbb{R}, +)$ ⇒ $v(K^\times) \cong \mathbb{Z}$.

Proof scheme

1) ⇒ 2) Show ideal is generated by smallest value element. one dir is find inverse.

3) ⇒ 4) noetherian rings 's ideals are f.g.

4) ⇒ 1) $v(K^\times) \cap (0,c) = \phi$.

lecture 3

note: $\mathrm{Frac}(\mathcal{O}_K) = K$

and that $\mathcal{O}_K[\frac{1}{x}]$ for any $x \in m$.

def DVR: a PID w/ exactly 1 nonzero prime ideal.

lem field to DVR & DVR to K to $\mathcal{O}_K$.

1) let v be a discrete valuation on a field K. then, $\mathcal{O}_K$ is a DVR.

2) Given DVR R, ∃ valuation v s.t. $K = \mathrm{Frac}(R)$ & $\mathcal{O}_K = R$.

(field + discrete valuation) → DVR $\mathcal{O}_K$

(DVR) → valuation s.t get K and $\mathcal{O}_K$

Proof 1) K a field, v a discrete valuation. want to show $\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}$ is DVR. Need to show PID & has one prime ideal.

PID: v discrete so $\mathcal{O}_K$ PID. ✓

One prime ideal: PID is where primes = max. But by prev thm, $\mathcal{O}_K$ has only max ideal.

2). let R be a DVR let m be its max id. let $M = (\pi)$. DVR are UFDs, so write $x \in R \setminus \{0\}$ uniquely as $\pi^n \cdot u$, $u \in K^\times$, $n \geq 0$

for any $x \in K \setminus \{0\}$, write uniquely as $x = \pi^n \cdot u$, $u \in K^\times$ $n \in \mathbb{Z}$.

define $v(\pi^m \cdot u) = m$ it's a valuation & $\mathcal{O}_K = R$.

Proof Scheme.

1. max = prime in PID
2. π be the element for PID, so write things uniquely

Def. Ring of $p$adic integers   Why exist?

$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ extends to $\mathbb{Q}_p$ discretely.

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

$\mathbb{Z}_p$ is $\mathcal{O}_K = \mathcal{O}_{\mathbb{Q}_p}$ and $p\mathbb{Z}_p$ is max ideal. nonzero ideals are $p^n \mathbb{Z}_p$. $n \geq 0$.

Prop relationship between $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$

↳ $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$ So $\mathbb{Z}_p$ is complete!

↳ " " " $\mathbb{Z}$ w.r.t. $|\cdot|_p$.

Proof: Want to show $\mathbb{Z}$ dense inside $\mathbb{Z}_p$

$$\mathbb{Z} \underset{\text{dense}}{\subseteq} \mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p \underset{\text{dense}}{\subseteq} \mathbb{Z}_p.$$

$\mathbb{Z} \underset{\text{dense}}{\subseteq} \mathbb{Z}_{(p)}$

let $\frac{a}{b}$, $p \nmid b$ in $\mathbb{Z}_{(p)}$.

want to find $x_i \in \mathbb{Z}$, st $bx_i \to a$ in $p$adic. $bx_i \equiv a \mod (p^n)$

we can pick $x_i = a \cdot b^{-1} \mod p^n$ as x^{-1} exists in each p^n.

$\mathbb{Q} \cap \mathbb{Z}_p \underset{\text{dense}}{\subseteq} \mathbb{Z}_p$ $\mathbb{Q}$ dense in $\mathbb{Q}_p$ but $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is open. so $\mathbb{Q} \cap \mathbb{Z}_p$ dense in $\mathbb{Z}_p$.

defn inverse limits

given
- $(A_n)_{n=1}^{\infty}$ sequence of sets/grps/rings
- $\varphi_n : A_{n+1} \to A_n$

then $\varprojlim_n A_n = \{ (a_n) \in A_n \mid \varphi_n(a_{n+1}) = a_n \}. \subseteq \prod_{i=1}^{\infty} A_i$

↳ sequences s.t. if given a big a_k, k big, you'll know all the $a_1, a_2, \cdots a_{k-1}$.

def proj map in $\varprojlim_n A_n$:

$$\theta_m \left(\varprojlim_n A_n \right) = A_m.$$

Prop universal property from a S/G/R to an inverse limit

let B be a SGR, with hom $\psi_n : B \to A_n$. S.t. follow commute for all n

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

there exist unique hom $\psi : B \to \varprojlim_n A_n$ s.t.

$$\begin{tikzcd} B \arrow[r, "\psi"] \arrow[rr, bend left, "\psi_n"] & \varprojlim_n A_n \arrow[r, "\theta_n"] & A_n \end{tikzcd}$$

$\theta_n \circ \psi = \psi_n$.   this commutes

proof define $\psi : B \to \prod_{i=1}^{\infty} A_i$ by $\psi(b) = (\psi_i(b))_{i=1}^{\infty}$

wanna show: 1) $\theta_n \circ \psi = \psi_n$ ✓

2) unique $\theta_n \circ f$ must be f_n and θ_n determines what is its value at A_n

3) satisfy inverse limit rule: $\varphi_n(f_{n+1}(b)) = f_n(b)$

Def I-adic completion, I-adic complete.

given R and I an ideal of R, the I-adic completion of R is $\varprojlim_n R/I^n$ by $R/I^{n+1} \to R/I^n$ by natural projection.

By universal property, exist $i: R \to \varprojlim_n R/I^n$.

a ring R is I-adicaly complete if i is an iso.

$\ker i = \bigcap_{n=1}^{\infty} I^n$

Prop let $(K, |\cdot|)$ be non-arch valued field. let $\pi \in \mathcal{O}_K$ be s.t. $|\pi|<1$. Assume K is complete w.r.t. $|\cdot|$. then,

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

2) any $x \in \mathcal{O}_K$ can be written as $\sum_{i=0}^{\infty} a_i\pi^i$ each $a_i \in A \subseteq \mathcal{O}_K$ is a set of equivalence class mod $\mathcal{O}_K/\pi\mathcal{O}_K$

moreover, any such $\sum_{i=0}^{\infty} a_i\pi^i$, $a_i \in A$ converges.

$\mathcal{O}_K$ complete: $\mathcal{O}_K$ closed and K complete, so $\mathcal{O}_K \subset K$ is complete.

Show that $i: \mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ is an iso.

injectivity: let $x \in \ker i$. so $x \in \bigcap \pi^n\mathcal{O}_K$. $v(x) \geq nv(\pi)$ $\forall n$. so $x=0$ b/c valuation is only undefined in 0.

Surjectivity: let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$. for each n, let y_n be a lift of x_n. then $y_{n+1} - y_n \in \pi^n\mathcal{O}_K$ so $v(y_n - y_{n+1}) = nv(\pi)$. So Cauchy. let $y = \lim y_n$. y maps to $(x_n)_{n=0}^{\infty}$ in $\varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$

hence surjective.

Proof second part: ex sheet 2

note: not discretely valued $\Rightarrow$ not always $\mathfrak{m}$-adicaly complete.

Cor every $x \in K$ can be written uniquely as $\sum_{i=-n}^{\infty} a_i \pi^i$, $a_i \in A$.
conversely, any such sequence converge & defines an element in K.

$K = \text{frac } \mathcal{O}_K$ so $\exists n \geq 0$ s.t. $\pi^n x \in \mathcal{O}_K$. then write $\pi^n x = \sum_{i=0}^{\infty} a_i \pi^i$

then write $x = \sum_{i=0}^{\infty} a_i \pi^{i-n}$

end of week 1

week 2 lec 1

$\mathbb{Z} \underset{\text{dense}}{\subseteq} \mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p \underset{\text{dense}}{\subseteq} \mathbb{Z}_p$

Cor $\begin{cases} \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \\ \text{all } x \in \mathbb{Q}_p \text{ can be written as } \sum_{i=n}^{\infty} a_i p^i,\ a_i \in \{0, \dots, p-1\} \end{cases}$

Pf 1: note: we know $\mathbb{Q}_p$ is complete, so we get $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p$

so it suffices to show $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p$.

we'll show that $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ for a fixed n.

let $f: \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map.

then $\ker(f) = \{x \in \mathbb{Z} \mid f(x) \in p^n\mathbb{Z}_p\} = \{x \in \mathbb{Z} \mid p^n | x\} = p^n\mathbb{Z}$

and f is surjective, as if we pick $y \in \mathbb{Z}_p/p^n\mathbb{Z}_p$. let $\bar{y} \in \mathbb{Z}_p$ be lift of y.

since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, pick $x \in \mathbb{Z}$ s.t. $|x - \bar{y}| < \frac{1}{p^n}$. So $f(x) = \bar{y} = y \mod p^n$

Pf 2: By prop every $x \in K$ can be written uniquely as $\sum_{i=n}^{\infty} a_i \pi^i$ of $a \in \mathcal{O}_K/\mathfrak{m}_{\mathcal{O}_K}$. so we take $a = \mathbb{Z}_p/p\mathbb{Z}_p$.

Thm Hensel's lemma

let K be complete, discrete valued field. let $f \in \mathcal{O}_K[x]$. Assume $\exists\ a \in \mathcal{O}_K$ s.t. $|f(a)| < |f'(a)|^2$. Then there exists unique $x \in \mathcal{O}_K$ s.t. $f(x) = 0$ and that $|x - a| < |f'(a)|$.

remember • condition: $|f(a)| < |f'(a)|^2$ • answer: $|x - a| < |f'(a)|$

Proof: let $\pi \in \mathcal{O}_K$ be the uniformizer.

let $r = v(f'(a))$ where v is normalized ($v(\pi) = 1$)

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

$$\begin{cases} f(x_n) \equiv 0 \mod \pi^{n+2r} \\ x_n \equiv x_{n+1} \mod \pi^{n+r} \end{cases}$$

Base construction take $x_1 = a$. WTS $f(x_1) \equiv 0 \mod \pi^{1+2r}$.

$|f(a)| < |f'(a)|^2$ implies that $v(f(a)) > 2v(f'(a)) = 2r$.

so $v(f(x)) = v(f(a)) \geq 2r+1$ so $f(x) \equiv 0 \mod \pi^{1+2r}$.

Inductive construction

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

need to show ① Prop 2 holds

② prop 1 holds

③ fraction lies in $\mathcal{O}_K$

① want $x_{n+1} \equiv x_n \mod \pi^{n+r}$

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

consider $v(f'(x_n))$. note that $x_1 \equiv x_2 \mod \pi^{1+r}$ and $x_2 \equiv x_3$ .... so $x_1 \equiv x_n \mod \pi^{1+r}$

so $f'(x_1) = f'(a) \equiv f'(x_n) \mod \pi^{1+r}$ but $r = v(f'(a))$ so $f'(x_n) \not\equiv 0 \mod \pi^{1+r}$. so $v(f'(x_n)) = r$.

$v(f(x_n)) \geq n+2r$. so $v\left(\frac{f(x_n)}{f'(x_n)}\right) \geq n+2r-r = n+r$.

$$\boxed{f(x+y) = f(x) + f'(x)y + g(x,y)y^2}$$

② want: $f(x_{n+1}) \equiv 0 \mod \pi^{n+1+2r}$

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

$v\left(\frac{f(x_n)}{f'(x_n)}\right) \geq n+r$ $2v(\cdot\cdot) \geq 2n+2r$

$$= \underbrace{f(x_n) + f'(x_n)\cdot\frac{-f(x_n)}{f'(x_n)}}_{=0} + \underbrace{g\left(f(x_n), \frac{-f(x_n)}{f'(x_n)}\right)\left(\frac{f(x_n)}{f'(x_n)}\right)^2}_{\text{By prev, know } \frac{f(x_n)}{f'(x_n)} \text{ has val} \geq n+2r+1}$$

$$\equiv 0 \mod \pi^{n+2r+1}$$

so now: done induction.

<u>complete thm.</u> x_n is Cauchy so $x_n \to x$. $f(x_n) \to 0$. f continuous $\Rightarrow f(x) = \lim f(x_n) = 0$.

and show $|x-a| < |f'(a)|$

$a \equiv x \mod \pi^{r+1}$ $x - a \equiv 0 \mod \pi^{r+1}$ so $v(x-a) \geq r+1 > r = v(f'(a))$.

<u>uniqueness</u>

let $x' \in \mathcal{O}_K$ be another $f(x') = 0$ and $|x'-a| < |f'(a)|$. let $\delta = x'-x \neq 0$.

$$\left.\begin{array}{l} |x'-a| < f'(a) \\ |x-a| < f'(a) \end{array}\right\} \Rightarrow |\delta| = |(x'-a)-(x-a)| \leq \max(|x'-a|, |x-a|) = |f'(a)|$$

on the other hand, $0 = f(x') = f(x+\delta) = \overset{0}{\overset{\shortparallel}{f(x)}} + \delta f'(x) + \underbrace{\delta^2 + \cdots}_{|\cdot| \leq |\delta|^2}$ so $0 = \delta f'(x) + \cdots$ $|\delta f'(x)| \leq |\delta^2|$

$\Rightarrow |f'(x)| < |\delta|$

but $a = x_1 \equiv x \mod \pi^{r+1}$ so $f'(a) \equiv f'(x) \mod \pi^{r+1}$ $\not\equiv 0$ so $|f'(a)| < |\delta|$.

Hensel proof scheme.

Statement: ① have $|f(a)| < |f'(a)|^2$. ② get $|x-a| < |f'(a)|$

Proof: set $r = v(f'(a))$. then setup is
- ① $f(x_n) \equiv 0 \mod \pi^{2r+n}$
- ② $x_n \equiv x_{n+1} \mod \pi^{n+r}$

induction
- Base: $x_1 = a$ show ① hold.
- inductive: construct. $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$
  - show ② holds, using $v(f'(a)) = v(f'(x_n))$
  - show ① hold $f(x_{n+1}) = f(x_n + c)$ using pow. ser. expansion.

    It canels out.

finishing theorem
- Cauchyness
- show $|x-a| < |f'(a)|$

uniqueness
- set $\delta = x - x'$.
  - use > & < argument on $|\delta|$ and $|f'(a)|$
  - $|x-a| < |f'(a)|$ & $|x'-a| < |f'(a)|$ $\Rightarrow$ one side.
  - $0 = f(x') = f(x+\delta)$ pow series expansion.

$\boxed{\text{key fake arg: } f'(x) = f'(x_n) = f'(a) \text{ with valuation } r.}$

Cor lifting root version of Hensel's lemma.

let $(K, |\cdot|)$ be complete, discretly valued field. let $f(x) \in \mathcal{O}_K[x]$. let $\bar{c} \in k$ be a simple root of $\bar{f} \in k[x]$. Then, $\exists\, x \in \mathcal{O}_K$ st $f(x) = 0$ and that $x \equiv \bar{c} \mod k$.

Proof: let $c \in \mathcal{O}_K$ be any lift. of $\bar{c}$. then $|f(c)| < |f'(c)|^2$ b/c $|f'(c)|^2 = 1$ (simple root) but $f(c) = 0 \mod \pi$. So Hensel gives us a root $x \in \mathcal{O}_K$ $f(x) = 0$.

Proof scheme

Take a lift. That lift plays a. use hensel.

Cor. Multiplicative structure of p-adic integers

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

✱ chris's notes

Pf: $p>2$.

consider $f(x)=x^2-b$.

$b\in(\mathbb{Z}_p^\times)^2 \Leftrightarrow \bar{b}\in(\mathbb{F}_p^\times)^2$

$\longrightarrow$ b a square in $\mathbb{Z}_p$. reducing $\to \bar{b}$ sq in $(\mathbb{F}_p^\times)^2$

$\longleftarrow$ lifting simple root.

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

why? $f:\mathbb{Z}_p^\times \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ is surj & has ker $(\mathbb{Z}_p^\times)^2$

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

But $\begin{cases} \mathbb{Z}_p^\times\times\mathbb{Z} \cong \mathbb{Q}_p^\times \\ (u,n)\mapsto p^n u. \end{cases}$ $\quad (\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_p^\times)^2\times 2\mathbb{Z}$

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

$\cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

$p=2$. no simple roots x^2-b

let $b\in\mathbb{Z}_2^\times$. consider $f(x)=x^2-b$.

$b\equiv 1 \mod 8$. $f(x)=x^2-b$.

$|f(1)|_2 = |1^2-b|_2 \leq 2^{-3}$ $\quad \Rightarrow f(x)$ has root in $\mathbb{Z}_2$.

$|f'(1)|_2^2 = |2|_2^2 = 2^{-2}$

so $b\in(\mathbb{Z}_p^\times) \Rightarrow b\equiv 1 \mod 8$. $\quad$ note: x is sq root in $\mathbb{Z}_2$ iff $x\equiv 1 \mod 8$.

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

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

reduction mod 8 $\quad \phi:\mathbb{Z}_2^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$. $\quad \ker(\phi)=(\mathbb{Z}_2^\times)^2$

now, retry on your own.

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

Proof: $p>2$.

① show $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times) \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$

consider $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$

· surjective ✓

· kernel : let $b \in \mathbb{Z}_p^\times$, s.t. $x^2-\bar{b}=0$ in $\mathbb{F}_p$. $\Leftrightarrow$ x^2-b has root in $\mathbb{Z}_p^\times$

$\Leftrightarrow$ $b \in (\mathbb{Z}_p^\times)^2$

But $\left.\begin{array}{l}\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z} \\ (\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_p^\times)^2 \times 2\mathbb{Z}\end{array}\right\} \Rightarrow \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_p^\times)/(\mathbb{Z}_p^\times)^2 \oplus \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^2$

② $\mathbb{Z}_2^\times \xrightarrow{\phi} (\mathbb{Z}/8\mathbb{Z})^\times$ ☆ 1 is the id in ring $(\mathbb{Z}/8\mathbb{Z})^\times$: 1, 3, 5, 7.

$\ker(\phi) = ?$

Claim $\ker(\phi) = (\mathbb{Z}_2^\times)^2$

$\ker(\phi) \in (\mathbb{Z}_2^\times)^2$. If $b \in \ker(\phi)$. then x^2-b has root by hensel using !

$(\mathbb{Z}_2^\times)^2 \subseteq \ker(\phi)$. odd # in $(\mathbb{Z}_2^\times)$'s sq must be 1 .

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

Proof scheme

note $\left.\begin{array}{l}\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z} \\ (\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_p^\times)^2 \times 2\mathbb{Z}.\end{array}\right\} \Rightarrow \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \times \mathbb{Z}/2\mathbb{Z}.$

then: in $p \neq 2$: $\mathbb{Z}_p^\times \longrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ with $\ker = (\mathbb{Z}_p^\times)^2$

then in $p=2$: $\mathbb{Z}_p^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ with $\ker = (\mathbb{Z}_p^\times)^2$.

thm Hensel version 2

let $(K, |\cdot|)$ be a complete discrete valued field. let $f(x) \in \mathcal{O}_K[x]$. let $\bar{f} \in k[x]$ be f reduced modulo m. If $\exists\, \bar{g}, \bar{h} \in k[x]$, $\bar{g}(x)\bar{h}(x) = \bar{f}(x)$. Then exists $g(x), h(x) \in \mathcal{O}_K[x]$ s.t. $f(x) = g(x)h(x)$ and $g \equiv \bar{g} \bmod m$, $h \equiv \bar{h} \bmod m$.

week 2 lec 2

Cor: a cor of 2^{nd} ver of Hensel.

let $(K, |\cdot|)$ be a CDVF. Then, let $f(x) \in K[x]$ write $f(x) = a_n x^n + \cdots + a_0$ s.t. $a_0, a_n \neq 0$.

If $f(x)$ irred, $|a_i| \leq \max\{|a_0|, |a_n|\}$ $\forall i$

Proof: Spare not. Scale $f(x) \in \mathcal{O}_K[x]$ s.t. $\max_i |a_i| = 1$. Then, let r be the minimal value s.t. $|a_r| = 1$. $0 < r < n$.

modulo m, all terms with $|\cdot| < 1$ disappear.

$$\overline{f(x)} = a_n x^n + a_{n-1} x^{n-1} + \cdots + \underbrace{x^r a_r}_{\text{no disappear}}$$

$$= x^r (\underbrace{a_n x^{n-r} + \cdots + a_r}_{\deg < n})$$ mod m. Two poly factors coprime.

then we get lift to $\mathcal{O}_K[x]$. ※

Proof Scheme. WLOG to $\mathcal{O}_K[x]$ s.t. $\max_i |r_i| = 1$. Then set for ※, then mod m & factor.

Teichmuller lifts

defn a ring R with $\text{char}(R) = p$ is perfect if $fr: x \to x^p$ is bijection.

$\hookrightarrow \mathbb{F}_{p^n}$, $\overline{\mathbb{F}_p}$ perfect fields.

thm Teichmuller lift thm

let K be complete DVF. let $k := \mathcal{O}_K/m$. If k has char p and k is perfect,

then, $\exists$ map $[\cdot]: k \to \mathcal{O}_K$ s.t

1) $[a] \equiv a$ mod m $\forall a$

2) $[ab] = [a][b]$ mod m $\forall a, b \in k$.

furthermore if K has char p, then $[\,]$ is a homomorphism.

lem. $(K, |\cdot|)$ as theorem, fix $\pi \in \mathcal{O}_K$ a uniformizer. then if $x, y \in \mathcal{O}_K$ and $k \geq 1$

if $x \equiv y$ mod π^k

$x^p \equiv y^p$ mod π^{k+1}

Proof of lem

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

then $x^p = (y + \pi^k u)^p$

$$= y^p + \underbrace{\binom{p}{1} y^{p-1} (\pi^k u) + \cdots + \binom{p}{p} (\pi^k u)^p}$$

but $p \in \pi \mathcal{O}_K$. So all $\equiv 0 \bmod \pi^{k+1}$

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

Proof of theorem

construct 1). let $a \in K$. define $y_i \in \mathcal{O}_K$ to be a lift of $a^{\frac{1}{p^i}}$. define $x_i = y_i^{p^i}$.

claim x_i is cauchy & $x_i \to x$ & x do not depend on y_i's choices.

↳ cauchy: $y_i \equiv y_{i+1}^p \bmod \pi$ $\quad (a^{1/p^i} = (a^{1/p^{i+1}})^p$

so by lemma, $y_i^{p^r} \equiv y_{i+1}^{p^{r+1}} \bmod \pi^r$

$r = i \Rightarrow$ $\underset{x_i}{\underset{\|}{y_i^{p^i}}} \equiv \underset{x_{i+1}}{\underset{\|}{y_{i+1}^{p^{i+1}}}} \bmod \pi^i$

So cauchy

↳ independent of lift ys.

Say $(x_i')_{i=1}^\infty$ arise from another choice of y_i' lifting a^{1/p^i}. Say $x_i' \to x'$.

consider $x_i'' = \begin{cases} x_i & i \text{ even} \\ x_i' & i \text{ odd} \end{cases}$ $\quad x_i''$ arise by lifting $y_i'' = \begin{cases} y_i & " \quad " \\ y_i' & " \quad " \end{cases}$

apply argument again, w.r.t. y_i, y_{i+1}' get that x_i'', is cauchy.

But $x'' \to x'$, $x'' \to x$. So $x' = x$.

satisfy 1): $x_i = y_i^{p^i} \equiv (a^{1/p^i})^{p^i} = a \bmod m$

Satisfy 2): let $b \in k$, $u_i \in \mathcal{O}_K$ be lifts of b^{1/p^i} let $z_i := u_i^{p^i} \to z = [b]$

$u_i y_i$ is lift of $a^{1/p^i} \cdot b^{1/p^i} = (ab)^{1/p^i}$

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

If K has char p, get that $[\,]$ is hom. $\quad (x+y)^p = x^p + y^p \; \forall x, y$.

If char $K = p$, $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$

then $[a+b] = \lim (y_i + u_i)^{p^i} = \lim (y_i^{p^i}) + (u_i^{p^i}) = \lim x_i + \lim z_i = [a] + [b]$.

$[0] = 0$, $[1] = 1$. ✓

uniqueness of the $[\cdot]$.

let $\phi: k \to \mathcal{O}_K$ then $a \in k$, $\phi(a^{1/p^i})$ is lift of a^{1/p^i} then

$$[a] = \lim_{\uparrow} \phi(a^{1/p^i})^{p^i} = \lim \phi(a_i) = \phi(a)$$

By prev arg if $\to a$

Proof Scheme

- construct $[\ ]$: $a \in k$, y_i lift of a^{1/p^i}, $x_i := y_i^{p^i}$
  - show x is cauchy using $y_i = y_{i+1}^p \bmod \pi$ & lemma
  - show do not depend on choice of y_i. (alternating sequence)
- satisfy 1
- satisfy 2
- if char $K = p$, $[\cdot]$ is a hom. $\to$ $y_i + u_i$ is lift of $a_i^{1/p^i} + b_i^{1/p^i} = (a+b)^{1/p^i}$
- $[\cdot]$ unique : using property of ϕ.

__example root of unity:__

If $K = \mathbb{Q}_p$, $[\cdot]: \mathbb{F}_p \to \mathbb{Z}_p$. $a \in \mathbb{F}_p^\times$ then $[a]^{p-1} = [a^{p-1}] = [1] = 1 \to [a]$ is a root of unity

__lem. roots of unity in CDVR__

let $(K, |\cdot|)$ be a CDVF. if $k := \mathcal{O}_K/m \subseteq \overline{\mathbb{F}_p}$ then $[a] \in \mathcal{O}_K^\times$ are roots of unit.

__Proof.__ $a \in k \Rightarrow a \in \mathbb{F}_{p^n}$ for some n.

$$[a]^{p^n-1} = [a^{(p^n-1)}] = [1] = 1$$

Idea: If residue field is subfield of $\overline{\mathbb{F}_p}$ then all lifts of k are roots of unity.

Thm $(K, |\cdot|)$ a CDVR w/ char $K = p > 0$. If k is perf then
$K \cong k((t))$

Idea K CDVF with char p. k perf. $\cong$ laurent series

Pf. Since $\mathcal{O}_K$ = frac F

Suffice to show $\mathcal{O}_K \cong k[[t]]$ let $\pi \in \mathcal{O}_K$ be a uniformizer.

let $[-] : k \to \mathcal{O}_K$ be teichmuller lift.

define $\phi : k[[t]] \longrightarrow \mathcal{O}_K$ be $\phi(\sum_{i=0}^{\infty} a_i t^i) = \sum_{i=0}^{\infty} [a_i] \pi^i$

ϕ is ring hom b/c K has char p.

ϕ is a bijection b/c ($\mathcal{O}_K$ uniquely written as).

Week 2 lec 3

Big theorem for field extensions

Thm given $(K, |\cdot|)$. CDVF, L/F finite extension of degree n. then,

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

$|\cdot|_L : L \to K$

$|y|_L = |N_{L/K}(y)|^{1/n} \quad \forall y \in L$

ii) L is complete w.r.t. $|\cdot|_L$.

def $N_{L/K}(y) = \det(\text{mult}_y)$ where mult_y is linear map $L \to L$ by mult by y.

$N_{L/K}(y) = \pm a_0^m$ where a_0 is constant term of min. poly and $m \geq 1$

def let $(K, |\cdot|)$ be non arch field. Then a norm on V, a v.s. of K can also be defined.

def. equivalent norms: two norms are equivalent if $\exists$ C, D s.t.

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

Note that equivalent norms induce same topology.

def Sup norm that arised from abs value.

let V be a f.d v.s. of K, $e_1, \dots, e_n$ a basis of V. Then define $\|x\|_{sup} = \max_i |x_i|$

where $x = \sum_i x_i e_i$

Prop. let $(K, |\cdot|)$ be complete, non-arch, V a f.d.v.s over K, then V is complete w.r.t. $\|\cdot\|_{sup}$.

Proof: let $(v_i)_{i=1}^{\infty}$ be cauchy in V. write $v_i = \sum_{j=1}^n x_j^i e_j$ then, by $\|\ \|_\infty$, we have $(\|x_i^j\|)_{j,i}^{\infty}$ is cauchy for each j. let $x_j^i \to x_j$ as K is complete.

then $\sum_j x_j e_j$ is lim v_i.

Thm. let $(K, |\cdot|)$ be complete, non-arch and V a f.d.v.s over K. Then, any two norms on V is equivalent. Also, V is complete w.r.t any norms as K is complete & any norm $\sim$ to supnorm.

Proof. norm $\sim$ is an $\sim$ relation. Suffice to show any $\|\cdot\| \sim \|\cdot\|_\infty$.

let $e_1, \cdots e_n$ be basis for V.

show that $\|x\| \leq D\|x\|_\infty$, set $D = \max_i \|e_i\|$

then
$$\|x\| = \|\textstyle\sum_{i=1}^n x_i e_i\|$$
$$\leq \max_i \|x_i e_i\|$$
$$\leq \max_i |x_i| \|e_i\|$$
$$\leq D\|x\|_\infty$$

now want to show $C\|x\|_\infty \leq \|x\|$

this needs induction on $n = \dim V$.

when $n=1$, $\|x\| = \|x_1 e_1\| = |x_1| \|e_1\|$ set $C = \|e_1\|$.

when $n>1$. Suppose that $n-1$ dim v.s. are complete. Then, we set each $V_i = \text{span}\langle e_1, \cdots \hat{e_i}, \cdots e_n \rangle$.

By induction, V_i is complete w.r.t. $\|\ \|$. So each $e_i + V_i$ is closed $\forall i$. Set $S = \bigcup_{i=1}^n e_i + V_i$

it's a closed subset not containing 0. So S's complement is open and contain 0. So $\exists C$ s.t. $B(0,C) \subset S^{comp}$.

now, write $x = \sum x_i e_i$. let j be index where $|x_j| = \|x\|_{sup}$. then $\frac{x}{x_j} \in e_j + V_j \in S$ so $\left\|\frac{x}{x_j}\right\| > C$

$\|x\| > C|x_j|$

completeness follows since V complete w.r.t. $\|\cdot\|_{sup}$. $= C\|x\|_\infty$.

Proof scheme.

one side: set $\max_i \|e_i\|$.

Other side: induction. set $V_i = \text{Span}\langle \hat{e_j} \rangle$ $S = \bigcup e_i + V_i$. $0 \notin S$ closed. find some $B(0,c) \in S^c$.

examine $\frac{x}{x_j}$ where $\|x_j\| = \|x\|_\infty$.

def $\mathcal{O}_L$

given field extension and abs value on L, define $\mathcal{O}_L = \{x \in L \mid |x|_L \leq 1\}$.

def $R \subseteq S$ rings then $s \in S$ is integral over R if $\exists f[x] \in R[x]$ monic, $f(s)=0$

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

example: int closure of $\mathbb{Z}$ inside $\mathbb{Q}[i]$ is $\mathbb{Z}[i]$.

def $R \subseteq S$ is integrally closed if integral closure of $R^{\text{int}(S)} = R$.

Prop. $R^{\text{int}(S)}$ is a subring of S, and it's integrally closed

lem. $(K, |\cdot|)$ is non-arch valued field. then $\mathcal{O}_K$ is int closed in K.

Pf let $x \in K$. $x \neq 0$. let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0 \in \mathcal{O}_K[x]$

if $|x| > 1$, then $|x^n| = |a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0|$

$|x| = |a_{n-1} + \cdots + a_1/x^{n-2} + a_0/x^{n-1}| \leq \max\{|a_i/x^{n-i-1}|\}$

≤ 1 b/c $|x| \geq 1$, $|a_i| < 1$.

Claim $\mathcal{O}_L = \mathcal{O}_K^{\,cl(L)}$ (prove later).

Proof of big thm

WTS $|y|_L = |N_{L/K}(y)|^{1/n}$ satisfy 3 axioms of abs value.

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

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

fact from 64 $\iff y = 0$

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

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

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

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

3) let $x, y \in L$. WLOG, $|x|_L \leq |y|_L$ so $\left|\frac{x}{y}\right|_L \leq 1$ $\frac{x}{y} \in \mathcal{O}_L$. By claim $\mathcal{O}_L$ is a ring,

so $1 + \frac{x}{y} \in \mathcal{O}_L$. $\left\|1 + \frac{x}{y}\right\|_L \leq 1 \Rightarrow |x+y|_L \leq |y|_L = \max\{|x|_L, |y|_L\}$.

Week 3 lec 1

lem $\mathcal{O}_K^{\mathrm{int}(L)} = \mathcal{O}_L$.

Proof

first show claim:

let $0 \neq y \in L$. let $f(x) \in K[x]$ be the min poly of y.

then, show claim

subclaim: y integral over $\mathcal{O}_K \Leftrightarrow f(x) \in \mathcal{O}_K[x]$.

pf of subclaim:

$\Leftarrow$ Clear

$\Rightarrow$ let $g(x) \in \mathcal{O}_K[x]$ be poly s.t. $g(y) = 0$. But f is min poly, $f | g$. all roots of f are roots of g.

$\Rightarrow$ all root of f in $\bar{K}$ is integral over $\mathcal{O}_K$. But coefficients can be written as a root of the same poly. So a_i integral over $\mathcal{O}_K$

$\mathcal{O}_K$ int closed $\Rightarrow a_i \in \mathcal{O}_K$.

now, having shown the subclaim, note: $|a_i| \leq \max(1, |a_0|)$

and $N_{L/K}(y) = \pm a_0^m \in \mathcal{O}_K$

$$\begin{aligned}
& y \in \mathcal{O}_L \\
\Leftrightarrow\ & |y|_L \leq 1 \\
\Leftrightarrow\ & |N_{L/K}(y)| \leq 1 \\
\Leftrightarrow\ & |a_0| \leq 1 \\
\Leftrightarrow\ & |a_i| \leq 1 \ \forall i \quad \text{(by prev cor)} \\
\Leftrightarrow\ & f(x) \in \mathcal{O}_K[x] \\
\Leftrightarrow\ & y \text{ is integral over } \mathcal{O}_K.
\end{aligned}$$

So $\mathcal{O}_K^{\mathrm{int}(L)} = \mathcal{O}_L$.

Proof scheme

subclaim: $y \in L$, then y integral over $\mathcal{O}_K \Leftrightarrow \overset{\text{min poly}}{f(x)} \in \mathcal{O}_K[x]$

using subclaim, $y \in L$, then $y \in \mathcal{O}_L \underset{\text{min poly stuff}}{\Leftrightarrow} y$ int over $\mathcal{O}_K \underset{\text{subclaim.}}{\Leftrightarrow} f(x) \in \mathcal{O}_K[x]$

Prop: uniqueness of extension of $|\cdot|$.

let $|\cdot|_L'$ be another abs extending $|\cdot|$ on L. viewed as norms, same top, so eq. abs values. then $|\cdot|_L^c = |\cdot|_L'$ $c \in \mathbb{R}_{\geq 0}$. But agree on K, so $c=1$.
completeness follow by vector space claim

Now, write $(K, |\cdot|)$ CDVF non-arch, discretely valued.

Cor let L/K be a finite extension.
i) L is discretely valued w.r.t. $|\cdot|_L$.
ii) $\mathcal{O}_L$ is integral closure of $\mathcal{O}_K$ in L.

Pf ii) shown earlier
i) $n = [L:K]$.
let $y \in L^\times$, $|y|_L = |N_{L/K}(y)|^{1/n}$

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

$$v_L(L^\times) \subseteq \frac{1}{n} v(K^\times) \subseteq \mathbb{Z}$$

So $v_L(L^\times)$ is discrete.

Cor let $\bar{K}/K$ be alg closure of K. Then $|\cdot|$ extends uniquely to an abs val on $\bar{K}$.

Proof: let $x \in \bar{K}/K$ let L be a finite extension of K that contains x.
let $|x|_{\bar{K}} = |x|_L$. uniqueness of $|x|_L$ is true by uniqueness from prev. thm.
uniqueness for $|x|_{\bar{K}}$ follow from uniqueness again.
note: $|\cdot|_{\bar{K}}$ is never discrete.

"downstairs is simple implies upstairs is simple"
Prop L/K finite field extension, CDVF if
1. $\mathcal{O}_K$ compact
2. k_L/k is finite & separable
then $\exists \alpha \in \mathcal{O}_K$ s.t. $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

does upstairs finite imply ?
$\Downarrow$

condition: the fields are CDVF, finite extension then $\begin{cases} k_L/k \text{ sep \& finite} \\ \mathcal{O}_K \text{ compact.} \end{cases}$

then $\mathcal{O}_K[\alpha] = \mathcal{O}_L$ for some $\alpha \in \mathcal{O}_L$.

Proof: k_L/k finite and separable implies simple, so $k_L = k[\bar{\alpha}]$. $\bar{\alpha} \in k_L$. pick $\alpha \in \mathcal{O}_L$ to be a lyft of $\bar{\alpha}$. let $\bar{g}$ be min poly of $\bar{\alpha}$ in $k[\bar{\alpha}]$. Then take $g \in \mathcal{O}_K[x]$ be lyft of $\bar{g}$.

fix $\pi_L \in \mathcal{O}_L$ a uniformizer. $\bar{g}(x) \in k[x]$ is irred & separable.

$$g(\alpha) \equiv 0 \mod \pi_K \Rightarrow g(\alpha) \equiv 0 \mod \pi_L$$

separability $\Rightarrow g'(\alpha) \not\equiv 0 \mod \pi_K \Rightarrow g'(\alpha) \not\equiv 0 \mod \pi_L$.

now, can pick α s.t. $v(g(\alpha)) = 1$. i.e. if $g(\alpha) \equiv 0 \mod \pi_L^2$ then consider

$$g(\alpha + \pi_L) = \underbrace{g(\alpha)}_{0 \bmod \pi_L^2} + \underbrace{\pi g'(\alpha)}_{\pi \bmod \pi_L^2} + \underbrace{\pi_L^2 \cdots}_{0 \bmod \pi_L^2} \quad \text{so} \quad v(g(\alpha + \pi_L)) = 1$$

This implies that can pick α s.t. $v(g(\alpha)) = 1$. let $\beta = g(\alpha)$. so β is a uniformize in L. $\beta \in \mathcal{O}_K[\alpha]$.

let $\psi: \mathcal{O}_K^n \to L \; (x_0, \cdots x_{n-1})$

$(x_1, \cdots x_n) \mapsto \sum_{i=0}^{n-1} x_i \alpha^i \qquad n = [K(\alpha):K]$

$\text{Im}(\psi) = \mathcal{O}_K[\alpha]$ it's compact. so $\mathcal{O}_K[\alpha]$ closed.

now, $k_L = k[\bar{\alpha}]$, $\mathcal{O}_K[\alpha]$ contains a set of coset reps for $k_L = \mathcal{O}_L/\pi_L\mathcal{O}_L = \mathcal{O}_L/\beta\mathcal{O}_L$.

so any $y \in \mathcal{O}_L$ can be written as $y = \sum_i n_i \beta^i$ $n_i \in \mathcal{O}_K[\alpha]$. each partial sum in $\mathcal{O}_K[\alpha]$, closedness implies that $y \in \mathcal{O}_L$.

Proof scheme

- Set $k_L = k(\bar{\alpha})$, lift $\bar{\alpha}$ and its min poly $\bar{g}(x)$.

  pick π_L a unif have $g(\alpha) \equiv 0 \mod \pi_L$ $g'(\alpha) \not\equiv 0 \mod \pi_L$

- pick $\pi_L + \alpha$ if needed s.t. $g(\alpha) \not\equiv 0 \mod \pi_L^2$
- set $\beta = g(\alpha) \in \mathcal{O}_K[\alpha]$.

  ↳ $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$ clear

  ↳ $\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$

  use $\psi: \mathcal{O}_K^n \to L(x_0, \cdots x_{n-1})$ to show ↳ $\text{im}\,\psi = \mathcal{O}_K[\alpha]$

  ↳ $\mathcal{O}_K[\alpha]$ closed

  $k_L = k(\bar{\alpha}) \Rightarrow$ can find repns for $\mathcal{O}_L/m_{\mathcal{O}_L} = \mathcal{O}_L/\beta\mathcal{O}_L$

  so $y = \sum n_i \beta^i$ $n_i \in \mathcal{O}_K[\alpha] \Rightarrow y \in \mathcal{O}_L[x]$.

Proof scheme again

- Set $k_L = k(\bar{\alpha})$ let α, $g(\alpha)$ be lift of $\bar{\alpha}$, and monic lift of min poly of $\bar{\alpha}$.
- properties of g: $g(\alpha) \equiv 0 \bmod \pi_L$, $g'(\alpha) \not\equiv 0 \bmod \pi_L$, pick α s.t. $g(\alpha) \not\equiv 0 \bmod \pi_L^2$, $v(g(\alpha)) = 1$.
- Set $\beta = g(\alpha) \in \mathcal{O}_K[\alpha]$.
- $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$: clear
- $\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$:
  - use $\theta : \mathcal{O}_K^n \to L(x_0, \cdots x_{n-1})$ to show $\operatorname{im}\theta = \mathcal{O}_K[\alpha]$, $\mathcal{O}_K[\alpha]$ closed.
  - show $\mathcal{O}_L/m = \mathcal{O}_L/\beta\mathcal{O}_L$ has repn in $\mathcal{O}_K[\alpha]$ using $k_L = k[\alpha]$.
  - so y = partial sum in $\mathcal{O}_L[\alpha]$ so done.

Week 3 lecture 2

local fields & global fields.

def. let $(K, |\cdot|)$ be a valued field.

K is local if it's complete & locally compact.

locally cpt: $\forall x \in K$, $\exists U$ open, s.t. $x \in U \subseteq Z$, Z compact. i.e. all $x \in K$ has a cpt nbd.

e.g. $\mathbb{R}$, $\mathbb{C}$ are local fields.

<u>Prop 7.2</u> let $(K, |\cdot|)$ be an non-arch complete valued field. TFAE:

1) K is locally compact
2) $\mathcal{O}_K$ is compact
3) v is discretely valued, $\mathcal{O}_K/m$ is finite.

pf: 1) → 2) since K is locally compact, let $0 \in U$ be a compact nbd of 0. Then, $\exists x \in \mathcal{O}_K$ s.t. $x\mathcal{O}_K \subseteq U$. $\mathcal{O}_K$ closed, $x\mathcal{O}_K$ closed. bdd → compact.

But $x\mathcal{O}_K \xrightarrow{x^{-1}} \mathcal{O}_K$ is a homeo. so $\mathcal{O}_K$ compact.

2) → 1) let $a \in K$. then $a + \mathcal{O}_K$ is a compact nbd of a.

2) → 3) $\mathcal{O}_K$ compact.

$\mathcal{O}_K/m$ finite : Let $x \in m$. (want unif?) Then let A_x be set of representatives of $\mathcal{O}_K/x\mathcal{O}_K$. Then $\mathcal{O}_K = \bigcup_{y \in A_x} y + x\mathcal{O}_K$ But $\mathcal{O}_K$ compact so A_x finite.

$\mathcal{O}_K/m = \mathcal{O}_K/x\mathcal{O}_K$ is finite.

v discrete: Suppose not, then $\exists x_1, x_2, x_3, \cdots$ $v(x_1) > v(x_2) > v(x_3) > \cdots > 0$

so $x_1\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq \cdots \subsetneq \mathcal{O}_K$ infinite seq. All subgroups of $\mathcal{O}_K/x_1\mathcal{O}_K$.

But as we showed it's a finite group. so X.

$3) \to 2)$. $\mathcal{O}_K$ metric space, suffice to show sequentially compact.

let $(x_n)_{n=1}^{\infty}$ be a seq in $\mathcal{O}_K$ fix $\pi \in \mathcal{O}_K$ a uniformizer.

note $\pi^i \mathcal{O}_K / \pi^{i+1}\mathcal{O}_K \cong k$. so each $\mathcal{O}_K/\pi^i\mathcal{O}_K$ is finite.

now, since $\mathcal{O}_K/\pi\mathcal{O}_K$ finite, $\exists a_1 \in \mathcal{O}_K/\pi\mathcal{O}_K$ & subseq $X_1 = (x_{1n})_{n=1}^{\infty}$ s.t. $x_{1n} \equiv a$ mod π. $\forall n$.

" $\mathcal{O}_K/\pi^2\mathcal{O}_K$ finite $\exists a_2 \in \cdot\cdot/\pi^2$ subseq of x_{1n}, x_{2n}, $x_{2n} \equiv a$ mod π^2 $\forall n$

By this fashion, construct subseq $(x_{in})_{n=1}^{\infty}$, s.t.

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

2) $\forall i$, $\exists a_i \in \mathcal{O}_K/\pi^i\mathcal{O}_K$ s.t. $x_{in} \equiv a_i$ mod π^i $\forall n$.

so $a_i \equiv a_{i+1}$ mod π^i, $\forall i$.

pick $y_i = x_{ii}$. This is a subseq of $(x_n)_{n=1}^{\infty}$

$$\left.\begin{aligned} y_i &\equiv a_i \text{ mod } \pi^i \\ &\equiv a_{i+1} \text{ mod } \pi^i \\ &\equiv y_{i+1} \text{ mod } \pi^i \end{aligned}\right\} \quad y_i \text{ cauchy. so } y_i \to y.$$

Proof scheme.

1) K is locally compact

2) $\mathcal{O}_K$ compact

3) $\mathcal{O}_K/m$ is finite & v discrete.

$1) \to 2)$ find nbd of 0, scale by x s.t. $x\mathcal{O}_K \subset U$.

$2) \to 1)$ $\forall a \in K$, $a + \mathcal{O}_K$ satisfy local compactness.

$2) \to 3)$ finite: $m \in \mathcal{O}_K$, let A_x be repn of $\mathcal{O}_K/x\mathcal{O}_K$. Then find cover to show $|A_x| < \infty$

discrete: if $v(x_1) \geq \cdots \geq v(x_n) \geq \cdots > 0$, get strict chain subgroups. But $\mathcal{O}_K/x_1\mathcal{O}_K$ is finite.

$3) \to 2)$ WTS seq. compact.

fix a uniformizer π. notice $\mathcal{O}_K/\pi\mathcal{O}_K$ finite so is $\mathcal{O}_K/\pi^i\mathcal{O}_K$.

given any $(x_n)_{n=1}^{\infty}$, pick $(x_{in})_{n=1}^{\infty}$ s.t.

1) $(x_{(i+1)n})_n$ is subseq of $(x_{in})_n$

2) $\forall i$, $\exists a_i \in \mathcal{O}_K/\pi^i\mathcal{O}_K$ s.t. $x_{in} \equiv a_i$ mod π^i.

$\Rightarrow a_i \equiv a_{i+1}$ mod π^i

pick $y = x_{ii}$ $\Rightarrow$ y cauchy. done.

More on inverse limits.

let $(A_n)_{n=1}^{\infty}$ seq of SGR, $\varphi_{n+1}: A_{n+1} \to A_n$ homs.

<u>def Profinite topology</u> on $A = \varprojlim_n A_n$ is the weakest top on A

s.t. proj maps $A \to A_n$ is cts $\forall n$, A_n is equipped w/ discrete topology.

i.e. weakest on A s.t. proj maps are cts. A_n finite w/ discrete top.

note A w/ profinite top is compact, totally disconnected, Hausdorff.

<u>Prop K be a nonarch</u> local field. Recall $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^k$ is iso.

We actually have it's an iso of topological spaces.

Proof: claim $B = \{a + \pi^n \mathcal{O}_K \mid a \in \mathcal{O}_K, n \in \mathbb{Z}_{\geq 1}\}$ is basis for $\mathcal{O}_K$ & $\varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$.

for $|\cdot|$: clear w.r.t. $|\cdot|$

for profinite top:

$\alpha \in \mathcal{O}_K/\pi^n \mathcal{O}_K$ is a basis b/c discrete top.

$\theta_n^{-1}\alpha = \alpha + \pi^n \mathcal{O}_K$. so θ_n cts $\Leftarrow \alpha + \pi^n \mathcal{O}_K$ open.

<u>lem K a nonarch local field.</u> If L/K finite, then L is also local.

<u>Proof</u> need to show L complete & locally compact. Complete shown. to show locally compact,

need to show L is $\underbrace{\text{discretely valued}}_{\text{shown}}$ + finite.

It remains to show $k_L = \mathcal{O}_L/\mathfrak{m}$ is finite.

let $\alpha_1, \dots, \alpha_n$ be a basis of L over K. note since $\|\cdot\|_{sup}$ w.r.t. this basis is

equivalent to the abs on L. hence, by equivalence of norms, $\exists r > 0$ s.t.

$\mathcal{O}_L \subseteq \{x \in L \mid \|x\|_{sup} \leq r\}$. take $a \in K$, $|a| > r$, then

$\{\|x\|_{sup} \leq r\} \subseteq \bigoplus a \cdot \alpha_i \mathcal{O}_K$.

each component $\leq r \Rightarrow$

$\in a \cdot \alpha_i \mathcal{O}_K$

$\mathcal{O}_L \leq \bigoplus_{i=1}^{n} a \cdot \alpha_i \mathcal{O}_K$

basis

$|\;|_L \leq |$ $\quad$ $|a\mathcal{O}_K| = |a||\mathcal{O}_K| > r \cdot 1 = r$

write $\mathcal{O}_L$ is a f.g. $\mathcal{O}_K$ module. $\mathcal{O}_K$ Noetherian $\Rightarrow$ k_L finitely generated k-module.

so k_L is finite.

Proof scheme.

- remains to show k_L is finite.
- let $a_1, \dots, a_n$ be basis
- note by $=$ of norm, $\mathcal{O}_L \subseteq \{x \in L \mid \|x\|_{sup} < r\} \subseteq \bigoplus a_i \cdot a \cdot \mathcal{O}_K$

  $\Downarrow$ each component of x is at most r as sup.

  $a \in K$ be $|a| > r$ ($\Uparrow$ sup norm.)

- So $\mathcal{O}_L$ f.g. $\mathcal{O}_K$ mod, k_L f.g. k mod $\to$ k_L finite

def a non-arch valued field $(K, |\cdot|)$ has $=$ char if char $K =$ char k

mixed o.w.

Thm K a non-arch real field of $=$ char $p > 0$. then $K \cong \mathbb{F}_{p^n}((t))$

K complete ✓ DVR ✓ of $+$ char ✓

K char p ✓ k is perfect because k is finite. Since k char p, $k \cong \mathbb{F}_{p^m}$ $m \geq 1$.

So by the thm of Teichmuller lift, $K \cong \mathbb{F}_{p^m}((t))$

lem absolute values on K is non arch $\Leftrightarrow$ $|n|$ is bdd $\forall n \in \mathbb{Z}$

pf $\Rightarrow$ $|n| = |1+1+\dots+1| \leq \max\{|1|\}$ bounded.

$\Leftarrow$ Say $|n| \leq B$ $\forall n \in \mathbb{Z}$.

let $x, y \in K$ be arbitrary. WLOG, $|x| \leq |y|$

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

But taking root, $|x+y| \leq (m+1)^{1/m} B^{1/m} |y| \to |y|$ as $m \to \infty$.

$\Rightarrow |x+y| \leq |y|$

Proof scheme

- one side is clear.
- another side: $\hookrightarrow$ set $B \geq |n|, \forall n \in \mathbb{Z}$

  $\hookrightarrow$ compute $|(x+y)^m|$ and take roots.

Scratch:

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

$$\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$$
$$u^n \leftrightarrow (u, n)$$

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times \qquad p>2.$$

$\mathbb{Z}_p^\times \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ has kernel $(\mathbb{Z}_p^\times)^2$

so $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$

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

Week 3 lec 3

thm Ostrowski's thm

Any nontrivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or p-adic absolute value for some prime p.

Proof :

Case I: $|\cdot|$ is archimedean.

↳ $|\cdot|$ unbounded, find $b \in \mathbb{Z}$ s.t. $|b| > 1$. let $a \in \mathbb{Z}$, let a be s.t. $a > 1$

↳ write b^n in base a.

$b^n = c_m a^m + c_{m-1} a^{m-1} + \cdots + c_1 a^1 + c_0$ each c_i has $0 \le c_i < a$, $c_m \neq 0$.

↳ take bounds

write $B = \max_i |c_i|$ then $|b^n| \le (m+1) \cdot B \cdot \max(1, |a|^m)$

↳ take n^{th} roots and logs.

$a^m \le b^n$

$m \le n \log_a b$

so $|b^n| \le (n \log_a b + 1) \cdot B \cdot \max(1, |a|^{n \log_a b})$

$|b| \le \underbrace{(n \log_a b + 1)^{1/n}}_{\to 1} \cdot \underbrace{B^{1/n}}_{\to 1} \cdot \max(1, |a|^{\log_a b})$

$n \to \infty$,

So $|b| \le \max(1, |a|^{\log_a b})$ but $|b| > 1$ so

$|b| \le |a|^{\log_a b}$, switching roles, $|a| \le |b|^{\log_b a}$

$\frac{\log |b|}{\log |a|} = \log_{|a|} |b| \le \log_a b = \frac{\log b}{\log a}$, $\frac{\log |a|}{\log |b|} = \log_{|b|} |a| \le \log_b a = \frac{\log a}{\log b}$

get $\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} = \eta$ $\quad |\alpha| = \alpha^\eta \ \forall \alpha \in \mathbb{Z}, \to |x| = x^\eta \ \forall x \in \mathbb{Q}$.

so $|\cdot|$ equiv to $|\cdot|_\infty$.

Case II: $|\cdot|$ is nonarchimedean.

We have $\forall n \in \mathbb{Z}$, $|n| \le 1$. But b/c non-discrete, $\exists$ $n \in \mathbb{Z}_{>1}$ be $|n| < 1$.

write $n = p_1^{e_1} \cdots p_r^{e_r}$ then, exists some p, s.t. $|p| < 1$, $p \in \{p_1, \cdots p_n\}$.

p is the only prime w $|\cdot| < 1$. if there are two of them, p, q, s.t. $p \neq q$,

$|p| < 1$, $|q| < 1$ then $1 = |ps + qt| \le \max(|ps|, |qt|) < 1$. ※.

So $|p| = \alpha < 1$, $|q| = 1$ $\forall$ other prime q. So $|\cdot|$ equiv $|\cdot|_p$.

Proof scheme

Case I: archimedean: ↳ pick integers $a, b > 1$, $|b| > 1$

↳ write b^n in base a. bound coefficients with C.

↳ $a^m \le b^n$, $m \le n \log_a b$.

↳ rewrite bound, take $1/n^{th}$ root

↳ take $n \to \infty$ $|b| \le |a|^{\log_a b}$ swap roles, take log,

so same ratio, extend to $\mathbb{Q}$, so $\cong$ metric.

case II: non-archimedean

↳ all $n \in \mathbb{Z}$, $|n| \le 1$ pick n, $|n| < 1$

↳ write $n = p_1^{a_1} \cdots p_k^{a_k}$

↳ one p_i has $|\cdot| < 1$. if two p_i has $|\cdot| < 1$ then contradiction

↳ so $|p_i| < 1$, $|p_j| = 1, \forall j \ne i$.

↳ $\sim$ to p-adic.

Thm let $(K, |\cdot|)$ be a non-arch, local field, of mixed char, then K is a finite extension of $\mathbb{Q}_p$ for some p prime.

K mixed character $\Rightarrow$ char $K = 0$, $\mathbb{Q} \subseteq K$.

K non-arch $\Rightarrow$ $|\cdot| \sim |\cdot|_p$ for some p prime

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

so need to show $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}_p$-module.

let $\pi \in \mathcal{O}_K$ be unif, let v be normalized valuation on K. $v(\pi) = 1$. let $v(p) = e$ then

$\mathcal{O}_K / p\mathcal{O}_K = \mathcal{O}_K / \pi^e \mathcal{O}_K$ is finite since each $\pi^i \mathcal{O}_K / \pi^{i+1} \mathcal{O}_K$ is.

$\mathcal{O}_K / p\mathcal{O}_K$ is a f.d. $\mathbb{F}_p$ vector space. let $x_1, \cdots x_n \in \mathcal{O}_K$ be set of coset repn for $\mathbb{F}_p$ basis $\mathcal{O}_K / p\mathcal{O}_K$. Then, $\sum a_i x_i$, $a_i \in \{0, \cdots p-1\}$ is a set of coset repn for $\mathcal{O}_K / p\mathcal{O}_K$.

any $y \in \mathcal{O}_K$ has power series

$y = \sum_{i=0}^{\infty} \sum_{j=1}^{n} a_{ij} x_n p^i = \sum b_j x_j$ so x_j form $\mathbb{Z}_p$ basis of $\mathcal{O}_K$.

↑ <u>continue from above: show $\mathcal{O}_K$ is finite as a $\mathbb{Z}_p$ module.</u>

$\pi \in \mathcal{O}_K$ uniformizer. v a normalized valuation on K. $v(p) = e$.

$\mathcal{O}_K / p\mathcal{O}_K = \mathcal{O}_K / \pi^e \mathcal{O}_K$ is finite, since $\pi^i \mathcal{O}_K / \pi^{i+1} \mathcal{O}_K \cong \mathcal{O}_K / \pi \mathcal{O}_K$ finite.

$\mathbb{F}_p = \mathbb{Z}_p / p\mathbb{Z}_p \xhookrightarrow{\text{injects into}} \mathcal{O}_K / p\mathcal{O}_K$ so $\mathcal{O}_K / p\mathcal{O}_K$ is a $\mathbb{F}_p$ vector space.

it's finite as a group, so it's a finite dim $\mathbb{F}_p$ vec. space.

let $x_1, \dots, x_n \in \mathcal{O}_K$ be <u>coset repn of $\mathbb{F}_p$ basis</u> for $\mathcal{O}_K / p\mathcal{O}_K$.

then $\{ \sum_{j=1}^{n} a_j x_j \mid a_i \in \{0, 1, \dots, p-1\} \}$ is a set of coset repns for $\mathcal{O}_K / p\mathcal{O}_K$.

let $y \in \mathcal{O}_K$. By 3.5 again,

$$y = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{n} a_j x_j \right) p^i \quad a_i \in \{0, \dots, p-1\}.$$

$$= \sum_{j=1}^{n} \Big(\underbrace{\sum_{i=0}^{\infty} a_{ij} p^i}_{\in \mathbb{Z}_p} \Big) x_i$$

$\Rightarrow \mathcal{O}_K$ finite over $\mathbb{Z}_p$.

Example Sheet 2: K complete $\Rightarrow$ $K \cong \mathbb{C}$ or $\mathbb{R}$.

Proof scheme

1. WTS $\mathcal{O}_K$ is f.g. as $\mathbb{Z}_p$ module.
2. $\mathbb{F}_p \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K$ & $\mathcal{O}_K/p\mathcal{O}_K$ is finite $\Rightarrow$ f.d. $\mathbb{F}_p$ vector space.
3. use power series rearrangement.

Summary any local fields are isomorphic to

1) $\mathbb{R}$, $\mathbb{C}$ (arch)
2) $\mathbb{F}_{p^m}((t))$ (non-arch, = char)
3) finite ext of $\mathbb{Q}_p$ (non arch, mixed char).

§ Global fields

def Global field.

A global field is either

i) an algebraic number field. (finite extension of $\mathbb{Q}$)

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

lem Same absolute value under the image of the Galois group.

$(K, |\cdot|)$ be complete DVR. L/K finite Galois extension with $|\cdot|_L$ extending $|\cdot|$.

then, for $x \in L$, $\sigma \in \mathrm{Gal}(L/K)$ $|\sigma(x)|_L = |x|_L$.

Proof: note that $|x|' = |\sigma(x)|_L$ is another absolute value on L extending K. using uniqueness of $|\cdot|_L$, we have $|x|' = |x|_L$.

lem. Krasner's lemma

$(K, |\cdot|)$ a complete DVF. let $f(x) \in F[x]$, be a separable, irreducible polynomial, with $\alpha_1, \cdots \alpha_n \in \bar{K}$ (separable closure of K)

Suppose $\beta \in \bar{K}$ with $|\beta-\alpha_1| < |\beta-\alpha_i|$ for $i=2,3,\dots n$ then $K(\alpha_1) \subseteq K(\beta)$

<u>Proof</u> let $L=K(\beta)$, $L'=L(\alpha_1,\dots \alpha_n)$ then, L'/L is galois. let $\sigma \in Gal(L'/L)$.

have $|\beta-\sigma(\alpha_1)| = \underset{\text{since } \beta \in L}{|\sigma(\beta)-\sigma(\alpha_1)|} = |\sigma(\beta-\alpha_1)| = |\beta-\alpha_1|$

must have $\forall \sigma \in Gal$, σ fix α_1 $\Rightarrow$ $\alpha_1 \in L=K(\beta)$.

Proof scheme: look at $K(\beta)(\alpha_1,\dots,\alpha_n)$

<u>Prop. Nearby polynomials define same extensions</u>

$(K,|\cdot|)$ complete discrete valuation fields. let $f(x)=\sum_{i=0}^m a_i x_i \in \mathcal{O}_K[x]$ be sep, irred, monic.

fix $\alpha \in \bar{K}$ a root of K.

then $\exists\ \epsilon > 0$ s.t. $\forall\ b_0,\dots b_m$, $g(x)=\sum_{i=0}^m b_i x_i \in \mathcal{O}_K[x]$, monic, with $|a_i-b_i|<\epsilon$, $\exists$ root β of g

s.t. $K(\alpha)=K(\beta)$.

<u>Proof</u>: let $\alpha=\alpha_1, \alpha_2, \dots \alpha_n \in \bar{K}$ be root of f. they're distinct b/c separable. so $f'(\alpha_1)\neq 0$.

Pick ϵ sufficiently small s.t. for $|b_i-a_i|<\epsilon$, $\underbrace{|g(\alpha_1)|}_{\text{defined by } \beta} < \underbrace{|f'(\alpha_1)^2|}_{\text{nonzero.}}$ and $\underbrace{|f'(\alpha_1)-g'(\alpha_1)|}_{\substack{g \text{ sufficiently close to } f'(\alpha_1)\\ \text{so have same sign.}}} < |f'(\alpha_1)|$

$f(\alpha_1)=0$, so g has some freedom of moment.

to see possible, expand on

$|g(\alpha)| = |g(\alpha)-f(\alpha)|$

claim $|f'(\alpha_1)|=|g'(\alpha_1)|$. if not,

$|g'(\alpha_1)-f'(\alpha_1)| \leq \max(|f'(\alpha)|, |g'(\alpha)|)$ is true with equality

so $|g'(\alpha_1)-f'(\alpha_1)| = \max(|f'(\alpha)|,|g'(\alpha)|) \geq |f'(\alpha)|$ but contradicts

so $|g(\alpha_1)| < |f'(\alpha_1)^2|$
$= |g'(\alpha_1)^2|$

nonarch: $|x|<|y| \Rightarrow |x\pm y| = |y|$ $\quad \begin{cases} |x\pm y| \leq \max(|x|,|y|) = |y| \\ |y| \leq \max(|x\pm y|, |-x|) = |x\pm y| \end{cases}$

now, $|x+y| \leq |y|$ with $=$ if $|x|<|y|$

if $|x|=|y|$, $|2y| = |y| \Rightarrow |2|=1$ $\neq$. nontrivial. so, $=$ hold iff strictly less.

now, have $|g(\alpha_1)|<|f'(\alpha_1)|^2$, $|f'(\alpha_1)-g'(\alpha_1)|<|f'(\alpha_1)|$, $|g(\alpha_1)| < |g'(\alpha_1)|^2$

apply hensel to $K(\alpha_1)$, $\exists\ \beta \in K(\alpha_1)$ s.t. $g(\beta)=0$, $|\beta-\alpha_1| < |g'(\alpha_1)|$

But $|g'(\alpha_1)| = |f'(\alpha_1)| = \prod_{i=2}^n |\alpha_1-\alpha_i| \leq |\alpha_1-\alpha_i|$ for each $i=2,\dots,n$.

each $|\alpha_1-\alpha_i|\leq 1$
each α_i is integral.

$f(x) = \prod_{i=1}^n (x-a_i)$

$\ln f(x) = \sum_{i=1}^n \ln(x-a_i)$ apply $\frac{d}{dx}$ both sides.

$\frac{f'(x)}{f(x)} = \sum_{i=1}^n \frac{1}{x-a_i}$

$f'(x) = f(x) \sum_{i=1}^n \frac{1}{x-a_i}$

$= \sum_{i=1}^n \frac{f(x)}{x-a_i}$

$= \sum_{i=1}^n \prod_{j\neq i} (x-a_i)$

$f'(a_k) = \prod_{j\neq i} (x-a_i)$

$\boxed{|x|<|y| \Rightarrow |y+x| = |y|}$

Since $|\underbrace{\beta-\alpha_1}_{x}| < |\underbrace{\alpha_1-\alpha_i}_{y}| = |\beta-\alpha_i|$

Krasner's lemma gives $\alpha_1 \in K(\beta)$.

So $K(\alpha_1) \subseteq K(\beta)$ ✓

why $K(\beta) \subseteq K(\alpha_1)$? (by hensel, $\beta \in K(\alpha_1)$.)

Proof scheme.

↳ pick ε s.t. $|g(\alpha_1)| < |f'(\alpha_1)^2|$

$|f'(\alpha_1) - g'(\alpha_1)| < |f'(\alpha_1)|$

↳ $|g(\alpha_1)| \leq |g'(\alpha_1)|^2$

↳ apply Hensel to $K(\alpha_1)$, get $\beta \in K(\alpha_1)$

↳ $|\beta-\alpha_1| < |g'(\alpha_1)| = |f'(\alpha_1)| = \prod \ldots$ use Krasners to show $K(\alpha_1) \subseteq K(\beta)$.

Week 4 lec 1

thm. local fields are completion of global fields.

let K be a local field. Then it's the completion of a global field.

Case 1: $|\cdot|$ archimedean

$\mathbb{R}$ is the completion of $\mathbb{Q}$ w.r.t $|\cdot|_\infty$

$\mathbb{C}$ is the completion of $\mathbb{Q}(i)$.

Case 2: $|\cdot|$, non-arch and equal char.

$K \cong \mathbb{F}_q((t))$ where K is the completion of $\mathbb{F}_q(t)$ w.r.t. p-adic abs value.

Case 3: $|\cdot|$ non-arch, mixed char.

K is finite extension of $\mathbb{Q}_p$. It's separable, (not char p,) So $K = \mathbb{Q}_p(\alpha)$ for some $\alpha \in K$. WLOG α integral over $\mathbb{Q}_p$. let $f(x) \in \mathbb{Z}_p(x)$ be its min. poly. $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, so $\exists\, \varepsilon$ (nearby poly define same extension) pick $g(x) \in \mathbb{Z}[x]$ as the prop.

So $K = \mathbb{Q}_p(\beta)$. $\mathbb{Q}(\beta)$ is dense in $\mathbb{Q}_p(\beta)$, K is the completion of it.

Pf scheme

↳ $k = \mathbb{Q}_p(\alpha)$, let f be α's min poly.

↳ use nearby poly define same ext.

↳ $g \in \mathbb{Z}[x]$, $f \in \mathbb{Z}_p[x]$, $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$ is completion of $\mathbb{Q}(\beta)$, a # field.

§ Dedekind domains

<u>defn. Dedekind domains</u>

They're rings s.t.

1) R is Noetherian integral domain
2) R is integrally closed in $\mathrm{Frac}(R)$
3) every nonzero prime ideal is maximal

ex:

↳ field of integers in number field is int. closed.

↳ Any PID / DVR is dedekind domains

<u>thm (main thm of lecture)</u>

A ring is a DVR $\Leftrightarrow$ it's DDK & has exactly one nonzero prime ideal.

~~lem prime ideals with product subset of ideal~~

Let R be a Noetherian ring. Let I be an ideal. (nonzero). Then $\exists$ nonzero $P_1, P_2, \cdots P_n \subseteq R$ prime ideals s.t. $P_1 P_2 \cdots P_n \subseteq I$.

Pf: Suppose not. Let I be a maximal such ideal.

I is not prime. so $\exists\, x, y \in R$, $x \notin I$, $y \notin I$, but $xy \in I$.

then $I+(x)$, $I+(y)$ are ideals. But $I \subsetneq I+(x)$, $I \subsetneq I+(y)$ so by maximality,

$I+(x) \supseteq P_1 P_2 \cdots P_n$, $I+(y) \supseteq q_1 q_2 \cdots q_m$.

But $P_1 P_2 \cdots P_n q_1 q_2 \cdots q_m \subseteq (I+(x))(I+(y)) \subseteq I$. $\times\!\!\times$.

Pf scheme maximality, cook up two new ideals lem. If $xI \subseteq I$, then $x \in R$

let R be an ID. let R be integrally closed in $K := \mathrm{Frac}(R)$.
let $I \subseteq R$ be an nonzero f.g. ideal. let $x \in K$. If $xI \subseteq I$ then $x \in R$

pf: let $I = (c_1, \cdots c_n)$ each $xc_i \in I$ so write $xc_i = \sum_{j=1}^{n} a_{ij} c_j$, $a_{ij} \in R$.

let A be the matrix $(a_{ij})_{1 \le i,j \le n}$ set $B = xId_n - A \in M_{n\times n}(K)$.

let $\mathrm{adj}(B)$ be adjugate matrix of B.

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

$\times(\mathrm{adj}\, B)$ both sides

$$\det(B) Id_n \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

So $\det(B) = 0$ But $\det(B)$ is a monic polynomial in x. $\Rightarrow$ x is integral with coefficients in R. So x is integral over R $\Rightarrow$ R is int closed, $x \in R$.

Proof Scheme set $B = xId_n - A \in M^{n\times n}(K)$

Pf of thm 9.2 DVR $\Leftrightarrow$ DDK dom w/ 1 prime ideal.

$\Rightarrow$ Clear.

$\Leftarrow$ need to show R is a PID.

let $m \subseteq R$ be its unique prime ideal. (+) necessarily maximal.

WTS: all ideals are principal

Step 1: m is principal (to help step 2).

let $0 \neq x \in m$. then $\exists n$ minimal, s.t $(x) \supseteq m^n$ (By prev lemma)

so $(x) \not\supseteq m^{n-1}$ so, $\exists y \in m^{n-1} \setminus (x)$.

set $\pi := \frac{x}{y}$.

WTS: $(\pi^{-1}) m = R$

here $ym \subseteq m^n \subseteq (x)$. $\pi^{-1} m = \left(\frac{y}{x}\right) m \subseteq R$

to show $=$, suppose $\pi^{-1} m \subsetneq R$, i.e. $\pi^{-1} m$ is a proper ideal, then $\pi^{-1} m \subseteq m$ (maximal ideal.) then by prev. lemma, $\pi^{-1} = \frac{y}{x} \in R$, by prev. lemma. $y \cdot (x^{-1}) \in R$ $\Rightarrow$ $y(x^{-1}) \cdot x \in (x)$ $\Rightarrow$ $y \in (x)$ ※.

So $(\pi^{-1}) m = R$

$m = (\pi)$

Step 2: using step 1 to show R is a PID.

let $I \subseteq R$ be any nonzero ideal.

Consider the sequence of fractional ideals one of these is R

$$I \subsetneq \pi^{-1} I \subsetneq \pi^{-2} I \subsetneq \cdots\cdots \text{ in } K$$

hiccup

since $\pi^{-1} \notin R$, each containment is strict by prev. lemma.

R noetherian, ascending chain condition, so it eventually contains R.

$$\boxed{\begin{array}{l} \pi^{-(n+1)} I = \pi^{-n} I \\ I = \pi I \end{array}}$$

pick n maximal s.t. $\pi^{-n} I \subset R$. → why is this possible?

If all $\pi^{-n} I \subset R$ then you get an ascending ideal of R. This is impossible so at one point must contain smth not in R. then it's in field, so get 1. then get R.

We claim $\pi^{-n} I = R$

If $\pi^{-n} I \neq R$, $\pi^{-n} I \subset m = (\pi)$

$\pi^{-(n+1)} I \subset R$ contradicting maximality of n.

$\Rightarrow$ $\pi^{-n} I = R$ so $I = (\pi)^n$

Proof scheme

Step 1: m is principal.

set $y \in m^{n-1} \setminus (x)$

claim $\frac{x}{y} = \pi$, $(\pi^{-1}) m = R$

Step 2: all ideals are principal.

$$I \subsetneq \pi^{-1} I \subsetneq \pi^{-2} I \subsetneq \cdots\cdots \subseteq K$$

eventually contain R. pick max n, $\pi^{-n} I \subset R$ claim $=$.

<u>Def: localization</u>

$1 \in S$, $x, y \in S \Rightarrow xy \in S$.

let R be an ID, $S \subseteq R$, mult. closed set.

then, localization is

$$S^{-1} R = \left\{ \frac{x}{y} \quad x \in R,\ y \in S \right\} \subseteq \mathrm{Frac}(R)$$

i.e. if P is a prime ideal of S, $S \setminus P$ is a mult set.

$R_{(P)}$ is localization of $S = R \setminus P$.

facts: • R noetherian $\Rightarrow$ $S^{-1}R$ noetherian.

• $\exists$ bijection $\{$prime ideals in $S^{-1}R\} \leftrightarrow \{$prime ideals $\mathfrak{p} \subseteq R$ s.t. $\mathfrak{p} \cap S = \emptyset\}$.

Cor DDK domains localized is DVR

let R be DDK. let $P \subseteq R$ be prime ideal. Then $R_{(p)}$ is a DVR.

Pf.

By properties of localisation, $R_{(p)}$ is a Noetherian ID with unique nonzero ideal given by $\mathfrak{p} R_{(p)}$. By thm (DVR $\Leftrightarrow$ DDK w/ one nonzero prime ideal) & defn of DDK, WTS $R_{(p)}$ is DDK. So suffice to show it's integrally closed in $K = \text{frac}(R)$.

let $x \in \text{frac}(R)$ be integral over $R_{(p)}$.

let f be a monic poly satisfied by x, multiply denoms, get

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

(i.e. get $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ each bo has some s in denom. so multiply it out)

multiply by s^{n-1} $\Rightarrow$ xs integral over R. $xs \in R$ $x \in R_{(p)}$ ■

Proof scheme.

↳ main goal show $R_{(p)}$ is DDK

↳ show integral

↳ multiply out the denoms in the coefficients.

Week 4 lecture 2

def V_p

let R be a DDK. $P \subseteq R$ a prime ideal $\neq 0$. V_p is the normalized valuation on $Frac(R) = Frac(R_{(p)})$ corresponding to the DVR $R_{(p)}$.

e.g. $R=\mathbb{Z}$, $P=(p)$. V_p is the p-adic valuation.

thm. Dedekind domain's ideals factors.

let R be a DDK. Then every nonzero ideal $I \subseteq R$ can be written uniquely as a product of prime ideals, i.e. $I = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$, P_i distinct.

Proof :

needs two properties of localisation.

(i) I, J ideals $\Leftrightarrow$ $IR_{(p)} = JR_{(p)}$ $\forall p$ prime ideal.

(ii) R is DDK. P_1, P_2 nonzero prime ideals.

$$P_1 R_{(P_2)} = \begin{cases} R_{(P_2)} & \text{if } P_1 \neq P_2 \\ P_2 R_{(P_2)} & \text{if } P_1 = P_2. \end{cases}$$

$\rightarrow$ $R_{(P_2)}$'s ideals avoid $R \backslash P_2$ so its only ideal is R_2. here. $P_1 R_{(P_2)}$ is whole ring.

$R_{(P_2)} = \dfrac{R}{R \backslash P_2}$

Chris Williams pg 65.

Back to the proof.

let $I \subseteq R$ be nonzero prime ideal. By prov lemma, $\exists$ distinct prime ideals $P_1, P_2 \cdots P_r$, $P_1^{B_1} \cdots P_r^{B_r} \subseteq I$. $B_i > 0$.

(existence then uniqueness.)

existence proof.

let p be a prime ideal, $p \notin \{P_1, \cdots P_r\}$.

then fact i $\Rightarrow$ $P_i R_{(p)} = R_{(p)}$

$\Rightarrow$ $P_1^{B_1} \cdots P_r^{B_r} R_{(p)} = R_{(p)}$

$\Rightarrow$ $I R_{(p)} = R_{(p)}$

$\subseteq$ is true

$\supseteq$ b/c $R_{(p)} \subseteq P_1^{B_1} \cdots P_r^{B_r} R_{(p)} \subseteq I R_{(p)}$.

prov corollary: $R_{(p)}$ is DVR $\Rightarrow$ so each ideal is a power of max ideal.

$$I R_{(P_i)} = (P_i R_{(P_i)})^{\alpha_i} = P_i^{\alpha_i} R_{(P_i)}$$

for some $0 \leq \alpha_i \leq \beta_i$

thm all non-zero ideals of a DVR is power of its maximal ideal.

so By prev property, $I = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ (B/C localised at p or p_i are same).

now, Show uniqueness. Say

$$I = p_1^{\alpha_1} \cdots p_n^{\alpha_n} = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$$

then $p_i^{\alpha_i} R_{(p_i)} = p_i^{\gamma_i} R_{(p_i)}$ so $\alpha_i = \gamma_i \ \forall i$.

So we're done.

Proof scheme:

↳ Two important facts about localisation of ideals

↳ Show existence, $\begin{cases} I R_{(p)} = p_i R_{(p)} & \forall p \in \{p_1, \cdots p_n\} \\ I R_{(p_i)} = p_i^{\alpha_i} R_{(p_i)} & \forall i \end{cases}$

$\Rightarrow \quad I = p_i^{\alpha_i}$

↳ show uniqueness. Same base, diff power.

§ Dedekind domains & extensions.

fact: trace written as sum of where embeddings send it.

let L/K be a finite extension.

For $x \in \ell$, write $Tr_{L/K}(x) \in K$, for trace of K linear map $L \to L$ $y \mapsto xy$.

If L/K is separable of degree n, $\underbrace{\sigma_1, \cdots \sigma_K}_{\text{distinct}} : L \to \bar{K}$ denote the set of embeddings of L into alg closure of K, $Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$

lem trace form is non-degenerate.

let L/K be a finite separable extension of fields.

then the symmetric bilinear pairing

$$\left.\begin{aligned} (-, -) : L \times L &\to K \\ x, y &\mapsto Tr_{L/K}(xy) \end{aligned}\right\} \text{trace form}$$

is degenerate.

Proof. L/K separable $\Rightarrow$ $L = K(\alpha)$ and L/K as a vector space has basis $1, \alpha, \cdots \alpha^{n-1}$.

Then $Tr_{L/K}(\alpha^{i+j}) = A_{ij} = [BB^T]$

where $B := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & & \sigma_n(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha^n) & \sigma_2(\alpha^n) & & \sigma_n(\alpha^n) \end{bmatrix}$ $\underbrace{\begin{bmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^n) \\ 1 & & \ddots & \\ \vdots & & & \\ 1 & \sigma_n(\alpha) & & \sigma_n(\alpha^n) \end{bmatrix}}_{B^T}$

$\det(A) = \det(BB^T) = (\det(B))^2 = \left[\prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha))\right]^2 \neq 0.$ as $\sigma_i \neq \sigma_j$ if $i \neq j$ by separability.

in fact, extension separable $\Leftrightarrow$ trace form is nondegenerate.

Proof scheme

↳ write $L = K(\alpha)$, $A_{ij} = tr(\alpha^{i+j}) = [BB^T]$ vandermonde matrix.

↳ separable $\Rightarrow \det[BB^T] \neq 0$ so A_{ij} is nondegenerate.

lem integral closure of dedekind domain is DDK.

let $\mathcal{O}_K$ be a DDK. & a finite separable extension of $K := Frac(\mathcal{O}_K)$. Then the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L is a Dedekind domain.

Pf. to show $\mathcal{O}_L$ is DDK domain

1) $\mathcal{O}_L$ is Noetherian ID ← $\mathcal{O}_L$ subring of L, which is ID.

2) $\mathcal{O}_L$ integrally closed in L.

3) every $\neq 0$ prime ideal P in $\mathcal{O}_L$ is maximal.

1) WTS $\mathcal{O}_L$ is Noetherian:

let $e_1, \cdots e_n$ be a K-basis of L. assume $e_i \in \mathcal{O}_L$ $\forall i$ upon scaling.

non-degen $\Rightarrow$ let $f_1, \cdots f_n \in L$ be the dual basis for e_i in $(-,-)$ (i.e. $(e_i, f_i) = \delta_{ij}$)

let $x \in \mathcal{O}_L$, write $x = \sum_{i=1}^n \lambda_i f_i$, $\lambda_i \in K$ ($\lambda_i \in \mathcal{O}_K$)

then, $\boxed{\lambda_i = T_{L/K}(e_i, x)}$ $x = \sum_{i=1}^n T_{L/K}(e_i, x) f_i$

$tr(x) = \sum_{i=1}^n Tr(T_{L/K} e_i, x_i) f_i$

$\lambda_i = T_{L/K}(e_i, x) = Tr(e_i x) = \sum_{j=1}^n \sigma_j(e_i x) \in \mathcal{O}_K$

each $e_i \in \mathcal{O}_L$, $x \in \mathcal{O}_L$. so $e_i x \in \mathcal{O}_L$, $\sigma(e_i x) \in \mathcal{O}_L$

so $\lambda \in K \cap \mathcal{O}_L = \mathcal{O}_K$.

$Tr_{L/K}(z) \in K$ is integral over $\mathcal{O}_K$.

$Tr_{L/K}(z) \in \mathcal{O}_K$

$\mathcal{O}_L \subseteq \mathcal{O}_K f_1 + \mathcal{O}_K f_2 + \dots + \mathcal{O}_K f_n$ is a sub-$\mathcal{O}_K$ module generated by f's.

$\mathcal{O}_K$ noetherian $\mathcal{O}_L$ is a finite $\mathcal{O}_K$ module hence noetherian.

ii) ex sheet 2

iii) let P be a $\neq 0$ prime ideal of $\mathcal{O}_L$. (WTS: P is maximal)

let $p = P \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.

since $P \neq 0$, $\exists\, 0 \neq x \in P$, $0 \neq N_{L/K}(x) \in P \cap \mathcal{O}_K = p$ ($N_{L/K}(x) \in P$ b/c P is an ideal, and $N_{L/K}(x) \in \mathcal{O}_K$ by properties of norm)

so $p \neq 0$. $\mathcal{O}_K$ is dedekind, p is maximal. So $k = \mathcal{O}_K/p$ is a field.

now $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induces embedding

$$\underset{\text{field so injective}}{k = \mathcal{O}_K/p} \hookrightarrow \mathcal{O}_L/P.$$

But above, $\mathcal{O}_L$ is a f.d. K- alg.

Since P is prime, $\mathcal{O}_L/P$ is an ID, If $0 \neq y \in \mathcal{O}_L/P$, multiplication is injective.

as k- linear map, nullity $=0$. rank-nullity, mult by y is invertible.

$\mathcal{O}_L/P$ is field $\Rightarrow$ P is maximal.

done later again

Proof Scheme:

1) show Noetherian.

↳ get c_i, get f_i

↳ for $x \in \mathcal{O}_L$, write $x = \sum n_i f_i$

↳ WTS $n_i \in \mathcal{O}_K$. It indeed is by Trace.

2) ex sheet

3) prime ideals are maximal

↳ let $P \subseteq \mathcal{O}_L$ be prime, let $p = P \cap \mathcal{O}_K$.

↳ p nonempty $\mathcal{O}_K/p$ is field & injects onto $\mathcal{O}_L/P$.

↳ in $\mathcal{O}_L/P$, mult by y is invertible. So P is maximal.

done again later

iii) prime ideals are maximal try again

let $\mathfrak{P} \neq 0$ be a prime ideal in $\mathcal{O}_L$.

Let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. it's a prime ideal in $\mathcal{O}_K$.

<u>$\mathfrak{p}$ nonzero</u> :

let $0 \neq x \in \mathfrak{P}$. then, it satisfy $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ $a_i \in \mathcal{O}_K$. $a_0 \neq 0$

then, $a_0 \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ so $\mathfrak{p} \neq \emptyset$.

<u>field injection argument</u>:

$\mathcal{O}_K$ is DDK, $\mathfrak{p}$ maximal $\mathcal{O}_K/\mathfrak{p}$ field.

then the inclusion $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{P}$ is injective. $\hookrightarrow$ b/c domain is a field. So $\mathcal{O}_L/\mathfrak{P}$ contains a "copy" of $\mathcal{O}_K/\mathfrak{p}$ so it's a f.d.v.s. over $\mathcal{O}_K/\mathfrak{p}$ (f.g. $\mathcal{O}_K$ module).

$\mathcal{O}_L/\mathfrak{P}$ is an ID $\Rightarrow$ a field (rank-nullity argument).

Proof Scheme

↳ let $\mathfrak{P} \subseteq \mathcal{O}_L$ be prime let $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$

↳ $\mathfrak{p} \neq \emptyset$

↳ $\mathcal{O}_K/\mathfrak{p}$ field so injects into $\mathcal{O}_L/\mathfrak{P}$

↳ f.g. algebra, ID $\Rightarrow$ field.

<u>cor ring of integers of a number field is a Dedekind domain</u>

L is finite ext of $\mathbb{Q}$.

so $\mathcal{O}_L$ is the integral closure of $\mathbb{Z}$ in L.

using above thm, $\mathcal{O}_L$ is DDK.

<u>def</u>. let K be a number field with ring of integers $\mathcal{O}_K$

let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$.

then the $\mathfrak{p}$-adic absolute value defined on K is

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

week 4 lec 3

Preliminaries : $\mathcal{O}_K$ is dedekind domain, $K = \mathrm{Frac}(\mathcal{O}_K)$.

L/K a finite separable extension.

$\mathcal{O}_L \subseteq L$ integral closure of $\mathcal{O}_K$ in L which is a DDK.

<u>lem. let $0 \neq x \in \mathcal{O}_K$.</u> then

$$(x) = \prod_{\substack{\mathfrak{p} \neq 0 \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{p}^{v_\mathfrak{p}(x)}$$

<u>Pf</u> : WTS $x\mathcal{O}_K = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_\mathfrak{p}(x)}$

note that $x(\mathcal{O}_K)_{(\mathfrak{p})} = (\mathfrak{p}\, \mathcal{O}_{K(\mathfrak{p})})^{v_\mathfrak{p}(x)}$ by defn of $v_\mathfrak{p}(x)$

as ideals in $\mathcal{O}_{K(\mathfrak{p})}$, here

i.e. $(x) = (\mathfrak{p})^{v_\mathfrak{p}(x)}$

using lemma about localisation ($I = J \Leftrightarrow IR_{(\mathfrak{p})} = JR_{(\mathfrak{p})}$ $\forall \mathfrak{p}$ prime ideals)

so, $(x) = \prod_{\substack{\mathfrak{p} \text{ prime} \\ \mathfrak{p} \neq 0}} \mathfrak{p}^{v_\mathfrak{p}(x)}$

<u>defn. let $\mathfrak{P} \subseteq \mathcal{O}_L$, $\mathfrak{p} \subseteq \mathcal{O}_K$, prime ideals.</u>

write $\mathfrak{P} \mid \mathfrak{p}$ if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$ and $\mathfrak{P} = \mathfrak{P}_i$ for some i. $e_r > 0$.

<u>Thm. absolute values of L extending $|\cdot|_\mathfrak{p}$.</u>

let $\mathcal{O}_K, \mathcal{O}_L, K, L$ as above. let $\mathfrak{p} \neq 0$ a prime ideal of $\mathcal{O}_K$.

write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ $(e_i > 0)$

then the absolute values on L extending $|\cdot|_\mathfrak{p}$ are $|\cdot|_{\mathfrak{P}_1}, \cdots |\cdot|_{\mathfrak{P}_n}$. up to equiv

<u>Proof</u> Two directions

$\hookrightarrow$ $|\cdot|_{\mathfrak{P}_i}$ extends $|\cdot|_\mathfrak{p}$. lemma: $(x) = \prod_{\substack{\mathfrak{p} \text{ prime} \\ \neq 0}} \mathfrak{p}^{v_\mathfrak{p}(x)}$

for any $0 \neq x \in \mathcal{O}_K$, $i = 1, \cdots r$, $v_{\mathfrak{P}_i}(x) = e_i v_\mathfrak{p}(x)$

so up to equiv, $|\cdot|_{\mathfrak{P}_i}$ extends $|\cdot|_\mathfrak{p}$.

$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$

$(x) = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{v_\mathfrak{p}(x)}$

$= \prod_{\mathfrak{p} \text{ prime}} (\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r})^{v_\mathfrak{p}(x)}$

so $v_{\mathfrak{P}_i}(x) = e_i v_\mathfrak{p}(x)$.

↳ Show converse: if $|\cdot|$ is an abs on L extending $|\cdot|_p$, then it must be $|\cdot|_{\mathfrak{p}_i}$.

Suppose $|\cdot|$ on L extends $|\cdot|_p$.
then $|\cdot|$ is bounded on $\mathbb{Z}$ as $\mathbb{Z} \subseteq K \Rightarrow$ is non-archimedean.

Idea:
use this to make a prime ideal in $\mathcal{O}_L$.

↳ let $R = \{x \in L \mid |x| \le 1\} \subseteq L$ be the valuation ring for $|\cdot|$.
then, since $\mathcal{O}_K \subseteq R$.
R is integrally closed in L, and $\mathcal{O}_K \subseteq \mathcal{O}_L$, so $\mathcal{O}_K$'s int closure is in R. so $\mathcal{O}_L \subseteq R$.

↳ Set $\mathfrak{p} = \{x \in \mathcal{O}_L \mid |x| < 1\}$
$= \mathcal{O}_L \cap m_R$

↳ since m_R is prime, $\mathcal{O}_L \cap m_R$ is prime so $\mathfrak{p}$ is prime id of $\mathcal{O}_L$.

↳ nonzero because $p \in \mathfrak{p}$.

now we can localize $\mathfrak{p}$.

$\mathcal{O}_{L(\mathfrak{p})} \subseteq R$ as if $s \in \mathcal{O}_L \setminus \mathfrak{p} \Rightarrow |s| = 1$. So s is invertible but has $|\cdot| = 1$ so still in R.

But $\mathcal{O}_{L(\mathfrak{p})}$ is a DVR $\Rightarrow$ max subring of L.

So $\boxed{\mathcal{O}_{L(\mathfrak{p})} = R}$ as R is a maximal subring of L.

So $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}}$.
↓ R is its max subring
↓ $\mathcal{O}_{L(\mathfrak{p})}$ is its max subring

lastly. Show that $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}_i}$.
since $|\cdot|$ extends p, $\mathfrak{p} \cap \mathcal{O}_K = p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$

$\Rightarrow \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subseteq \mathfrak{p}$.

$\Rightarrow \mathfrak{p}_i = \mathfrak{p}$ (if $\mathfrak{p}$ is prime id, $I_1 I_2 \subset \mathfrak{p}$, then $I_1 \subset \mathfrak{p}$ or $I_2 \subset \mathfrak{p}$)

Proof scheme

two direction

1) $|\cdot|_{\mathfrak{p}_i}$ extend $|\cdot|_p$ indeed by lemma.

2) show $|\cdot|$ is precisely $\mathfrak{p}_i$.

make $\mathfrak{p}$:

↳ $|\cdot|$ is nonarchimedean

↳ let R be $|\cdot|$'s valuation ring. $\mathcal{O}_K \subseteq R$, int closure $\Rightarrow$ $\mathcal{O}_L \subseteq R$

↳ set $\boxed{\mathfrak{p} = \mathcal{O}_L \cap m_R}$

localize at $\mathfrak{p}$:

↳ $\mathfrak{p}$ is prime ideal of $\mathcal{O}_L$, so localize at $\mathfrak{p}$.

↳ $\mathcal{O}_{L(\mathfrak{p})} = R$

↳ $|\cdot|$ is equiv to $|\cdot|_{\mathfrak{p}}$.

show $\mathfrak{p} = \mathfrak{p}_i$ for some i.

↳ $\mathfrak{p} \cap \mathcal{O}_K = p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ $\Rightarrow$ $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset \mathfrak{p}$ $\Rightarrow$ one is $=$.

R : DVR w.r.t $|\cdot|$ $\qquad\qquad$ $\mathcal{O}_{L(\mathfrak{p})}$: DVR w.r.t. $|\cdot|$

m_R max id $\qquad\qquad$ $\mathfrak{p}$ max id.

<u>Cor 10.6</u> <u>(generalization of ostrowski)</u>

classification of abs value on number fields.

let K be a number field with ring of integers $\mathcal{O}_K$. then any absolute value on K is equivalent to

i) $|\cdot|_p$ for some nonzero prime ideal $p \subseteq \mathcal{O}_K$.

ii) $|\cdot|_\gamma$ for some $\gamma : K \to \mathbb{R}$ or $\mathbb{C}$.

Pf: case I. non-arch.

$|\cdot|_\infty$ is equivalent to $|\cdot|_p$ for some prime p.

By ostrowski + thm, $|\cdot| \sim |\cdot|_{\mathfrak{p}}$ for some $p | \mathfrak{p}$ a prime ideal in $\mathcal{O}_K$.

case II. example sheet.

§ Completions (of Dedekind Domains)

$\mathcal{O}_K$ dedekind domain, L/K finite separable

let $p \subseteq \mathcal{O}_K$, $\mathfrak{p} \subseteq \mathcal{O}_L \neq 0$ prime ideals.

$\mathfrak{p}|p$ and K_p, $L_\mathfrak{p}$ be completions of K and L w.r.t. class of abs values $|\cdot|_p$ and $|\cdot|_\mathfrak{p}$ respectively.

<u>lem 10.9.</u>

i) the natural

$$\pi_\mathfrak{p} : L \otimes_K K_p \to L_\mathfrak{p} \text{ is surjective}$$
$$(l, k) \mapsto lk$$

ii) $[L_\mathfrak{p} : K_p] \leq [L:K]$ ← degree

<u>Proof:</u> let $\underset{\substack{\| \\ \mathrm{Im}(\pi_\mathfrak{p})}}{M} = LK_p \subseteq L_\mathfrak{p}$

L/K sep'ble, $L = K(\alpha)$ then $M = LK_p = K_p(\alpha)$ $\Rightarrow M$ is finite ext of K_p.

and $\underset{\substack{\| \\ [K_p(\alpha):K_p]}}{[M:K_p]} \leq [L:K]$ b/c poly satisfied in L/K is satisfied in $(K_p(\alpha)/K_p)$.

M is complete b/c it's a finite extension of a complete value field.

M lies between L and $L_\mathfrak{p}$ $\Rightarrow M = L_\mathfrak{p}$.

Proof Scheme:

↳ consider $M = LK_p = K_p(\alpha)$

↳ $[M:K_p] \leq [L:K]$

↳ M complete, and M between L, $L_\mathfrak{p}$ $\Rightarrow M = L_\mathfrak{p}$.

<u>lemma (CRT)</u>

let R be a ring. let $I_1, \cdots I_n \subseteq R$ be ideals and $I_i + I_j = R$ whenever $i \neq j$.

then i) $\bigcap_{i=1}^n I_i = I_1 \cdots I_n = I$

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

Thm 10.9

the natural map $L \otimes_K K_p \to \prod_{\mathfrak{p}|p} L_{\mathfrak{p}}$ is an iso

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

write $f(x) = f_1(x) \cdots f_n(x)$ in $K_p[x]$. each f_i are distinct & irred (separability).

Since $L \cong K[x]/f(x)$, have

$$L \otimes K_p \cong \left(K[x]/f(x)\right) \otimes K_p \cong K_p[x]/f(x) \cong \prod_{i=1}^{n} K_p[x]/f_i(x).$$

set $L_i = K_p[x]/f_i(x)$, a finite ext of K_p.

note L_i contains both L and K_p $\Big(\underbrace{\overset{L}{\overset{\shortparallel}{K[x]/f(x)}} \hookrightarrow K_p[x]/f_i(x)}_{\text{well defined field morphism hence injective}}\Big)$

L is dense in L_i because K dense in K_p, can approx elements of $\underbrace{K_p[x]/f_i(x)}_{L_i}$ with element in $\underbrace{K[x]/f(x)}_{L}$.

the theorem then follow from 3 claims.

i) $L_i \cong L_{\mathfrak{p}}$ for some $\mathfrak{p}$ of $\mathcal{O}_L$ dividing p.

ii) each $\mathfrak{p}$ appear at most once

iii) each $\mathfrak{p}$ appear at least once.

i): $[L_i : K_p] < \infty$ so there's unique absolute value on L_i extending $|\cdot|_p$.

thm $\Rightarrow$ $|\cdot|$ restrict to L is equivalent to $|\cdot|_{\mathfrak{p}}$ for some $\mathfrak{p}|p$.

L dense in L_i, L_i complete, so $L_i \cong L_{\mathfrak{p}}$.

ii) Say φ_i makes $L_i \cong L_j$, is an iso preserving L and K_p. then

$\varphi_i : K_p[x]/f_i(x) \to K_p[x]/f_j(x)$ must send x to x. which can only happen

if $f_i = f_j$. $\Rightarrow i = j$

iii) By the lemma, $\pi_{\mathfrak{p}} : L \otimes_K K_p \to L_{\mathfrak{p}}$ is surjective, $\forall\, \mathfrak{p} | p$.
Since $L_{\mathfrak{p}}$ is a field, $\pi_{\mathfrak{p}}$ factor through L_i for some i
so $L_i \cong L_{\mathfrak{p}}$ by surjectivity.

i.e. $L \otimes_K K_p / \ker(\pi_{\mathfrak{p}}) \cong L_{\mathfrak{p}}$

$$\Big(\prod_{i=1}^n K_p[x]/f_i(x) \Big) / \ker(\pi_{\mathfrak{p}})$$

i.e. ker either 0 or whole field.

Proof scheme:

Statement: $L \otimes_K K_p \to \prod_{\mathfrak{p}|p} L_{\mathfrak{p}}$ is an iso

Proof:

↳ write $L = K(\alpha)$ let $f(x)$ be min poly, factor as $f(x) = \prod_{i=1}^n f_i(x)$ in $K_p[x]$,

↳ $L \otimes_K K_p \cong K[x]/f(x) \otimes K_p \cong K_p[x]/f(x) \cong \prod_{i=1}^n K_p[x]/\underset{\uparrow}{f_i(x)}$ distinct

↳ set $L_i = K_p[x]/f_i(x)$

↳ L_i contains L and K_p, L is dense in L_i

then 3 claims
1) $L_i \cong L_{\mathfrak{p}}$ for some $\mathfrak{p}|p$. (restrict to L, use thm)
2) each $\mathfrak{p}$ appear $\leq$ once (set an iso, then ✻).
3) each $\mathfrak{p}$ appear $\geq$ one. ($\pi_{\mathfrak{p}}$ surjective, factor thru)

<u>Example</u> $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$ $f(x) = x^2+1$ hensel's lemma $\sqrt{-1} \in \mathbb{Q}_5$ as 2's simple root.
(5) splits in $\mathbb{Q}(i)$, $5\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$

Week 5 lec 1

$\mathcal{O}_K$ dedekind domain, L/K finite separable, $0 \in \mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal.

cor. write $N_{L/K}(x)$ as a product

for $x \in L$, $N_{L/K}(x) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(x)$

Proof: let $B_1, \dots B_r$ be bases of $L_{\mathfrak{P}_1}, \dots, L_{\mathfrak{P}_r}$, as $K_\mathfrak{p}$ vector spaces.

then $B = \bigcup B_i$ is a basis for $L \otimes K_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$.

let $[\text{mult}(x)]_B$ (resp $[\text{mult}(x)]_{B_i}$)

be the matrix for

$\text{mult}(x): L \otimes K_\mathfrak{p} \to L \otimes K_\mathfrak{p}$ (resp $L_{\mathfrak{P}_i} \to L_{\mathfrak{P}_i}$)

w.r.t basis B (resp B_i)

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

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

§ Decomposition groups

let $0 \neq \mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$.

$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ distinct products of prime ideals in $\mathcal{O}_L$,

with $e_i > 0$.

Rmk: $\mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_K$, $\forall i$

: for any i, $\mathfrak{p} \subseteq \mathcal{O}_K \cap \mathfrak{P}_i \subsetneq \mathcal{O}_K$

Since $\mathfrak{p}$ maximal, $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}_i$.

defn ramification index and ramifies

1) e_i is the ramification index of $\mathfrak{p}_i$ over $\mathfrak{p}$.
2) we say $\mathfrak{p}$ is ramified in L if $e_i > 1$ for some i

(ramifies: more complicated? higher powers?)

Example of ramification

Eg: $\mathcal{O}_K = \mathbb{C}[t]$ $\quad \mathcal{O}_L = \mathbb{C}[T]$

$$\mathcal{O}_K \to \mathcal{O}_L$$
$$t \mapsto T^n$$

$t\mathcal{O}_L = T^n \mathcal{O}_L$ so ramification index of (T) over (t) is n.

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

makes sense b/c $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{p}_i$ is injective

as $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{p}_i$ so $\mathfrak{p} \subseteq \mathfrak{p}_i$, and $i: \mathcal{O}_K \to \mathcal{O}_L/\mathfrak{p}_i$, $\mathfrak{p} \subseteq \ker(i)$

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

Proof: let $S = \mathcal{O}_K \setminus \mathfrak{p}$. Then we get following properties of localisation:

* left as exercise !!!

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

main point of these properties: e and f don't change when we replace $\mathcal{O}_K$ and $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_K$ and $S^{-1}\mathcal{O}_L$.

(remember all info about $\mathfrak{p}$ but not other prime ideals)

So, we can assume that $\mathcal{O}_K$ is a DVR (i.e. assume after localisation)

so $\mathcal{O}_K$ is a PID.

By CRT, we have

$\mathcal{O}_L/p\mathcal{O}_L = \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{p}_i^{e_i}$ $\boxed{\text{(note: NTS } \mathfrak{p}_1, \mathfrak{p}_2 \text{ are coprime)}}$

We count dimension of both sides as $k = \mathcal{O}_K/p$ vector space.

RHS: $\prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{p}_i^{e_i}$: for each i, there is an increasing seq of subspaces:

$$0 \subseteq \mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i} \subseteq \cdots \subseteq \mathfrak{p}_i/\mathfrak{p}_i^{e_i} \subseteq \mathcal{O}_L/\mathfrak{p}_i^{e_i}$$

so $\dim_k \mathcal{O}_L/\mathfrak{p}_i^{e_i} = \sum_{i=0}^{e_i-1} \dim_k (\mathfrak{p}_i^{i}/\mathfrak{p}_i^{i+1})$. note that

$\boxed{\mathfrak{p}^i/\mathfrak{p}^{i+1} \text{ is an } \mathcal{O}_L/\mathfrak{p}_i}$ module, and $x \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ is a generator.

??? NOT SURE WHY.

so $\dim_k \mathfrak{p}^i/\mathfrak{p}^{i+1} = \dim_k \mathcal{O}_L/\mathfrak{p}_i = \deg \text{ of } [\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/p] = f_i$

so $\dim_k \mathcal{O}_L/\mathfrak{p}_i^{e_i} = e_i f_i$. and $\dim_k \prod_{i=1}^{r} \mathcal{O}_L/\mathfrak{p}_i^{e_i} = \sum_{i=1}^{r} e_i f_i$.

LHS: $\mathcal{O}_L/p\mathcal{O}_L$ structure theorem over $\mathcal{O}_K$ of rank $n = [L:K]$.

$\mathcal{O}_L$ torsion free $\Rightarrow \mathcal{O}_L$ free module over $\mathcal{O}_K$ of rank $n = [L:K]$

$\mathcal{O}_L/p \cong (\mathcal{O}_K/p)^n$ as $\mathcal{O}_K/p$ module. $\dim_k \mathcal{O}_L/p = n$.

Proof Scheme:

↳ a bunch of properties about localisation so that e, f stay the same after localisation

↳ so we can assume $\mathcal{O}_K$ is DVR

↳ replace $\mathcal{O}_K$, $\mathcal{O}_L$ by $S^{-1}\mathcal{O}_K$, $S^{-1}\mathcal{O}_L$

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

↳ count both side's degree as $k = \mathcal{O}_K/p$ vector space.

↳ LHS: structure thm for modules: free parts, so $(\mathcal{O}_L/p) \cong (\mathcal{O}_K/p)^n$

↳ RHS: $0 \subseteq \mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i} \subseteq \mathfrak{p}_i^{e_i-2}/\mathfrak{p}_i^{e_i} \subseteq \cdots \subseteq \mathfrak{p}_i/\mathfrak{p}_i^{e_i} \subseteq \mathcal{O}_L$

each $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is an $\mathcal{O}_L/\mathfrak{p}$ module so $\deg = \sum_{r=0}^{e_i-1} f_i = e_i f_i$.

Prop. L/K Galois, then Gal(L/K) acts on $\mathfrak{p}_i$

Assume L/K is Galois. let $\sigma \in Gal(L/K)$ $\sigma(\mathfrak{p}_i) \cap \mathcal{O}_K = \mathfrak{p}$

so that $\sigma(\mathfrak{p}_i) \in \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$.

so Gal(L/K) acts on $\mathfrak{p}_i$.

Prop. The action of Gal(L/K) on $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_K\}$ is transitive

Proof: Suppose not. $\exists\, i, j$, $i \neq j$ and $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$ for all $\sigma \in Gal(L/K)$.

By CRT, we can choose

$x \in \mathcal{O}_L$ s.t. $\begin{cases} x \equiv 0 \mod \mathfrak{p}_i \\ x \equiv 1 \mod \sigma(\mathfrak{p}_j) \ \forall \sigma \in Gal(L/K) \end{cases}$

! check satisfy CRT's co-prime-ness.

$N_{L/K}(x) = \prod_{\sigma \in Gal\, L/K} \sigma(x) \in \underset{\substack{\uparrow \\ x \in \mathcal{O}_L}}{\mathcal{O}_K} \cap \underset{\substack{\uparrow \\ x \equiv 0 \mod \mathfrak{p}_i \\ \text{so } x \text{ in ideal.}}}{\mathfrak{p}_i} = \mathfrak{p} \subset \mathfrak{p}_j$

$\mathfrak{p}_j$ is prime, so $\prod_{\sigma \in Gal(L/K)} \sigma(x) \subset \mathfrak{p}_j$ means some $\tau \in Gal(L/K)$ have $\tau(x) \in \mathfrak{p}_j$

$\tau(x) \equiv 0 \mod \mathfrak{p}_j \Rightarrow x \equiv 0 \mod \tau^{-1}(\mathfrak{p}_j)$ but $\tau^{-1} \in Gal(L/K)$.

Proof Scheme:

↳ assume not, so $\exists\, i, j$, $i \neq j$ and $\mathfrak{p}_i \neq \sigma(\mathfrak{p}_j)$ $\forall \sigma \in Gal(L/K)$

↳ $x \in \mathcal{O}_L$ $\begin{cases} 0 \mod \mathfrak{p}_i \\ 1 \mod \sigma(\mathfrak{p}_j) \end{cases}$

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

↳ $\tau(x) \in \mathfrak{p}_j$ for some j. So $x \in \tau^{-1}(\mathfrak{p}_j)$ ※.

Cor L/K Galois, $n=efr$

If L/K is Galois, then $\begin{cases} e:= e_1 = e_2 = \cdots = e_r \\ f:= f_1 = f_2 = \cdots = f_r \end{cases}$ and $n = efr$.

Proof:

suffice to show $e_1 = e_2$, $f_1 = f_2$.

Let $\sigma \in Gal(L/K)$ be s.t. $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$. Then,

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = \mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p})\mathcal{O}_L = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_r)^{e_r}$$
$$= \mathfrak{p}_2^{e_1} \cdots \quad \text{so } e_1 = e_2$$

also $\mathcal{O}_L/\mathfrak{p}_1 = \mathcal{O}_L/\sigma(\mathfrak{p}_1) \cong \mathcal{O}_L/\mathfrak{p}_2$ implies that $f_1 = f_2$.

so $n = \sum_{i=1}^{r} e_i f_i = ref$

Proof idea: $\sigma(p) = p$.

Cor Invariants for extensions of DVF (instead of DDK)

If L/K is extension of complete, DVF, with normalised valuations v_L, v_K and uniformizers π_L, π_K. Then $\begin{cases} \text{ramification index is } e = e_{L/K} = v_L(\pi_K) \\ \text{residue class deg is } f = f_{L/K} = [k_L : k] \\ [L:K] = ef. \end{cases}$

cus only one prime ideal lying above p upstairs.

Prove it for non-separable ?

Back to the setting $\mathcal{O}_K$ dedekind, L/K finite & Galois.

defn decomposition groups

$\mathcal{O}_K$ dedekind, L/K finite & Galois. Then the decomposition group at prime $\mathfrak{P}$ of $\mathcal{O}_L$ is the subgroup of $Gal(L/K)$ (stab) by

$$G_{\mathfrak{P}} = \{ \sigma \in Gal(L/K) \quad \sigma(\mathfrak{P}) = \mathfrak{P} \}$$

Prop for any $\mathfrak{P}, \mathfrak{P}'$ dividing p, $G_{\mathfrak{P}}, G_{\mathfrak{P}'}$ are conjugates.

Proof: $Gal(L/K)$ acts transitively on $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_n\}$.

or, $\mathfrak{P}, \mathfrak{P}'$ have same orbit under $\sigma \in Gal(L/K)$

? transitive meaning?

Week 5 lec 2

$\mathcal{O}_K$ DDK, L/K finite & sep'able, $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal.

Prop. Completion of Galois extensions

If L/K is Galois, $\mathfrak{P}|\mathfrak{p}$ is prime ideal of $\mathcal{O}_L$ then

1) $L_{\mathfrak{P}} / K_{\mathfrak{p}}$ is Galois

2) there is a natural map

$$\text{res}: \text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \text{Gal}(L/K)$$

which is injective & have image $G_{\mathfrak{P}}$.

Proof:

1) Recall that in characteristic 0,

field ext E/F is Gal $\Leftrightarrow$ E is splitting field of poly in $F[X]$.

L/K Galois $\Rightarrow$ L is splitting field of $f \in K[X]$. Since $L \subset L_{\mathfrak{P}}$ so f splits in $L_{\mathfrak{P}}$.

and $L_{\mathfrak{P}} = K_{\mathfrak{p}}(\alpha)$ for some root $\alpha \in f$. But any intermediate field $K_{\mathfrak{p}} \subset M \subset L_{\mathfrak{P}}$ doesn't contain α. f cannot split over any such M. So $L_{\mathfrak{P}}$ is splitting field of f over $K_{\mathfrak{p}}$.

So $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois.

2) let $\sigma \in \text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, since L/K is normal, σ fixes L. ???

$\text{res}: \text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \text{Gal}(L/K)$ is therefore well defined. It is injective as L is dense in $L_{\mathfrak{P}}$.

By lemma ($|\sigma(x)| = |x|$ for $x \in L$),

$|\sigma(x)|_{\mathfrak{P}} = |x|_{\mathfrak{P}}$ $\forall \sigma \in \text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, $x \in L_{\mathfrak{P}}$. ???? $x \in \mathfrak{P} \Leftrightarrow \{y \in \mathcal{O}_L \mid |x|_{\mathfrak{P}} < 1\} \Leftrightarrow x \in \sigma(\mathfrak{P})$

$\Rightarrow$ σ fixes $\boxed{\mathfrak{P}}$ $\forall \sigma \in \text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.
as a set

So $\text{res}(\sigma) \in G_{\mathfrak{P}}$.

now, to show injectivity, suffices to show

$$[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef = |G_{\mathfrak{P}}|$$

- $|G_{\mathfrak{P}}| = ef$: $n = efr$ where $r = 1$
- $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef$: apply " L/K finite sep'able $\Rightarrow [L:K] = ef$ " to $[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$, e, f don't change when we take completions!

Proof Scheme

1) L/K is splitting field of a poly. L_p/K_p is splitting field of that poly in K_p.

2) restriction is injective

↳ $\sigma \in Gal(L_p/K_p)$ then σ fix L.

↳ σ fix L, restriction is injective as L dense in L_p.

↳ $|\sigma(x)|_p = |x|_p \Rightarrow \sigma$ fixes $p \Rightarrow \sigma \in G_p$.

surjectivity: $res: Gal(L_p/K_p) \to G_p$ surjective, show $[L_p:K_p] = ef = |G_p|$

$\boxed{p = p_1 p_2 \text{ in } \mathbb{Z}[i] \text{ iff } p = x^2+y^2 \ ?}$???

different and discriminant

let L/K be extension of algebraic number fields. $[L:K]=n$.

def Δ

let $x_1, \cdots x_n \in L$,

$\Delta(x_1, \cdots x_n) = \det(Tr_{L/K}(x_i x_j)) \in K$??? why this true? number fields?

$= \det(\sigma_i(x_j))^2 \in K$ $\quad \sigma_i : L \to \bar{K}$ distinct embeddings

note: if $y_i = \sum_{j=1}^n a_{ij} x_j$ $\quad a_{ij} \in K$,

$\Delta(y_1, \cdots y_n) = \det(A)^2 \Delta(x_1, \cdots x_n)$ $\quad A = (a_{ij})$

if $x_1, \cdots x_n \in \mathcal{O}_L$, $\Delta(x_1, \cdots x_n) \in \mathcal{O}_K$.

lemma. trace form is nondegenerate in perfect field. $\Leftrightarrow R \cong \prod R$

K is a perfect field. R a K-algebra, f.d. as a vector space.

then the trace form $(\_,\_) : R \times R \to K$

$(x,y) = Tr_{R/K}(xy) := Tr_R(\text{mult}(xy))$ is nondegen

$\Leftrightarrow R \cong R_1 \times \cdots \times R_n$, R_i/K are finite /hence sep'able extensions

Proof: don't know either. ??? need to review!

Thm. ramified & unramified w.r.t. Δ

let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$. prime.

i) if $\mathfrak{p}$ ramifies in L, then $\forall x_1, \cdots x_n \in L$, $\mathfrak{p} \mid \Delta(x_1, \cdots x_n)$

ii) if $\mathfrak{p}$ is unramified in L, $\exists x_1, \cdots x_n \in L$, $\mathfrak{p} \nmid \Delta(x_1, \cdots x_n)$

Proof

i) let $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ $0 \neq \mathfrak{p}_i \subseteq \mathcal{O}_L$, distinct, prime, $e_i > 0$

CRT $\Rightarrow R = \mathcal{O}_L / \mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^{r} \mathcal{O}_L / \mathfrak{p}^{e_i}$

$\mathfrak{p}$ ramifies in $L \Rightarrow e_i > 1$ for some i $\mathfrak{p}^{e_i}$ is not a prime ideal, $\Rightarrow \prod \mathcal{O}_L/\mathfrak{p}^{e_i}$ not ID

$\Rightarrow$ have nilpotent $\Rightarrow \mathcal{O}_L / \mathfrak{p}\mathcal{O}_L$ has nilpotent.

$\Rightarrow$ Trace form $Tr_{R/k}(-,-)$ is degenerate. pick $\bar{x_i}$ basis, x_i are lifts.

$\Rightarrow \Delta(\bar{x_1}, \cdots \bar{x_n}) = 0 \quad \forall \bar{x_i} \in \mathcal{O}_L / \mathfrak{p}\mathcal{O}_L$ (Δ is the det of trace form)

$\Rightarrow \Delta(x_1, \cdots, x_n) = 0 \mod \mathfrak{p} \quad \forall x_1, \cdots x_n \in \mathcal{O}_L$.

ii) $\mathfrak{p}$ unramified.

$\Rightarrow \mathcal{O}_L/\mathfrak{p}$ is product of finite extensions of $k = \mathcal{O}_K/\mathfrak{p}$

$\Rightarrow$ trace form non degenerate.

$\Rightarrow$ let $\bar{x}_1, \cdots, \bar{x}_n$ be bases of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ as k v.s. $\Delta(\bar{x}_1, \cdots \bar{x}_n) \neq 0$

def discriminant

the ideal $d_{L/K} \subseteq \mathcal{O}_K$ generated by $\Delta(x_1, \cdots x_n)$ by all choices of $(x_1, \cdots x_n) \in \mathcal{O}_L$.

Cor $\mathfrak{p}$ ramifies in $L \Leftrightarrow \mathfrak{p} \mid d_{L/K}$

only finitely many primes ramify. ??? how to show $\leftarrow$

def. inverse different

$D_{L/K}^{-1} = \{ y \in L : Tr_{L/K}(xy) \in \mathcal{O}_K \quad \forall x \in \mathcal{O}_L \}$. an $\mathcal{O}_L$- submodule of L containing $\mathcal{O}_L$.

lemma $D_{L/K}^{-1}$ is a fractional ideal

let $x_1, \cdots x_n \in \mathcal{O}_L$, be a basis of L as a K v.s.

$d = \Delta(x_1, \cdots x_n) = \det(Tr_{L/K}(x_i x_j)) \in \mathcal{O}_K$ Want to "scale down" by d.

for $x \in D^{-1}_{L/K}$, $x = \sum_{j=1}^{n} \lambda_j x_j$ $\lambda_j \in K$.

then $\boxed{Tr_{L/K}(x x_i) = \sum_{j=1}^{n} \lambda_j Tr_{L/K}(x_i x_j)}$

linearity of trace.

set $A_{ij} := Tr_{L/K}(x_i x_j)$ mult by $Adj(A) \in M_n(O_K)$

$$d \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = Adj(A) \begin{pmatrix} Tr_{L/K}(x x_1) \\ \vdots \\ Tr_{L/K}(x x_n) \end{pmatrix}$$ each in O_K

$\times$ adjugate matrix on each side

$\Rightarrow \lambda_i \in \frac{1}{d} O_K \Rightarrow x \in \frac{1}{d} O_L$ so $D^{-1}_{L/K} \subseteq \frac{1}{d} O_L \Rightarrow D^{-1}_{L/K}$ is fractional ideal.

proof scheme

- $x_i \in O_L$ a basis of L as K v.s.
- $d = \Delta(x_1, \cdots, x_n)$
- $x \in D^{-1}_{L/K}$, write $x = \sum \lambda_j x_j$
- some vector / matrix mult $\rightarrow \lambda_i \in \frac{1}{d} O_K$, $x \in \frac{1}{d} O_L$

def. if p is a nonzero prime ideal of O

fractional ideal: $p^{-1} = \{x \in K \mid xp \subset O\}$

$p^{-1} p = O$.

def. the different ideal

$D_{L/K} \subseteq O_L$ is inverse of $D^{-1}_{L/K}$. It's an ideal.

prop. fractional ideals

fractional ideals form a group

I_K I_L are groups of fractional ideal for K, L respectively

$\Rightarrow I_K \cong \bigoplus_{\substack{0 \neq p \\ \text{prime ideal}}} \mathbb{Z}$ $\qquad I_L \cong \bigoplus_{\substack{0 \neq P \\ \text{prime ideal}}} \mathbb{Z}$.

def $N_{L/K}$

$N_{L/K}: I_L \to I_K$ group homomorphism

$P \to p^f$, where $p = P \cap O_K$, $f = f(P/p)$ res. class degree.

Week 5 lec 3

Setting: L/K degree n, ext of number fields. I_L, I_K group of fractional ideals

$N_{L/K} : I_L \to I_K$

$\mathfrak{P} \to p^f \qquad p = \mathfrak{P} \cap \mathcal{O}_K$

Prop $L^\times, K^\times, I_L, I_K$ commutes w.r.t two defns of $N_{L/K}$

fact:

$$\begin{tikzcd} L^\times \arrow[r] \arrow[d, "N_{L/K}"'] & I_L \arrow[d, "N_{L/K}"] \\ K^\times \arrow[r] & I_K \end{tikzcd}$$

field norm → $N_{L/K}$

hom between fractional ideals.

commutes

Proof: $\boxed{v_{\mathfrak{P}}(N_{L_{\mathfrak{P}}/K_p}(x)) = f_{\mathfrak{P}/p}\, v_{\mathfrak{P}}(x)}$ $\quad x \in L_{\mathfrak{P}}^\times$ & cor 10.10: $N_{L/K}(x) = \prod_{\mathfrak{P}|p} N_{L_{\mathfrak{P}}/K_p}(x)$

Thm 12.7. $\underbrace{N_{L/K}(D_{L/K})}_{\text{ideal in } \mathcal{O}_L} = \underbrace{d_{L/K}}_{\text{ideal in } \mathcal{O}_K}$

$N_{L/K}: I_L \to I_K$

$\mathfrak{P} \mapsto p^f$

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

$d_{L/K} =$ ideal generated by all $\Delta(x_1, \cdots, x_n)$ $\forall x_1, \dots, x_n \in \mathcal{O}_L$, this value in K.

Proof sketch (details omitted)

Assume $\mathcal{O}_K, \mathcal{O}_L$ are PIDs.

$x_1, \cdots, x_n$ be an $\mathcal{O}_K$ basis for $\mathcal{O}_L$

$y_1, \cdots, y_n$ be dual basis w.r.t trace form. $\quad ((x_i, y_j) = \delta_{ij})$

then, $y_1, \cdots, y_n$ is a basis for $D^{-1}_{L/K}$.

let $\sigma_1, \cdots, \sigma_n : L \to \bar{K}$ be distinct embeddings.

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

but $\Delta(x_1, \cdots, x_n) = \det[\underbrace{\sigma_i(x_j)}_{\text{matrix}}]^2$ so $\Delta(x_1, \cdots x_n)\Delta(y_1, \cdots, y_n) = 1$

$\Delta(x_1, \cdots x_n)\Delta(y_1, \cdots y_n) = \det[\sigma_i(x_j)]^2 \Delta(y_1, \cdots, y_n)$

$= \det(\sigma_i(x_j))^2 \det(\sigma_i(y_j))^2$

$= 1$ transpose inverse of matrix y.

write $D^{-1}_{L/K} = \beta \mathcal{O}_L$ (assumed L is a PID), $\beta \in L$ (the fractional part.)

then $d^{-1}_{L/K} = (\Delta(x_1, \cdots x_n))^{-1}$ ← PID, so ideal generated by it.

unsure why?

$= \Delta(y_1, \cdots, y_n)$ $\quad$ ~~y_i basis for D^{-1}~~

$= \Delta(\beta x_1, \cdots, \beta x_n)$ $\quad$ } change of basis b/c invertible, βx_i also a basis

$= N_{L/K}(\beta)^2 \Delta(x_1, \cdots x_n)$

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

in general, just localise. localise at $S = \mathcal{O}_K \setminus \mathfrak{p}$.

$$S^{-1} D_{L/K} = D_{S^{-1}\mathcal{O}_L / S^{-1}\mathcal{O}_K} \qquad S^{-1} d_{L/K} = d_{S^{-1}\mathcal{O}_L / S^{-1}\mathcal{O}_K}.$$

---

* unfam with proof

Proof scheme:
- ↳ x_i basis, y_i dual basis
- ↳ $\Delta(x_1, \cdots x_n)\Delta(y_1, \cdots y_n) = 1$
- ↳ $D_{L/K}^{-1} = \beta \mathcal{O}_L$
- ↳ $d_{L/K}^{-1} = (\Delta(x_1, - x_n)) = N_{L/K}(\beta^2)\,\Delta(x_1, - x_n)$
- ↳ to generalize, use localisation.

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

If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and α has a monic polynomial $g(\alpha) \in \mathcal{O}_K[x]$. then $D_{L/K} = (g'(\alpha))$

Proof.

let $\alpha_1, \cdots \alpha_n$ be roots of g

write $\dfrac{g(x)}{x-\alpha} = \beta_{n-1}x^{n-1} + \beta_{n-2}x^{n-2} + \cdots + \beta_0$, $\beta_i \in \mathcal{O}_L$ $\beta_{n-1} = 1$

coeff at x^s is β_s

we claim that $\sum_{i=1}^{n} \dfrac{g(x)}{x-\alpha_i} \cdot \dfrac{\alpha_i^r}{g'(\alpha_i)} = x^r \quad \forall\, 0 \le r \le n-1$

- ↳ this is because that the diff of two sides is a poly strictly less than n.
- ↳ at each α_j at $i \neq j$, it's 0, at $i = j$, $\dfrac{(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_i) \cdots (\alpha_i - \alpha_n)}{g'(\alpha_i)} \cdot \alpha_i^r = \alpha_i^r$ ✓

Now, equating the coefficients of x^s

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

(LHS, coeff at x^s is $\left(\sum \beta_s \cdot \dfrac{\alpha_i^r}{g'(\alpha_i)}\right)$ but $=$ trace $\left(\beta_s \dfrac{\alpha^r}{g'(\alpha)}\right)$ since trace(smth) $= \sum \sigma(x_i)$)

trace form

since $\mathcal{O}_L$ has an $\mathcal{O}_K$ basis $1, \alpha, \alpha^2, \cdots \alpha^{n-1}$, $D_{L/K}^{-1}$ has $\mathcal{O}_K$ basis given by

$\dfrac{\beta_0}{g'(\alpha)}, \dfrac{\beta_1}{g'(\alpha)}, \cdots, \dfrac{\beta_{n-1}}{g'(\alpha)} = \dfrac{1}{g'(\alpha)}$ } form dual basis.

each $\beta_i \in \mathcal{O}_L$, as ideal, generated by $\dfrac{1}{g'(\alpha)}$.

$\Rightarrow D_{L/K}^{-1} = \left(\dfrac{1}{g'(\alpha)}\right) \quad \Rightarrow D_{L/K} = (g'(\alpha))$

Proof scheme:
- ↳ let $\alpha_1, \cdots, \alpha_n$ be roots
- ↳ write $\beta_i = \dfrac{g(x)}{x-\alpha}$
- ↳ claim $x^r = \boxed{}$
- ↳ use trace/ dual basis to show $D_{L/K}^{-1} = \dfrac{1}{g'(\alpha)}$

reminder that $\mathcal{P}$ prime of $\mathcal{O}_L$, $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$.

define $D_{L_\mathcal{P}/K_\mathfrak{p}}$ similarly using $\mathcal{O}_{K_\mathfrak{p}}, \mathcal{O}_{L_\mathcal{P}}$

identify $D_{L_\mathcal{P}/K_\mathfrak{p}}$ with power of $\mathcal{P}$.

thm. $D_{L/K} = \prod_{\mathcal{P}} D_{L_\mathcal{P}/K_\mathfrak{p}}$ (similar to $K_\mathfrak{p} \otimes L \cong \prod_{\mathcal{P}} L_\mathcal{P}$)

Proof: let $x \in L$, $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal.

then (*) $Tr_{L/K}(x) = \sum_{\mathcal{P}|\mathfrak{p}} Tr_{L_\mathcal{P}/K_\mathfrak{p}}(x)$ (proof same as cor 10.10) ($x \in L \Rightarrow N_{L/K}(x) = \prod_{\mathcal{P}|\mathfrak{p}} N_{L_\mathcal{P}/K_\mathfrak{p}}(x)$) just change Norm to Trace.

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

show $\subseteq$ ($D_{L/K} \subseteq \prod_{\mathcal{P}} D_{L_\mathcal{P}/K_\mathfrak{p}}$) WTS $(r(\mathcal{P}) \geq s(\mathcal{P}))$ ☆ don't quite get containment valuation bigger $\Rightarrow$ correspond to a subset ? " product of local inverse different is contained in the global inverse different "

in the fractional ideal $\mathcal{P}^{-1}$

let $x \in L$ s.t. $v_\mathcal{P}(x) \geq -s(\mathcal{P})$ $\forall \mathcal{P}$ so it's in local different. WTS in global different.

then $Tr_{L_\mathcal{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in \mathcal{O}_L$ and $\forall \mathcal{P}$.

(*) $\Rightarrow$ $Tr_{L/K}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in \mathcal{O}_L$ $\forall \mathfrak{p}$

$\Rightarrow$ $Tr_{L/K}(xy) \in \mathcal{O}_K$ $\forall y \in \mathcal{O}_L$

so $x \in D_{L/K}^{-1}$

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

MUST REVIEW

show " $\supseteq$ " $r(\mathcal{P}) \leq s(\mathcal{P})$

fix $\mathcal{P}$ and let $x \in \mathcal{P}^{-r(\mathcal{P})} \setminus \mathcal{P}^{-r(\mathcal{P})+1}$

then $v_\mathcal{P}(x) = r(\mathcal{P})$, $v_{\mathcal{P}'}(x) \geq 0$ $\forall \mathcal{P}' \neq \mathcal{P}$

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

$\Rightarrow$ $Tr_{L_\mathcal{P}/K_\mathfrak{p}}(xy) \in \mathcal{O}_{K_\mathfrak{p}}$ $\forall y \in L_\mathcal{P}$

$\Rightarrow$ $x \in D_{L_\mathcal{P}/K_\mathfrak{p}}^{-1}$ i.e. $-v_\mathcal{P}(x) = r(\mathcal{P}) \leq s(\mathcal{P})$

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

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

proof: apply $N_{L/K}$ to $D_{L/K} = \prod_{\mathcal{P}} D_{L_\mathcal{P}/K_\mathfrak{p}}$

Unramified & totally ramified extensions of local fields.

Notation change: L/K finite, separable extension of non-arch local fields.

cor $[L:K] = e_{L/K} f_{L/K}$ $(*)$

lemma tower law for e, f

let $M/L/K$ be finite separable extension of non-arch local fields. Then we get tower law:

1) $f_{M/K} = f_{M/L} \cdot f_{L/K}$

2) $e_{M/K} = e_{M/L} \cdot e_{L/K}$.

Proof. 1) $f_{M/K} = [k_M : k] = [k_M : k_L] \cdot [k_L : k] = f_{M/L} \cdot f_{L/K}$

2) (i) + $(*)$ + tower law

$e_{M/K} f_{M/K} = [M:K] = [M:L][L:K] = e_{M/L} f_{M/L} \cdot e_{L/K} f_{L/K}$

def __ / un/ totally ramified

the extension L/K is

unramified	if	$e_{L/K} = 1$	$\Leftrightarrow$	$f_{L/K} = [L:K]$
ramified		$e_{L/K} > 1$	$\Leftrightarrow$	$f_{L/K} < [L:K]$
totally ramified		$e_{L/K} = [L:K]$	$\Leftrightarrow$	$f_{L/K} = 1$

Week 6 lec 1

L/K finite separable ext of local fields

thm. split extension into unram and tot. ram

There exists a field K_0 s.t. $K \subseteq K_0 \subseteq L$ and

1) K_0/K is unramified

2) L/K_0 is totally ramified.

$$\begin{tikzcd} L \arrow[dr, dash, "e_{L/K}"] \arrow[dd, dash] & \\ & K_0 \arrow[dl, dash, "f_{L/K}"] \\ K & \end{tikzcd}$$

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

Proof. let $k = \mathbb{F}_q$ be the residue field of K.

So the residue field of L is k_L where $k_L = \mathbb{F}_{q^f}$, $f = f_{L/K}$.

Set $m = q^f - 1$. $[\cdot\cdot\cdot] : \mathbb{F}_{q^f} \to L$ be teichmuller lift for L.

let α be a generator for $\mathbb{F}_{q^f}^\times$. let $\xi_m = [\alpha]$, ξ_m a m^{th} root of unity (lec 5). cyclotomic extns $\Rightarrow$ Galois.

Set $K_0 = K(\xi_m)$ then K_0/K is Galois, as it's the splitting field of $x^m - 1$.

K_0 has residue field $k_0 = \mathbb{F}_q(a) = \mathbb{F}_{q^f}$

let $res: Gal(K_0/K) \to Gal(k_0/k)$ be the natural map.

for $\sigma \in Gal(K_0/K)$, $\sigma(\xi_m) = \xi_m$ if $\sigma(\xi_m) \equiv \xi_m \mod m_0$ — max ideal in $\mathcal{O}_{K_0}$

since $\underbrace{\mathcal{O}_{K_0}^\times \to k_0^\times}$ induces a bijection in $\mathcal{O}_{K_0}$ between m^{th} root of unity (Hensel) hence res is injective.

Hensel's lemma: unique lift of ROU in $k_0^\times$, so if you know where $res(\sigma)$ sends ξ_m, you know where it sends ξ_m in $\mathcal{O}_K$ so injective.

Therefore $|(Gal\, K_0/K)| \leq |Gal\,(k_0/k)| = f_{K_0/K}$. because $f_{K_0/K} \leq [K_0:K]$ always, so

so $[K_0:K] = f_{K_0/K}$ $\Rightarrow$ res is iso and K_0/K is unramified.

since $k_0 = k_L$ $(= \mathbb{F}_{q^f})$ have $f_{L/K} = f_{K_0/K} = [K_0:K]$ $\quad e_{K_0/K} = 1$.

$\uparrow$ = by how K_0 is defined, $\uparrow$ = by defn beginning

so $f_{L/K_0} \cdot f_{K_0/K} = f_{L/K}$ $\Rightarrow$ $f_{L/K_0} = 1$ $\Rightarrow L/K_0$ totally ram.

$e_{L/K} = [L:K_0]$ by tower law.

$[L:K] = e_{L/K} \cdot f_{L/K} = [L:K_0][K_0:K]$
$\qquad\qquad\qquad\qquad\qquad\qquad f_{L/K}$

Proof scheme:

↳ set $k = \mathbb{F}_q$, $k_L = \mathbb{F}_{q^f}$, $f = f_{L/K}$. $m = q^f - 1$.

↳ define ξ_m

↳ set $K_0 = K(\xi_m)$ K_0/K is Galois

↳ $k_0 = k_L$.

↳ use the fact $res: Gal\,(K_0/K) \to Gal\,(k_0/k)$ injective to show $[K_0:K] = f_{K_0/K}$

↳ rest by tower law & $[A:B] = e_{A/B} f_{A/B}$.

thm unramified extensions are easy to understand. — just K adjoint a root of unity!

let $k = \mathbb{F}_q$. for each $n \geq 1$, $\exists$ unique unramified extension L/K of degree n.

Moreover, L/K is Galois and the natural map $res: Gal(L/K) \to Gal(k_L/k)$ is $\cong$.

in particular, $Gal\,(L/K) = \langle Frob_{L/K} \rangle$ is cyclic, where $Frob_{L/K}(x) = x^q \mod m_L$ $\forall x \in \mathcal{O}_L$

Proof for $n \geq 1$, take $L = K(\xi_m)$, $m = q^n - 1$

$\uparrow$ primitive m^{th} root of unity

as in prev. thm, $Gal(L/K) \to Gal(k_L/k)$ is an $\cong$.

$\cong Gal\,(\mathbb{F}_{q^n}/\mathbb{F}_q)$

so L/K is unramified, $Gal\,(L/K)$ is generated by a lift of $x \mapsto x^q$??

this shows $\exists$.

uniqueness: suppose L/K, L/K is unramified of degree n, using Teichmuller lifts, can show $\xi_m \in L$ for some primitive mth root of unity ξ_m, $m = p^n - 1$ then $L = K(\xi_m)$. (by degree reasons)

same as prev thm, take a unit & take lift again

Proof scheme

↳ existence, given n, follow same construction as above.

↳ uniqueness, using teichmuller lifts.

Cor L/K finite Galois, then the map

$$\text{res}: Gal(L/K) \longrightarrow Gal(k_L/k)$$ is surjective.

Proof. res factors as

$$Gal(L/K) \twoheadrightarrow Gal(K_0/K) \xrightarrow[\sim]{} Gal(k_L/k) \quad (\text{as } k_0 = k_L)$$

def. The inertia subgroup

L/K finite Galois, the inertia subgroup is

$$I_{L/K} = \ker(Gal(L/K) \to Gal(k_L/k)) \subseteq Gal(K/L)$$

Since $e_{L/K} f_{L/K} = [L:K]$, have $|I_{L/K}| = e_{L/K}$. (as $[L:K] = e \cdot f$, $|Gal(k_L/k)| = f$)

$I_{L/K} = Gal(L/K_0)$ controlls the totally ramified ones.

Now look @ totally ram part. (controlled by Eisenstein Poly)

def. Eisenstein polynomial

$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \mathcal{O}_K[x]$ is Eisenstein if $v_K(a_i) \geq 1 \ \forall i$, $v_K(a_0) = 1$

normalised valuation

Fact: Eisenstein $\Rightarrow$ irreducible

Thm. totally ramified & Eisenstein

1) let L/K be finite, totally ramified, $\pi_L \in \mathcal{O}_L$ unif, then the min poly of π_L is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ $(L = \mathcal{O}_K(\pi_L))$

2) conversely, if $f(x) \in \mathcal{O}_K[x]$ is eisenstein, α a root of f, $L = K(\alpha)/K$ is totally ramified and α is unif in L.

Proof :

i) $[L:K]=e$

coeff in $\mathcal{O}_K$, as integral over.

let $f(x)=x^m+a_{m-1}x^{m-1}+\dots+a_0 \in \mathcal{O}_K[x]$ be min poly for π_L. Then $m \le e$.

since $\underset{\text{valuation}}{v_L}(K^\times)=e\mathbb{Z}$, ? have $v_L(a_i\pi_L^i)\equiv i \mod e$, $i<m$.

norm

in $\mathcal{O}_K$ so v_L mult of e.

So these terms have distinct valuation. all diff mod e.

as $\pi_L=-\sum_{i=0}^{m-1} a_i\pi_L^i$, have $m=v_L(\pi_L^m)=\min_{0\le i\le m-1}(i+ev_K(a_i))$

$\Rightarrow v_K(a_i)\ge 1$ $\forall i$ (if any of them is 0, the above won't work) all have diff val, so = smallest val.

So $v_K(a_0)=1$ and $m=e$ (given constraint $m\le e$, this is only choice to make it work)

So $f(x)$ is Eisenstein, $m=e$, so $L=K(\pi_L)$

to show $\mathcal{O}_L=\mathcal{O}_K[\pi_L]$

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

then $v_L(y)=\min_{1\le i\le e-1}(i+ev_K(b_i))$

if any <0, every term <0.

so $y\in\mathcal{O}_L \Leftrightarrow v_L(y)\ge 0 \Leftrightarrow v_K(b_i)\ge 0 \Leftrightarrow y\in\mathcal{O}_K[\pi_L]$.

ii) let $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0\in\mathcal{O}_K[x]$ be Eisenstein. let $e=e_{L/K}$ ($L=K(\alpha)$, α a root)

then, $v_L(a_i)\ge e$ and $v_L(a_0)=e$.

If $v_L(\alpha)\le 0$ then have $\underbrace{v_L(\alpha^n)}_{n v_L(\alpha)} < \underbrace{v_L(\sum_{i=0}^{n-1} a_i\alpha^i)}_{\text{min of val of terms. so } v_L(a_i)+iv_L(\alpha) \text{ bigger than LHS.}}$ ※.

So $v_L(\alpha)>0$.

for $i\ne 0$, $\overbrace{v_L(a_i\alpha^i)}^{=v_L(a_i)+iv_L(\alpha)>e}>e=v_L(a_0)$

therefore $v_L(-\sum_{i=0}^{n-1}a_i\alpha^i)=e$ = min of val of each term. indeed min at a_0

$\qquad\qquad ||$

$\quad v_L(\alpha^n)=nv_L(\alpha)$

but $n=[L:K]\ge e$ $\Rightarrow$ $n=e$ and $v_L(\alpha)=1$

$ef=[L:K]$

Proof scheme:

1) $\hookrightarrow$ $[L:K]=e$. write min poly for π_L.

$\hookrightarrow$ $v_L(a_i\pi_L^i)\equiv 1 \mod e$. So each term have distinct valuation.

↳ $\pi_L^m = -\sum_{i=0}^{m-1} a_i \pi_L^i$

write $m = \min(\quad)$

↳ but only one choice of the coefficients.

↳ above show Eisenstein

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

↳ $v_L(y) = \min(\quad)$

↳ $y \in \mathcal{O}_L \Leftrightarrow$ ______

2) ↳ Assume Eisenstein, write coefficient in v_L.

↳ $v_L(\alpha) \leq 0 \Rightarrow$ ※

↳ $v_L(\alpha^n) = v_L(-\sum a_i \alpha^i) = \min_i (v_L(\quad))$ but each $i \neq 0$, $v_L(a_i \alpha^i) > e$.

so attain min at $i=0$

↳ $n = e$

Structure of units

def. absolute ram index

let $[K:\mathbb{Q}_p] < \infty$. $e: e_{K/\mathbb{Q}_p}$ be absolute ram index, π unit in K.

Week 6 lecture 2

Prop Structure of units, additive & multiplicative

if $r > e/_{p-1}$, $\exp(x) = \sum_{i=0}^{\infty} \frac{x^n}{n!}$ converge in $\pi^r \mathcal{O}_K$ and induces isomorphism in

$$(\pi^r \mathcal{O}_K, +) \cong (\underbrace{1+\pi^r \mathcal{O}_K}_{\text{subgroup of units in } \mathcal{O}_K}, \times)$$

Proof

↳ $\pi^r \mathcal{O}_K \longrightarrow 1+\pi^r \mathcal{O}_K$

since $[K:\mathbb{Q}_p] < \infty$, have

$$v_K(n!) = e\, v_p(n!) \underset{\text{ex sheet 1}}{\overset{=}{\uparrow}} \frac{e(n - S_p(n))}{p-1} \leq \frac{e(n-1)}{p-1}$$

for $x \in \pi^r \mathcal{O}_K$, $n \geq 1$, $v_K\left(\frac{x^n}{n!}\right) = n v_K(x) - v_K(n!)$

$$\geq nr - \frac{e(n-1)}{p-1} = r + (n-1)\underbrace{\left(r - \frac{e}{p-1}\right)}_{>0}$$

so $v_K\left(\frac{x^n}{n!}\right) \to \infty$ as $n \to \infty$

thus $\exp(x)$ converges (the sum $\sum \frac{x^n}{n!}$ is Cauchy)

Since $v_K\left(\frac{x^n}{n!}\right) \geq r$, (for each $n > 0$ have $\exp(x) \in 1+\pi^r \mathcal{O}_K$.)

$\hookrightarrow$ $1+\pi^r\mathcal{O}_K \longrightarrow \pi^r\mathcal{O}_K$

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

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

check convergence as before. TODO

Recall identity in $\mathbb{Q}[[x,y]]$, $\begin{cases} \exp(x+y) = \exp(x)\exp(y) \\ \exp(\log(1+x)) = 1+x \\ \log(\exp(x)) = x. \end{cases}$???

therefore, $\exp : (\pi^r\mathcal{O}_K, +) \xrightarrow{\sim} (1+\pi^r\mathcal{O}_K, \times)$ is an iso.

(not true for = char as factorial don't work in finite field). Proof scheme!

Proof scheme:

$\pi^r\mathcal{O}_K \to 1+\pi^r\mathcal{O}_K$:
- get bound on $v_p(n!) = \frac{e(n-1)}{p-1}$
- so $v_K\left(\frac{x^n}{n!}\right) \to \infty$, cauchy
- in $1+\pi^r\mathcal{O}_K$

$1+\pi^r\mathcal{O}_K \to \pi^r\mathcal{O}_K$
- define log
- just define some identity in $\mathbb{Q}[[x,y]]$.

Why not work in fields of = char?

---

def. The s^{th} unit group $U_K^{(s)}$

K a local field. $U_K := \mathcal{O}_K^\times$ and fix $\pi \in \mathcal{O}_K$ a uniformizer.

then for $s \in \mathbb{Z}_{\geq 1}$, the s^{th} unit group $U_K^{(s)}$ is defined by

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

Set $U_K^{(0)} = U_K$, then we have a filtration

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

Prop. quotients of filtration for unit groups

1) $U_K^{(0)} / U_K^{(1)} \cong (k^\times, \times)$ $\quad k = \mathcal{O}_K/\pi$

2) $U_K^{(s)} / U_K^{(s+1)} \cong (k^\times, +)$ $\quad s \geq 1$

Proof:

1) reduction modulo π.

$$U_K^{(0)} = U_K = \mathcal{O}_K^\times \qquad U_K^{(1)} = 1 + \pi\mathcal{O}_K$$

$\mathcal{O}_K^\times \longrightarrow k^\times$ is surjective with kernel $1+\pi\mathcal{O}_K = U_K^{(1)}$.

multiply here

addition here

2) $f : U_K^{(s)} \longrightarrow k$

$$1 + \pi^s x \longmapsto x \bmod \pi. \qquad x \in \mathcal{O}_K$$

check it gives hom:

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

but $\quad \pi^s xy + x + y = x+y \bmod \pi.$

f is a group hom, surjective, and with $\ker(f) = U_K^{(s+1)}$

Proof scheme
1) $U_K^{(0)}/U_K^{(1)}$ reduction mod π. just quotient, kernel works as expected.
2) $U_K^{(s)}/U_K^{(s+1)}$ define f, is a group hom, surj with correct kernel.

Cor finite index subgroup of $\mathcal{O}_K^\times \cong (\mathcal{O}_K, +)$

K mixed char. $[K:\mathbb{Q}_p] < \infty$. then, $\exists$ finite indexed subgroup of $\mathcal{O}_K^\times \cong (\mathcal{O}_K, +)$ why iso?

Proof: $r > \frac{e}{p-1}$, $U_K^{(r)} \cong (\mathcal{O}_K, +)$ by the exp and log thm.

$U_K^{(r)} \subseteq U_K$, finite indexed by the prev-prop (quotients of $U_K^{(s)}$)

note not true for K equal char:

(so $(\mathcal{O}_K, +) \cong U_K^{(r)}$ but $U_K^{(r)} \subseteq U_K = \mathcal{O}_K^\times$ so $(\mathcal{O}_K, +)$ is subgroup of $\mathcal{O}_K^\times$).

Proof scheme: $U_K^{(r)}$ is that one! Also, finite index by filtration & quotient thm.

example of unit groups

for $\mathbb{Z}_p$, $p > 2$, $e = 1$, take $r = 1$, as $r > \frac{e}{p-1}$

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

$$x \mapsto \left(x \bmod p, \frac{x}{[x \bmod p]}\right)$$ — teichmuller lifting.

for $p = 2$, $r = 1$ no longer works. Then take $r = 2$.

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

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

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

this gives another proof ?

$$\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 = \begin{cases} \mathbb{Z}/2\mathbb{Z} & p > 0 \\ (\mathbb{Z}/2\mathbb{Z})^2 & p = 0 \end{cases}$$

Higher Ramification groups

L/K finite Galois, extension of local fields, $\pi_L \in \mathcal{O}_L$, uniformizer.

defn. higher ramification groups

v_L be normalized valuation on L. For $s \in \mathbb{R}_{\geq -1}$, the s^{th} rami group is:

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

examples of ramification groups.

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

$$G_0(L/K) = \{ \sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) = x \mod \pi_L \quad \forall x \in \mathcal{O}_L \}$$

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

Don't quite get this eq

$$= I_{L/K}$$

$\mathcal{O}_L/\pi_L$

acts trivially on the field k_L. so any x, write as $x = y + z$ $y \in \pi_L$ $z \in \pi_L \mathcal{O}_K$

have $\sigma(x) = \sigma(y) + \sigma(z)$

But $\sigma(x) - x = \underbrace{y - \sigma(y)}_{0} + \underbrace{z + \sigma(z)}_{\in \pi_L \mathcal{O}_K} \Rightarrow \sigma(x) - x \equiv 0 \mod \pi_L.$

Write G_s as a normal subgroup

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

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

so $G_s(L/K)$ is a normal subgroup of $\mathrm{Gal}(L/K)$

get $G_s \subseteq G_{s-1} \subseteq G_{s-2} \subseteq \cdots \subseteq \underset{I_{K/L}}{G_0} \subseteq \underset{\mathrm{Gal}}{G_{-1}}$

remark: G_s only change at integers.

Thm Properties about higher ram group

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

ii) $\bigcap_{s=0}^{\infty} G_s = \{1\}$

iii) let $s \in \mathbb{Z}_{\geq 0}$ $\exists$ injective group hom

$$G_s / G_{s+1} \hookrightarrow U_L^{(s)} / U_L^{(s+1)}$$

induced by $\sigma \mapsto \dfrac{\sigma(\pi_L)}{\pi_L}$ this map is independent of the choice π_L.

Why allowed to replace?

Proof let $K_0 \subseteq L$ be the maximal unramified extension of K in L. replace K by K_0, assume L/K is totally ramified.

i) thm 13.8 (totally ramified $\Leftrightarrow$ Eisenstein) implies $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

$\supseteq$: Suppose $v_L(\sigma(\pi_L) - \pi_L) \geq s+1$, let $x \in \mathcal{O}_L$, then $x \in f(\pi_L)$ for some $f(x) \in \mathcal{O}_K[x]$,

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

$= f(\sigma(\pi_L)) - f(\pi_L)$ since same constant term

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

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

$\subseteq$: containment is trivial.

ii) Suppose $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \neq 1$. Then $\sigma(\pi_L) \neq \pi_L$ as $L = K(\pi_L)$ so $v_L(\sigma(\pi_L) - \pi_L) < \infty$

if $\sigma(\pi_L) = \pi_L$, it would fix all L as $L = K(\pi_L)$

so $\sigma \notin G_{1 + v_L(\sigma(\pi_L) - \pi_L)}$

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

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

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

We claim that the map $\varphi: G_s \longrightarrow U_L^{(s)} / U_L^{(s+1)}$

$\sigma \longmapsto \frac{\sigma(\pi_L)}{\pi_L}$ is a group hom with kernel G_{s+1}.

Show φ is a group homomorphism. $\quad$ why Gal: units $\to$ units ?

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

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

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

So $\frac{\sigma(u)}{u} \in 1 + \pi_L^{s+1} \mathcal{O}_L$ since u is a unit

So $\frac{\sigma\tau(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \cdot \frac{\tau(\pi_L)}{\pi_L} \mod U_L^{(s+1)}$ (reminder $U_L^{(s+1)} = 1 + \pi^{s+1} \mathcal{O}_L$)

So φ is a group homomorphism.

If it's in kernel have $\frac{\sigma(\pi_L)}{\pi_L} \in 1+\pi_L^{s+1}\mathcal{O}_L$

Show that $\ker(\varphi)$ is right

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

$= G_{s+1}$ by (i)

Show doesn't depend on uniformizer.

If $\pi_L' = a\pi_L$ is another uniformizer.

then $\frac{\sigma(\pi_L')}{\pi_L'} = \underbrace{\frac{\sigma(a)}{a}}_{\text{it's a unit.}} \cdot \frac{\sigma(\pi_L)}{\pi_L} = \frac{\sigma(\pi_L)}{\pi_L} \mod U_L^{(s+1)}$

Proof Scheme:

assume the extension is totally rami.

i) ↳ $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$

↳ assume $v_L(\sigma(\pi_L)-\pi_L) \geq s+1$

↳ let $x \in \mathcal{O}_L$ then $x = f(\pi_L)$

↳ expand $v_L(\sigma(x)-x)$.

ii) look at $\sigma(\pi_L) \neq \pi_L$ if $\sigma \neq 1$

iii) ↳ see that $\varphi: G_s \longrightarrow U_L^{(s)}/U_L^{(s+1)}$

$\sigma \longmapsto \frac{\sigma(\pi_L)}{\pi_L}$ is well defined.

↳ show it's hom: write $\tau(\pi_L) = u\pi_L$. $u \in \mathcal{O}_L^\times$

↳ show $\ker(\varphi) = G_{s+1}$ by (i)

↳ show doesn't depend on choice of π_L.

Week 6 lec 3

cor. 14.3 Given a finite Galois extension of local fields, $\mathrm{Gal}(L/K)$ is solvable.

Proof: $G_s/G_{s+1} \cong$ a subgroup of
$$\begin{cases} \mathrm{Gal}(k_L/k) & \text{if } s=-1 \quad 13.4 \\ (k_L^\times, \times) & \text{if } s=0 \\ (k_L, +) & \text{if } s\geq 1 \end{cases} \quad 13.11 + 14.2$$

then G_s/G_{s+1} is solvable for $s \geq -1$.

Rmk let $\mathrm{char}\, k = p$ then $|G_0/G_1|$ is coprime to p. $|G_1| = p^n$ for some $n \geq 0$. Thus, G_1 is the unique (since normal) sylow-p subgroup of $G_0 = I_{L/K}$.

Recall $\begin{cases} G_{-1} = \mathrm{Gal}(L/K) \\ G_0 = I_{L/K} \\ G_1 = \text{wild inertia} \end{cases}$

def (tamely ramified / wildly ramified)

The group G_1 is called the wild inertia group. G_0/G_1 is the tame quotient.

let L/K finite, separable extension of local fields. L/K is tamely ramified if char $k \nmid e_{L/K}$.
($\Leftrightarrow$ $G_1 = \{1\}$ if L/K is Galois) otherwise it's wildly ramified.
???

Thm 14.5 relating $D_{L/K}$ with ramified.

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

then $\delta(L/K) \geq e_{L/K} - 1$ with $=$ iff L/K is tamely ramified.

In particular, L/K unramified $\Leftrightarrow$ $D_{L/K} = \mathcal{O}_L$

Proof By ex sheet 3, $D_{L/K} = D_{L/K_0} D_{K_0/K}$ for any intermediate K_0. Take K_0 to be the maximal unramified extension, therefore, why suffice to show this way?

suffices to check 2 cases 1) L/K unramified 2) L/K totally ramified.

case 1. L/K unramified.

Prop 6.12 $\Rightarrow$ $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$, $k_L = k(\bar{\alpha})$

let $g(x) \in \mathcal{O}_K[x]$ be the min poly of α.

$[L:K] = [k_L : k]$ $\Rightarrow$ $\bar{g}(x) \in k[x]$ is min poly of $\bar{\alpha}$.

$\bar{g}$ is separable, so $g'(\alpha) \not\equiv 0 \mod \pi_L$.

thm 12.8 $\Rightarrow$ $D_{L/K} = (g'(\alpha)) = \mathcal{O}_L$

case 2: L/K totally ramified.

$[L:K] = e$, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ where π_L is root of $g(x) = x^e + \sum_{i=1}^{e-1} a_i x^i \in \mathcal{O}_K[x]$, eisenstein.

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

so $v_L(g'(\pi_L)) \geq e-1$, equality $\Leftrightarrow$ $p \nmid e$ (tamely ramified) $v_L = e-1$, why $p \nmid e$?

Proof scheme: fill in why $v_L(e) = 0 \Leftrightarrow p \nmid e$?

Cor 14.6

L/K extension of number fields. $\mathfrak{P} \subseteq \mathcal{O}_L$, $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, then $e(\mathfrak{P}/\mathfrak{p}) > 1$ iff $\mathfrak{P} \mid D_{L/K}$.

Proof thm 12.9: $D_{L/K} = \prod_{\mathfrak{P}\mid\mathfrak{p}} D_{L_\mathfrak{P}/K_\mathfrak{p}}$

then $e(\mathfrak{P}/\mathfrak{p}) = e_{L_\mathfrak{P}/K_\mathfrak{p}}$ and thm 14.5 gives result.

(i.e. $e(\mathfrak{P}/\mathfrak{p}) > 1 \Leftrightarrow e_{L_\mathfrak{P}/K_\mathfrak{p}} > 1 \Leftrightarrow$ ramified

$\overset{\text{thm 14.5}}{\Leftrightarrow} D_{L/K} \neq \mathcal{O}_L$

$\Leftrightarrow D_{L/K} = \prod_\mathfrak{P} D_{L_\mathfrak{P}/K_\mathfrak{p}}$ for some $\mathfrak{P}|\mathfrak{p}$.

$\Leftrightarrow \mathfrak{P} \mid D_{L/K}$.

Example. Computing higher ramification groups of p^n roots of unity

Let $K = \mathbb{Q}_p$, ξ_{p^n} be p^n th root of unity

$L = K(\xi_{p^n})$. The p^n cyclotomic poly is $\phi_{p^n}(X) = X^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + 1 \in \mathbb{Z}_p[x]$.

By Exsheet 3, $\phi_{p^n}(X)$ is irreducible ($\Rightarrow \phi_{p^n}(x)$ is min poly of ξ_{p^n})

so $L/\mathbb{Q}_p$ is Galois, totally ramified of degree $p^{n-1}(p-1)$.

· let $\pi = \xi_{p^n} - 1$ a uniformizer of $\mathcal{O}_L$.

so $\mathcal{O}_L = \mathbb{Z}_p[\xi_{p^n} - 1] = \mathbb{Z}_p[\xi_{p^n}]$ why same?

→ $\mathrm{Gal}(L/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ abelian,

via $\sigma_m \mapsto m$ where $\sigma_m \in \mathrm{Gal}(L/\mathbb{Q}_p)$ is $\sigma_m(\xi_{p^n}) = \xi_{p^n}^m$

to compute higher ram groups,

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

$v_L(\pi) = 0$?

let k be maximal s.t. $p^k | m-1$. then ξ_p^{m-1} is a primitive p^{n-k} th root of unity.

so $\xi_{p^n}^{m-1} - 1$ is a uniformizer π' on $L' = \mathbb{Q}_p(\xi_p^{m-1})$

primitive root -1 is unif ?

therefore

$$v_L(\xi_{p^n}^{m-1} - 1) = e_{L/L'} = \frac{e_{L/K}}{e_{L'/K}} = \frac{[L:K]}{[L':K]} = \frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k$$

so $\sigma_m \in G_i \Leftrightarrow p^k \geq i+1$ i.e.

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

??? ???

VI Local Class field theory

§ infinite Galois Theory

L/K : alg extension any field.

defn a set of definitions

↳ L/K separable if $\forall \alpha \in L$, the min poly $f_\alpha(X) \in K[X]$ is separable.

↳ L/K normal if $f_\alpha(X)$ splits in L $\forall \alpha \in L$.

↳ L/K is Galois if it's separable & normal.

↳ $Gal(L/K) = Aut(L/K)$

↳ if L/K finite Galois, Galois correspondence

$$\{\text{sub extension } K \subseteq K' \subseteq L\} \longleftrightarrow \{\text{subgroups of } Gal(L/K)\}$$

$$K' \longmapsto Gal(L/K')$$

$$L^H \longleftarrow H$$

we want to extend this to infinite case, which requires a topology on $Gal(L/K)$.

we generalize the notion of an inverse limit.

def. directed set

let $(I, \leq)$ be a partially ordered set. I is a directed set if $\forall i,j \in I$, $\exists$ some $k \in I$ s.t. $i \leq k$, $j \leq k$.

example: any totally ordered set

or $\mathbb{Z}_{\geq 1}$ ordered by divisibility

def. inverse system

let $(i, \leq)$ be a directed set, and $(G_i)_{i \in I}$ a collection of groups together with maps $\varphi_{ij} : G_j \to G_i$ s.t.

$\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ $\quad i \leq j \leq k$

$\varphi_{ii} = id.$

instead of $\varphi_{ij} : G_{i+1} \to G_i$, it must satisfy "transition homomorphism" for all level above to below.

Such $((G_i)_{i \in I}$ is an inverse system)

Inverse limit of $((G_i)_{i \in I}, \varphi_{ij})$ is $\varprojlim_{i \in I} G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \varphi_{ij}(g_j) = g_i\}$

Remark:

- $(\mathbb{N}, \leq)$ recovers our prev. definition
- $\exists$ proj map $\phi_j : \varprojlim_{i \in I} G_i \to G_j$ for each j.

assume G_i is finite, we can put profinite topology on $\varprojlim_{i \in I} G_i$ to be weakest topology s.t. ψ_j cts, $\forall j \in I$.

Prop. Putting inverse system on Galois group

let L/K be Galois. Then,

1) $I = \{ F \subset L,\ F/K \text{ finite Galois} \}$ is a directed set ordered under inclusion.

2) for $F, F' \in I$, $F \subset F'$, there's a natural map $Gal(F'/K) \to Gal(F/K)$ by restriction, so we get inverse system of groups, $\{ Gal(F/K) : F \subset L,\ F/K \text{ finite Galois} \}$ indexed by I.

the natural map $Gal(L/K) \to \varprojlim_{F \in I} Gal(F/K)$ is an $\cong$.

Proof example sheet.

Week 7 lec 1

Recall 16.3 $\Rightarrow$ $$Gal(L/K) \cong \varprojlim_{\substack{K \subseteq F \subseteq L \\ F/K \text{ finite Galois}}} Gal(F/K)$$

Example.

$K = \mathbb{F}_q$, $L = \overline{\mathbb{F}_q}$ alg closure.

$\{F/K \text{ finite Galois}\} \Leftrightarrow \mathbb{N}_{\geq 1}$

$\mathbb{F}_{q^n} \leftrightarrow n$

note $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n} \Leftrightarrow m \mid n$

$\exists$ commutative diagram

frobenius: $Fr_q : x \mapsto x^q$

$$\begin{array}{ccccccc} Fr_q & \in & Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) & \xrightarrow{\text{res}} & Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) & \ni & Fr_q \\ \downarrow & & \wr\| & & \wr\| & & \downarrow \\ 1 & \in & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\text{proj}} & \mathbb{Z}/m\mathbb{Z} & \ni & 1 \end{array}$$

so, $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \varprojlim_{n (\mathbb{N}_{\geq 1}, |)} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}$ $\leftarrow$ profinite completion of $\mathbb{Z}$.

$Fr_q \leftrightarrow 1$

let $\langle Frq \rangle \subseteq Gal(\bar{\mathbb{F}}_q / \mathbb{F}_q)$ be a subgroup generated by Frq.
the inclusion $\langle Frq \rangle \subseteq Gal(\bar{\mathbb{F}}_q / \mathbb{F}_q)$ corresponds to $\mathbb{Z} \subseteq \hat{\mathbb{Z}} \ (\cong \prod_{p \text{ prime}} \mathbb{Z}_p)$? not sure why

Thm (Fundamental thm of Galois Theory)

let L/K be Galois.
Endow $Gal(L/K)$ with profinite topology. (= discrete to if L/K finite)
then $\exists$ bijection

$$\left\{ \begin{matrix} F/K \text{ subextension} \\ \text{of } L/K \end{matrix} \right\} \overset{1-1}{\longleftrightarrow} \left\{ \begin{matrix} \text{closed subgroup} \\ \text{of } Gal(L/K) \end{matrix} \right\}$$

$$F \longmapsto Gal(L/F)$$

$$\text{fixed elements of } L \text{ under } H. \to L^H \longleftarrow H \leq Gal(L/F)$$

Moreover, F/K finite iff $Gal(L/F)$ open.
F/K Galois $\Leftrightarrow$ $Gal(L/F)$ is a normal subgroup of $Gal(L/K)$ as $Gal\, F/K \cong \frac{Gal(L/K)}{Gal(L/F)}$.
Proof: see ex 4. 16.2 and 16.3 are main takeaways. ???

§ Weil group.
K a local field, L/K separable algebraic extension.

defn 16.5 (the case of infinite extensions) unramified / totally ramified.
i) L/K is unramified if F/K is unramified for all F/K finite sub extension.
ii) L/K is totally ramified if F/K is tot. rami for all F/K finite subextension.

Prop 16.6. $Gal(L/K) \cong Gal(k_L/k)$

let L/K be unramified. then L/K is Galois and $Gal(L/K) \cong Gal(k_L/k)$

unram $\Rightarrow$ Gal yes

Proof: every finite subextension F/K is unramified. Hence Galois $\Rightarrow$ L/K normal + sep'able $\Rightarrow$ L/K Galois.

$\exists$ commutative diagram

NTS that this is iso

$$\begin{tikzcd}
\mathrm{Gal}(L/K) \arrow[r, "\mathrm{res}"] \arrow[d, phantom, "\overset{16.3}{\cong}"] & \mathrm{Gal}(k_L/k) \arrow[d, phantom, "\cong"] \\
\varprojlim_{\substack{F/K \text{ finite} \\ F\subseteq L}} \mathrm{Gal}(F/K) \arrow[dr, "\overset{13.4}{\cong}"] & \varprojlim_{\substack{k'/k \text{ finite} \\ k'\subseteq k_L}} \mathrm{Gal}(k'/k) \\
 & \varprojlim_{\substack{F/K \text{ finite} \\ F\subseteq L}} \mathrm{Gal}(k_F/k) \arrow[u, "\cong"]
\end{tikzcd}$$

13.4 $\left\{ \begin{matrix} F/K \text{ finite} \\ F\subseteq L \end{matrix} \right\} \xleftrightarrow{\text{1-1 bijection}} \left\{ \begin{matrix} k'/k \text{ finite} \\ k'\subseteq k_L \end{matrix} \right\}$

this diagram is commutative so res is an iso. $\blacksquare$

Notation

ex 3

L_1/K, L_2/K finite unram $\Longrightarrow$ L_1L_2/K unram

thus for any L/K, $\exists$ max unram subextension K_0/K.

K_0, L has same residue field. $k_0 = k_L$. k finite but k_L not necessarily finite.

let L/K Galois, $\exists$ surjection res $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K_0/K) \overset{\downarrow}{\cong} \mathrm{Gal}(k_L/k)$

set $I_{L/K} = \ker(\mathrm{res})$ be the inertia subgroup.

let $\mathrm{Fr}_{k_L/k} \in \mathrm{Gal}(k_L/k)$ be the Frobenius $x \mapsto x^{|k|}$

let $\langle \mathrm{Fr}_{k_L/k} \rangle$ be subgroup generated by $\mathrm{Fr}_{k_L/k}$.

def Weil group

let L/K Galois, the weil group $W(L/K) \subseteq \mathrm{Gal}(L/K)$ is $\mathrm{res}^{-1}(\langle \mathrm{Fr}_{k_L/k} \rangle)$

Rmk if k_L/k is finite then $W(L/K) = \mathrm{Gal}(L/K)$. Otherwise $W(L/K) \subsetneq \mathrm{Gal}(L/K)$.

commutative diagram of exact rows

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

def. Topology of $W(L/K)$

Topology of $W(L/K)$ (in this case, subspace topology is not good).

Endow $W(L/K)$ with the weakest topology s.t.

1) $W(L/K)$ is a topological group.
2) $I_{L/K}$ is an open subgroup of $W(L/K)$

$I_{L/K} = \mathrm{Gal}(L/K_0)$ equipped with profinite topology.

i.e. open sets are translations of open sets in $I_{L/K}$ by elements of $W(L/K)$.

warning if k_L/k is infinite, this top is not the subspace top on $W(L/K) \subseteq \mathrm{Gal}(L/K)$.

this one is finer than the subspace top.

i.e. $I_{L/K} \subseteq W(L/K)$ is not open in the subspace top.

Prop 16.8. We don't lose any info going from $\mathrm{Gal}(L/K)$ to $\mathrm{Weil}(L/K)$

let L/K be Galois.

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

ii) If F/K finite subextension of L/K then

$$W(L/F) = W(L/K) \cap \mathrm{Gal}(L/F)$$

$$\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}$$

iii) If F/K finite Galois extension, then

$$\frac{W(L/K)}{W(L/F)} \cong \mathrm{Gal}(F/K)$$

Proof

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

$\Leftrightarrow$ $\forall F/K$ finite Galois sub extension, $W(L/K)$ intersect every coset of $\mathrm{Gal}(L/F)$

$\Leftrightarrow$ $\forall F/K$ finite Galois, $W(L/K) \twoheadrightarrow \mathrm{Gal}(F/K)$???

consider diagram (WTS b is surjective)

$$\begin{array}{ccccccccc} 0 & \to & I_{L/K} & \to & W(L/K) & \to & \langle \mathrm{Fr}_{k_L/k} \rangle & \to & 0 \\ & & \downarrow a & & \downarrow b & & \downarrow c & & \\ 0 & \to & I_{F/K} & \to & \mathrm{Gal}(F/K) & \to & \mathrm{Gal}(k_F/k) & \to & 0 \end{array}$$

let K_0/K be max unramified extension contained in L.

then $K_0 \cap F$ is max unram extension contained in F.

then

$$\begin{tikzcd} Gal(L/K_0) \arrow[r, two heads] \arrow[dr, two heads] & Gal(F/K_0 \cap F) \arrow[d, phantom, "\cong"] \\ & Gal(K_0F/K_0) \end{tikzcd}$$

$\Rightarrow$ a is surjection

$Gal(k_F/k)$ is generated by $Fr_{k_F/k}$ so c is surjection

diagram chase $\Rightarrow$ b is surjection.

Week 7 lec 2

Proof of ii) If F/K finite subextension of L/K then $W(L/F) = W(L/K) \cap Gal(L/F)$

let F/K be finite subextension. consider

$$\begin{tikzcd} Gal(L/K) \arrow[r, two heads] & Gal(k_L/k) \supseteq \langle Fr_{k_L/k} \rangle \\ Gal(L/F) \arrow[r, two heads] \arrow[u, hook] & Gal(k_L/k_F) \supseteq \langle Fr_{k_L/k_F} \rangle \arrow[u, hook] \end{tikzcd}$$

for $\sigma \in Gal(L/F)$,

$\sigma \in W(L/F) \Leftrightarrow \sigma|_{k_L} \in \langle Fr_{k_L/k_F} \rangle$ ($W(L/K) \subseteq Gal(L/K)$ is $res^{-1}(\langle Fr_{k_L/k} \rangle)$)

note $Gal(k_L/k_F) \cap \langle Fr_{k_L/k} \rangle = \langle Fr_{k_L/k_F} \rangle$

$\Leftrightarrow \sigma|_{k_L} \in \langle Fr_{k_L/k} \rangle$

$\Leftrightarrow \sigma \in W(L/K)$

iii) If F/K finite Galois extension, then

$$\frac{W(L/K)}{W(L/F)} \cong Gal(F/K)$$

Proof: $W(L/K)/W(L/F) \overset{(ii)}{=} \dfrac{W(L/K)}{W(L/K) \cap Gal(L/F)}$

Theorem B of isomorphism $\frac{SN}{N} \cong \frac{S}{S \cap N}$

$$\cong \frac{W(L/K)\, Gal(L/F)}{Gal(L/F)}$$

$$\overset{(i)}{=} \frac{Gal(L/K)}{Gal(L/F)} = Gal(F/K) \quad \blacksquare$$

$\boxed{\text{If } B \text{ dense in } A/C \text{ then } BC = A.}$

§ statements of local class field theory

let K be a local field.

def 17.1 Abelian Extension

L/K is Abelian if it's Galois and $Gal(L/K)$ is Abelian.

facts about Abelian extensions

if L_1/K, L_2/K are Abelian then

i) L_1L_2/K is Abelian

ii) if $L_1 \cap L_2 = K$, $\exists$ canonical iso $Gal(L_1L_2/K) \cong Gal(L_1/K) \times Gal(L_2/K)$

fact i) $\Rightarrow$ $\exists$ maximal abelian extension K^{ab} of K inside K^{sep} ← separable closure
← Maximal Galois extension.

def K^{ur}

K^{ur} denote the max unramified extension of K inside K^{sep}. If $|k|=q$

then $K^{ur} = \bigcup_{m=1}^{\infty} K(\zeta_{q^m-1})$. $k_{K^{ur}} = \overline{\mathbb{F}}_q$

and $Gal(K^{ur}/K) \cong Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$

$$\begin{array}{ccc} \psi & & \psi \\ Fr_{k^m/k} & \longleftrightarrow & Fr_{\overline{\mathbb{F}}_q/\mathbb{F}_q} \end{array}$$

so K^{ur} is abelian, $K^{ur} \leq K^{ab}$.

There exists exact sequence:

$$0 \longrightarrow I_{K^{ab}/K} \longrightarrow W(K^{ab}/K) \longrightarrow \underset{\substack{\| \\ Fr\langle K^{ur}/K\rangle}}{\mathbb{Z}} \longrightarrow 0$$

(this exact sequence is a pattern proven earlier)

Thm 17.2

(1) (local Artin Reciprocity) There exists a unique topological isomorphism (group iso, homeo)

$$Art_K : K^\times \xrightarrow{\sim} W(K^{ab}/K)$$

Satisfying the following properties:

i) $Art_K(\pi)\big|_{K^{ur}} = Fr_{K^{ur}/K}$ for any uniformizer $\pi \in K$.

ii) for every finite subextension L/K in K^{ab}/K

$$\mathrm{Art}_K(N_{L/K}(L^\times))|_L = \{1\}. \quad (\text{identity map})$$

2) L/K finite Abelian, Then Art_K induces an iso

$$K^\times / N_{L/K}(L^\times) \cong \frac{W(K^{ab}/K)}{W(K^{ab}/L)} \cong \mathrm{Gal}(L/K)$$

Remarks: (i) special case local langlands

(ii) use it to characterize the global Artin map of global class field theory.

Properties of the Artin map

- (Existence theorem)

For $H \leq K^\times$ open finite index subgroup, $\exists L/K$ finite abelian s.t.

$N_{L/K}(L^\times) = H$

In particular, Art_K induces an inclusion reversing isomorphism of posets:

$$\begin{Bmatrix} \text{open finite index} \\ \text{subgroups of } K^\times \end{Bmatrix} \xleftrightarrow{1-1} \begin{Bmatrix} \text{finite abelian} \\ \text{extensions of } L/K \end{Bmatrix}$$

$$H \longmapsto (K^{ab})^{\mathrm{Art}_K(H)}$$

an element of $W(K^{ab}/K)$ so it's the field fixed by this

norms of $L^\times$ takes place in K so is a subgroup of K.

$$N_{L/K}(L^\times) \longleftarrow L/K$$

(Norm Functoriality) let L/K finite separable extension.

$\exists$ commutative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow[\sim]{\mathrm{Art}_L} & W(L^{ab}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ K^\times & \xrightarrow[\sim]{\mathrm{Art}_K} & W(K^{ab}/K) \end{array}$$

Rest of course: construct Artin map.

Prop 17.3 relationship between $e_{L/K}$ and $N_{L/K}$

let L/K be finite abelian deg n. then $e_{L/K} = [\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$ — see example sheet why

Proof given $x \in L^\times$, we have $v_K(N_{L/K}(x)) = f_{L/K}\, v_L(x)$ (follows since $v_K = e \cdot v_L$)

have surjection

$$K^\times / N_{L/K}(L^\times) \xrightarrow{v_K} \mathbb{Z}/f_{L/K}\mathbb{Z} \quad \text{with kernel} \quad \underbrace{\frac{\mathcal{O}_K^\times\, N_{L/K}(L^\times)}{N_{L/K}(L^\times)}}_{\text{Why is this kernel?}} \overset{3^{rd}\text{ iso thm}}{\cong} \mathcal{O}_K^\times / \mathcal{O}_K^\times \cap N_{L/K}(L^\times) = \mathcal{O}_K^\times / N_{L/K}(\mathcal{O}_L^\times)$$

but then thm 17.2. (2)   by above (size of image x size ker)

$$n = [K^\times : N_{L/K}(L^\times)] = f_{L/K}\,[\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$$

$$\Rightarrow [\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)] = e_{L/K}. \quad \blacksquare$$

Cor 17.4

L/K finite Abelian, then L/K is unramified iff $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$ $\blacksquare$

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

Recall $\mathbb{Q}_p^{un} = \bigcup_{m=1}^\infty \mathbb{Q}_p(\zeta_{p^m-1}) = \bigcup_{p \nmid m} \mathbb{Q}_p(\zeta_m)$

$\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ totally ramified of deg $p^{n-1}(p-1)$ with

$$\theta_n : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times$$

for $n \geq m \geq 1$, $\exists$ diagram

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

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

then $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$ is Galois and have

$$\theta : \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \xrightarrow{\sim} \varprojlim_{n \geq 1} (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$$

we have $\underset{\text{totally ram}}{\mathbb{Q}_p(\zeta_{p^\infty})} \cap \underset{\text{unram}}{\mathbb{Q}_p^{un}} = \mathbb{Q}_p$ so it must be trivial extension.

By property of Galois extensions,

get iso $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty}) \cdot \mathbb{Q}_p^{un}/\mathbb{Q}_p) \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$

Thm 17.5 (local- Kronecker - Weber)

$$\mathbb{Q}_p^{ab} = \underbrace{\mathbb{Q}_p^{ur}\ \mathbb{Q}_p(\zeta_{p^\infty})}_{\text{compositum}}$$

Proof omitted.

Construct $\mathrm{Art}_{\mathbb{Q}_p}$ as follows:

we have $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$

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

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

$$\in \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$$

$$\cong \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$$

Image lies in $W(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$

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

Week 7 lecture 3

§ Construction of Art K

let K be local field. π a uniformizer of K.

For $n \geq 1$, construct $K_{\pi,n}$ totally ramified Galois extension s.t.

i) $K \subseteq \cdots \subseteq K_{\pi,n} \subseteq K_{\pi,n+1} \subseteq \cdots$

ii) for $n \geq m \geq 1$, $\exists$ commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(K_{\pi,n}/K) & \twoheadrightarrow & \mathrm{Gal}(K_{\pi,m}/K) \\ \psi_n \downarrow \wr & & \wr\downarrow \psi_m \\ \mathcal{O}_K^\times / U_K^{(n)} & \xrightarrow{\text{res}} & \mathcal{O}_K^\times / U_K^{(m)} \\ \| & & \| \\ (1+\pi^n \mathcal{O}_K, \times) & & (1+\pi^m \mathcal{O}_K, \times) \end{array}$$

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

then ii) $\Rightarrow \exists$ iso (ex sheet 4)

$$\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \xrightarrow{\sim} \varprojlim_n \mathcal{O}_K / U_K^{(n)} \cong \mathcal{O}_K^\times$$

We define the Artin map Art_K by

$$\begin{array}{ccccc} K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times & \longrightarrow & \mathrm{Gal}(K^{un}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) & \overset{(iii)}{\hookrightarrow} & \mathrm{Gal}(K^{ab}/K) \\ \pi^n u \leftarrow (n, u) & \longmapsto & ((\mathrm{Fr}_{K^{un}/K})^n, \psi^{-1}(u)) & & \end{array}$$

so image lies in $W(K^{ab}/K)$

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

Both $K_{\pi,\infty}$ and the iso $K^\times = \mathbb{Z} \times \mathcal{O}_K^\times$ depend on π. For different choice of π, the maps defined agree. So Art_K is canonical.

For rest of course, construct $K_{\pi,n}$.

VII Lubin-Tate Theory

§ Formal group laws

let R be a ring.

$R[[X_1, \cdots, X_n]] = \{ \sum a_{k_1, \cdots k_n} X^{k_1} \cdots X^{k_n}, \ k_1, \cdots, k_n \in \mathbb{Z}_{\geq 0}, \ a_{k_1 \cdots k_n} \in R \}$

def 18.1 1-dim formal group law. (power series behave like Lie group)

A (1-dim, formal) group law over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying:

i) $F(X,Y) \equiv X+Y \pmod{\deg 2}$ [ignoring terms of deg 2]

ii) $F(X, F(Y,Z)) = F(F(X,Y), Z)$ (associativity)

iii) $F(X,Y) = F(Y,X)$ (commutativity)

Eg. $\hat{G}_a[X;Y] = X+Y$ formal additive gp

$\hat{G}_m[X;Y] = X+Y+XY$ formal multiplication gp

$F(X, F(Y,Z)) = F(X, Y+Z+YZ)$

$= X+Y+Z+YZ+XY+XZ+XYZ$

Lemma 18.2. Properties of formal group law

Let F be a formal group law over R.

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

ii) $\exists$ a unique $i(X) \in X R[\![X]\!]$ s.t.

$$F(X, i(X)) = 0$$

Proof. Example sheet 4.

Prop. Formal group law convergence

Let K be a complete non-arch valued field. F a formal group law over $\mathcal{O}_K$.

Then $F(x,y)$ converge $\forall x,y \in m_K$ to an element in m_K. (m_K is the residue field of K).

Why converge?

def. $(m_K, \cdot_F)$ as a group

define $x \cdot_F y = F(x,y)$, this turns $(m_K, \cdot_F)$ into a commutative group.

E.g. $\hat{G}_m / \mathbb{Z}_p$, $x \cdot_{\hat{G}_m} y = x+y+xy$ $(x,y \in p\mathbb{Z}_p)$

$$(p\mathbb{Z}_p, \cdot_{\hat{G}_m}) \cong (1+p\mathbb{Z}_p, \times)$$

$$x \mapsto 1+x$$

def 18.3 homomorphism and isomorphism of formal group laws

Let F, G be formal group laws over R. A homomorphism $f: F \to G$ is an element $f(X) \in X R[\![X]\!]$ s.t.

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

A homomorphism $f: F \to G$ is an isomorphism if $\exists g: G \to F$, s.t. $f g(X) = X$, $g f(X) = X$

define $\mathrm{End}_R(F)$ to be set of homs $f: F \to F$.

Prop 18.4 exp is an iso of formal gp laws

Let R be a $\mathbb{Q}$-algebra. Then there's an iso of formal group laws

$$\exp: \hat{G}_a \xrightarrow{\sim} \hat{G}_m$$

$$\exp(X) = \sum_{n=1}^{\infty} \frac{X^n}{n!}$$

verification process

$\log(\exp(X))$

$= \log\left(\sum_{n=1}^{\infty} \frac{X^n}{n!}\right)$

$= \underbrace{\sum_{m=1}^{\infty} (-1)^{m-1} \frac{\left(\sum_{n=1}^{\infty} \frac{X^n}{n!}\right)^m}{m!}}$

power $X^1 : X$

power X^k ?

Proof define $\log(X) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{X^n}{n!}$

then $\exists$ equality of formal power series

$$\begin{cases} \log(\exp(X)) = \exp(\log(X)) = X \\ \exp(\hat{G}_a(X,Y)) = \hat{G}_m(\exp(X), \exp(Y)) \end{cases}$$

How to verify this?

Lemma 18.5

in general, non commutative

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

Proof show well defined. (i.e. $f +_F g$, $f \circ g \in \mathrm{End}_K(F)$)

let $f, g \in \mathrm{End}_R(F)$.

$(f +_F g) \circ F(X,Y) = F(f(F(X,Y)), g(F(X,Y)))$

defn of f as homomorphism

$= F(F(f(x), f(y)), F(g(x), g(y)))$

ASSOC + comm

$= F(F(f(x), g(x)), F(f(y), g(y)))$

$= F(f +_F g(x), f +_F g(y))$

$\Rightarrow f +_F g \in \mathrm{End}_K(F)$

$f \circ g \circ F = f \circ F \circ g = F \circ f \circ g$ so $f \circ g \in \mathrm{End}_R(F)$

to check ring axioms is an exercise

§ Lubin Tate formal group

K local field. $|k| = q$.

defn 19.1 Formal $\mathcal{O}_K$-module

A formal $\mathcal{O}_K$ module of $\mathcal{O}_K$ is a formal group law $F(X,Y) \in \mathcal{O}_K[[X,Y]]$

together with a ring hom

$[\ ]_F : \mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_K}(F)$ s.t. $\forall a \in \mathcal{O}_K$, $[a]_F(X) \equiv aX \mod X^2$.

def. hom / iso of formal O_K modules.

A hom/iso $f: F \to G$ of formal O_K modules is a hom/iso of formal group laws s.t. $f \circ [a]_F = [a]_G \circ f$ $\forall a \in O_K$.

def. Lubin - Tate Series

let $\pi \in O_K$ be a uniformizer. Then a Lubin - Tate series for π is a power series $f(x) \in O_K[[x]]$ s.t.

a) $f(x) \equiv \pi x \mod x^2$

b) $f(x) \equiv x^q \mod (\pi)$

E.g. if $K = \mathbb{Q}_p$, $f(x) = (x+1)^p - 1$ is a lubin tate series for p.

Week 8 lec 1

K local field, π uniformizer, $|K| = q$.

Thm 193 (Big theorem, to be proven later)

let $f(x)$ be a lubin - Tate series for π.

Then, there are three properties for $f(x)$.

i) $\exists$ a unique formal group law F_f over O_K s.t. $f \in \mathrm{End}_{O_K}(F_f)$

ii) $\exists$ a ring hom

$[\ ]_f : O_K \to \mathrm{End}_{O_K}(F_f)$ which implies F_f is a formal O_K module over O_K.

iii) If $g(x)$ is another formal Lubin-Tate series for π, then $F_f \cong F_g$ as formal O_K modules.

(Proof is shown later in this lecture)

- Think of End as where you can make $F(f(x), f(y)) = f(F(x,y))$ commute
- Formal O_K module: give an element in O_K, spit out a $f \in O_K[[x]]$ that commutes with F_f.

def. The Lubin Tate formal gp law

Given π, then F_f is the unique Lubin Tate formal group law for π.

(only depends on π up to iso)

Example for Lubin Tate Formal group

$K=\mathbb{Q}_p$, $f(x)=(x+1)^p-1$. This is a Lubin-Tate series. The Lubin Tate formal group F_f is $\hat{G}_m$.

Suffice to show $f\circ \hat{G}_m = \hat{G}_m \circ f$

$$f\circ \hat{G}_m(x,y) = f(x+y+xy) = (x+y+xy+1)^p-1 = (x+1)^p(y+1)^p-1$$

$$\hat{G}_m\circ(f(x),f(y)) = G_m\left[(x+1)^p-1,\ (y+1)^p-1\right) = (x+1)^p-1+(y+1)^p-1+\left((x+1)^p-1\right)\left((y+1)^p-1\right)$$

$$= \cancel{(x+1)^p} + \cancel{(y+1)^p}-2+(x+1)^p(y+1)^p - \cancel{(y+1)^p} - \cancel{(x+1)^p}+1$$

$$= (x+1)^p(y+1)^p-1$$

Lemma 19.4 (Key lemma to prove 19.3)

let $f(x)$, $g(x)$ be Lubin Tate series for π. let $L(x_1,\cdots,x_n)=\sum_{i=1}^n a_i x_i$, $a_i\in\mathcal{O}_K$

then $\exists$ a unique power series $F(x_1,\cdots,x_n)\in\mathcal{O}_K[\![x_1,\cdots,x_n]\!]$ s.t

i) $F(x_1,\cdots x_n)\equiv L(x_1,\cdots x_n)$ mod degree 2. i.e. L be any $\mathcal{O}_K$ lin. comb of x_i.

ii) $f(F(x_1,\cdots,x_n)=F(g(x_1),g(x_2),\cdots g(x_n))$. Then exists $F\equiv L$ mod deg 2 s.t. F commutes, i.e. $f\circ F=F\circ g$

Proof: (idea: approximate power series by polynomials)

we will show by induction that $\exists F_m\in\mathcal{O}_K[x_1,\cdots x_n]$ of total degree $\le m$, s.t.

a) $f(F_m(x_1,\cdots x_n))\equiv F_m(g(x_1),g(x_2),\cdots g(x_n))$ mod deg $m+1$

b) $F_m(x_1,\cdots x_n)\equiv L(x_1,\cdots x_n)$ mod deg 2.

c) $F_m\equiv F_{m+1}$ mod deg $m+1$

So we proceed by induction.

For $m=1$, take $F_1=L$ (b) is automatically satisfied ✓

to check a), $f(F_1(x_1,\cdots,x_n)\equiv \pi F_1(x_1,\cdots x_n)$ mod deg 2

$f(x)\equiv\pi x$ mod deg 2
f is L-T

$\equiv \pi L(x_1,\cdots x_n) \equiv \pi\sum a_i x_i = \sum a_i(\pi x_i)$

Because g is also Lubin Tate
$g(x)\equiv\pi x$ (mod deg 2)

$\equiv F_1(g(x_1),\cdots g(x_n))$ mod deg 2. so a) is satisfied.

Now, inductive step. Suppose F_m constructed for $m \geq 1$

Set $F_{m+1} = F_m + h$, $h \in \mathcal{O}_K[x_1, \cdots x_n]$, homogenous of degree $m+1$. h is a polynomial whose value is TBD.

Then. Since $f(x+y) = f(x) + f'(x)y + y^2(\cdots)$ Showed up in Hensel's lemma

and $f'(\pi) \equiv \pi \mod x$

these two properties combine

$f \circ (F_m + h) = f(F_m) + f'(F_m) \cdot h + h^2(\cdots)$

$\equiv f \circ F_m + \pi h \mod \deg m+2$ I don't see why $f'(F_m) = \pi$?

$g(x) \equiv \pi x \mod x^2$

Similarly, $(F_m + h) \circ g \equiv F_m \circ g + h(\pi x_1, \cdots \pi x_n) \mod \deg m+2$

$\equiv F_m \circ g + \pi^{m+1} h(x_1, \cdots x_n) \mod \deg m+2$

Thus (a) + (b) + (c) are satisfied iff

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

Why? c) is automatically satisfied by construction of h. b) is always satisfied b/c add things $> \deg 2$. just need a) left.

for a), note that a) is true iff $f \circ (F_m + h) - (F_m + h) \circ g \equiv 0 (\mod \deg m+2)$

we know $f \circ (F_m + h) - (F_m + h) g \equiv \underbrace{f \circ F_m - F_m \circ g - (\pi - \pi^{m+1}) h \mod \deg m+2}_{\text{WTS this is 0 mod deg m+2}}$

2^{nd} property of Lubin Tate is useful now.

note that $f(x) \equiv g(x) \equiv x^q \mod \pi$.

So that $f \circ F_m - F_m \circ g \equiv F_m(x_1, \cdots, x_n)^q - F_m(x_1^q, \cdots x_n^q) \mod \pi$.

polynomial is a homomorphism in modulo π

$\equiv 0 \mod \pi$???

Thus that $f \circ F_m - F_m \circ g \in \pi \mathcal{O}_K[x_1, \cdots x_n]$.

let $r(x_1, \cdots x_n)$ be deg $m+1$ terms in $f \circ F_m - F_m \circ g$.

then set $h := \frac{1}{\pi(1-\pi^m)} r \in \mathcal{O}_K[x_1, \cdots x_n]$ (i.e. $\boxed{f \circ F_m - F_m \circ g \equiv (\pi - \pi^{m+1}) h \mod \deg m+2}$)

So that F_{m+1} satisfies (a) + (b) + (c)

This is unique since h is determined by property a).

Set $F = \lim_{m} F_m \in \mathcal{O}_K[[x_1, \cdots x_n]]$ by (i). Then $F(x_1, \cdots, x_n)$ satisfies (i) and (ii).

The the uniqueness of F follows from uniqueness of F_m.

∎

Proof of thm 19.3

we'll prove i), ii), iii) in order.

proven for $x_1, \cdots, x_n$ but use it for just x, y and $f=g$

i) By lemma 19.4, There exists a unique $F_f(X, Y) \in \mathcal{O}_K[[X, Y]]$ s.t.

- $F_f(X, Y) \equiv X+Y \mod \deg 2$
- $f(F_f(X, Y)) = F_f(f(X), f(Y))$

Now, WTS that F_f is a formal group law and f is in $\mathrm{End}_{\mathcal{O}_K}(F_f)$

$f \in \mathrm{End}_{\mathcal{O}_K}(F_f)$ is given by this

Associativity:

$$F_f(X, F_f(Y, Z)) \equiv X+Y+Z \mod \deg 2$$
$$\equiv F_f(F_f(X, Y), Z) \mod \deg 2.$$

and that
$$f \circ F_f(X, F_f(Y, Z))$$
$$= F_f(f(X), f(F_f(Y, Z)))$$
$$= F_f(f(X), F_f(f(Y), f(Z)))$$

Similarly,
$$f \circ F_f(F_f(X, Y), Z)$$
$$= F_f(f \circ F_f(X, Y), f(Z))$$
$$= F_f(F_f(f(X), f(Y)), f(Z))$$

By uniqueness in lemma 19.4, F_f satisfy i) and ii) in lemma, such F_f is unique so we must get associativity.

Commutativity (Similar method, fill in!)

F_f is again unique as the uniqueness in lemma 19.4.

$F(X, 0) = X$ and $F(0, Y) = Y$ by uniqueness.

ii) F_f is a formal $\mathcal{O}_K$-module.

By lemma 19.4, for $a \in \mathcal{O}_K$, using lemma for 1 var instead of n or 2.

$\exists!\ [a]_{F_f} \in \mathcal{O}_K[[X]]$ s.t.

$$\begin{cases} [a]_{F_f} \equiv aX \mod X^2 \\ f \circ [a]_{F_f} = [a]_{F_f} \circ f \end{cases}$$

Then $[a]_{F_f} \circ F_f \equiv aX + bY \equiv F_f \circ [a]_{F_f}$ mod deg 2.

and that $\begin{cases} f \circ [a]_{F_f} \circ F_f = [a]_{F_f} \circ f \circ F_f = [a]_{F_f} \circ F_f \circ f \\ f \circ F_f \circ [a]_{F_f} = F_f \circ f \circ [a]_{F_f} = F_f \circ [a]_{F_f} \circ f \end{cases}$ } not sure this step.

So $[a]_{F_f} \circ F_f = F_f \circ [a]_{F_f}$. Therefore $[a]_{F_f} \in \mathrm{End}_{\mathcal{O}_K}(F_f)$.

↳ The map $[\ ]_{F_f} : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F_f)$ is a ring hom by uniqueness.

↳ F_f is a formal $\mathcal{O}_K$-module.

↳ $[\pi]_{F_f} = f$ by uniqueness.

iii) WTS if g is another L.T. series, then the two F_f gives iso of formal $\mathcal{O}_K$ modules.

let $g(x)$ be another L.T. series for π.

let $\theta(x) \in \mathcal{O}_K[[x]]$ be unique power series s.t. $\theta(x) \equiv X$ mod X^2 and $\theta \circ f = g \circ \theta$

then by uniqueness, $\theta \circ F_f = F_g(\theta(X), \theta(Y))$ (uniqueness) ?

$\Rightarrow \theta \in \mathrm{Hom}(F_f, F_g)$

reversing roles of $f, g \longrightarrow$ obtain $\theta^{-1}(x) \in \mathcal{O}_K[[x]]$, s.t. $\theta^{-1} \in \mathrm{Hom}_{\mathcal{O}_K}(F_g, F_f)$.

then $\theta^{-1} \circ \theta = X$ and $\theta \circ \theta^{-1}(X) = X$ (uniqueness) $\Rightarrow \theta$ is an iso.

(uniqueness) $\Rightarrow \theta \circ [a]_{F_f}(X) = [a]_{F_g} \circ \theta(X)$ $\forall a \in \mathcal{O}_K$. and hence θ is an isomorphism of formal $\mathcal{O}_K$ module. ∎

<u>Week 8 lec 2</u>

§ Lubin - Tate extensions

K a non-arch local field. $|k| = q$. π is a unif.

$\bar{K}$ alg closure of K and $\bar{m} \subseteq \mathcal{O}_{\bar{K}}$ the max ideal. alg clo of local is local ?

<u>lemma 20.1 $\bar{m}$ as an $\mathcal{O}_K$-module</u>

F a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. Then, $\bar{m}$ is an (genuine) $\mathcal{O}_K$ module with

$$x +_F y = F(x,y), \quad x, y \in \bar{m}$$

$$a_F\, x = \underbrace{[a]_F}_{\mathrm{End}_{\mathcal{O}_K} F,\ \text{power series in 1 variable}}(x), \quad x \in \bar{m},\ a \in \mathcal{O}_K$$

} these power series are evaluated.

Proof: Note that $\bar{K}$ is not complete. (did we prove this?)

$x \in \bar{m} \Rightarrow x \in m_L$ for some L s.t. L/K is finite.

Show $[a]_f(x) \in \bar{m}$:

$[a]_f \in \mathcal{O}_K[[x]]$. $\Rightarrow$ $[a]_f(x)$ converges in L. Since m_L is closed, $[a]_F(x) \in m_L \subseteq \bar{m}$.

Show $x +_F y \in \bar{m}$:

$x +_F y = F(x,y)$. $x, y \in m_L$. $F(x,y)$ converge in L. m_L closed so $F(x,y) \in m_L \in \bar{m}$.

The module structure follows from definition.

def. The π^n torsion group

$f(x)$ Lubin-Tate Series. F_f Lubin Tate formal group law.

The π^n- torsion group is

$\mathcal{U}_{f,n} := \{x \in \bar{m} \mid \pi^n \cdot_{F_f} x = 0\}$ remember: $x \cdot_{F_f} y = F(x,y)$

why are they equivalent? $= \{x \in \bar{m} \mid f_n(x) = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}(x) = 0\}$

why these two series equivalent?

$F_f(\pi^n, x)$ $F(f(\pi), f(x)) = f(F(\pi, x))$

Facts: • $\mathcal{U}_{f,n}$ is an $\mathcal{O}_K$-module

$x, y \in \mathcal{U}_{f,n}$, $x +_F y = F(x,y)$ $F(\pi^n, F(x,y))$
$= F(F(\pi^n, x), y)$?
$= F(0, y) = 0$

• $\mathcal{U}_{f,n} \subseteq \mathcal{U}_{f,n+1}$

Example for Torsion group

• $K = \mathbb{Q}_p$, $f(x) = (x+1)^p - 1$ is a Lubin-Tate series.

$[p^n]_{F_f}(x) = f \circ f \circ \cdots \circ f = (x+1)^{p^n} - 1$.

this equality I dont get

with $[p^n]_{F_f}(x) = \pi^n \cdot_{F_f}(x) = f_n(x)$

$\mathcal{O}_K$-module scalar mult, I dont get above

• Thus $\mathcal{U}_{f,n} = \{\xi_{p^n}^i - 1 \mid i = 0, 1, \cdots p^n - 1\}$.

now let $f(x) = \pi x + x^q$ - Lubin-Tate Series for π.

then $f_n(x) = f \circ f_{n-1}(x) = f(f_{n-1}(x))$

$= \pi f_{n-1}(x) + (f_{n-1}(x))^q = f_{n-1}(x)(\pi + f_{n-1}(x)^{q-1})$

Set $h_n(x) := \dfrac{f_n(x)}{f_{n-1}(x)} = \pi + f_{n-1}(x)^{q-1}$ by convention $f_0(x) = x$.

def $f(x)$, $f_n(x)$, $h_n(x)$ in this context

Prop 20.3. $h_n(x)$ is a separable Eisenstein poly of degree $q^{n-1}(q-1)$

Proof :

It's clear $h_n(x)$ is monic of degree $q^{n-1}(q-1)$.

$f(x) \equiv x^q \bmod \pi \Rightarrow f_{n-1}(x)^{q-1} \equiv (x^{q^{n-1}})^{q-1} = x^{(q^{n-1})(q-1)} \bmod \pi$

Since f_{n-1} has no constant terms, $h_n = \pi + f_{n-1}(x)^{q-1}$ has constant term π. So h_n is Eisenstein.

Since $h_n(x)$ is irreducible, $h_n(x)$ is separable in two situations

$\begin{cases} \text{either} & \text{char } K = 0 \\ \text{or} & \text{char } K = p \text{ and } h_n'(x) \neq 0. \end{cases}$

assume char $K = p$. induct on n.

$h_1(x) = \pi + x^{q-1}$ is separable.

suppose $h_{n-1}(x), \cdots, h_1(x)$ are separable.

then $f_{n-1}(x) = h_{n-1}(x) \cdots h(x)$ is separable. (as it's a prod of separable irred-poly of diff degrees)

$h_n(x) = \pi + f_{n-1}(x)^{q-1}$

$h_n'(x) = \underset{\neq 0}{(q-1)} \underset{\neq 0}{(f_{n-1}(x))^{q-2}} \cdot \underset{\neq 0}{f_{n-1}'(x)}$ as f_{n-1} is separable.

so $h_n(x)$ is separable.

Proof scheme: (fill later).

Prop 20.4 $\mu_{f,n}$'s module structure and iso of $\mathcal{O}_K$-modules.

i) $\mu_{f,n}$ is a free module of rank 1 over $\mathcal{O}_K/\pi^n\mathcal{O}_K$

ii) if g is another Lubin-Tate series for π, then $\mu_{f,n} \cong \mu_{g,n}$ as $\mathcal{O}_K$-modules and $K(\mu_{f,n}) = K(\mu_{g,n})$

Proof:

i) let $\alpha \in K$ be a root of $h_n(x)$. Since $h_n(x)$, $f_{n-1}(x)$ is coprime,

we have $\alpha \in \mu_{f,n} \setminus \mu_{f,n-1}$. $\leftarrow$ α not a root of $f_{n-1}(x)$.

since $f_n(x) = h_n(x) f_{n-1}(x)$

Then the map

$$\tilde{\varphi} : \mathcal{O}_K \longrightarrow \mathcal{U}_{f,n}$$
$$a \longmapsto a_{F_f}\alpha$$

is an $\mathcal{O}_K$ module homomorphism with $\pi^n \mathcal{O}_K \subseteq \ker \tilde{\varphi}$ since $\alpha \in \mathcal{U}_{f,n}$.

as $\pi^n \cdot \alpha = 0$ $\left(\mathcal{U}_{f,n} = \{\alpha \in \bar{m} \mid \pi^n \cdot_{F_f} \alpha = 0\} \right)$

(furthermore, as $\alpha \in \mathcal{U}_{f,n} / \mathcal{U}_{f,n-1}$, $\pi^{n-1} \cdot_{F_f} \alpha \neq 0 \Rightarrow \pi^n \mathcal{O}_K = \ker \tilde{\varphi}$.)

Thus $\tilde{\varphi}$ induces an injection:

$$\varphi : \mathcal{O}_K / \pi^n \mathcal{O}_K \longrightarrow \mathcal{U}_{f,n}.$$

Since $f_n(x)$ is separable,

$$|\mathcal{U}_{f,n}| = \deg f_n(x) = q^n = (\mathcal{O}_K / \pi^n \mathcal{O}_K)$$

So φ is an isomorphism by counting.

Proof scheme: (fill later).

ii) let $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(F_f, F_g)$ isomorphism of formal $\mathcal{O}_K$- modules.

then θ induces a isomorphism $\theta : (\bar{m}, +_{F_f}, \cdot_{F_g}) \xrightarrow{\sim} (\bar{m}, +_{F_g}, \cdot_{F_g})$???

(lemma 20.1) $\Rightarrow$ $\mathcal{U}_{f,n} \cong \mathcal{U}_{g,n}$. ???

Since $\mathcal{U}_{f,n}$ is algebraic, $K(\mathcal{U}_{f,n})/K$ is finite and complete.

Since that $\theta(x) \in \mathcal{O}_K[[x]]$, for $x \in \mathcal{U}_{f,n}$, $\theta(x) \in K(\mathcal{U}_{f,n})$. ??? $\theta(x) \in K(\mathcal{U}_{g,n})$?

So $K(\mathcal{U}_{g,n}) \subseteq K(\mathcal{U}_{f,n})$

Same argument for θ^{-1} gives $K(\mathcal{U}_{f,n}) \subseteq K(\mathcal{U}_{g,n})$

$\Rightarrow$ $K(\mathcal{U}_{g,n}) = K(\mathcal{U}_{f,n})$ ∎

def. Lubin - Tate extensions

$K_{\pi,n} := K(\mathcal{U}_{f,n})$. $K_{\pi,n}$ are called Lubin - Tate extensions.

Remark 1) $K_{\pi,n}$ doesn't depend on f by prop 20.4.

2) $K_{\pi,n} \subseteq K_{\pi,n+1}$

Prop 20.6 $K_{\pi,n}$ are totally ramified and Galois extension of degree $q^{n-1}(q-1)$

Proof: We may choose $f(x) = \pi x + x^q$.

$K_{\pi,n}/K$ is Galois since $K_{\pi,n} = K(\mu_{f,n})$. $K_{\pi,n}/K$ Galois since $K_{\pi,n} = K(\mu_{\pi,n})$ is splitting field of $f_n(x)$.

let α be a root of $h_n = \frac{f_n(x)}{f_{n-1}(x)}$

Suffice to show $K(\alpha) = K(\mu_{f,n})$. since α is a root of Eisenstein poly of deg $q^{n-1}(q-1)$

"$\subseteq$" Clear.

($\mu_{f,n}$ is a rank 1 free mod over $\mathcal{O}_K/\pi^n\mathcal{O}_K$)

"$\supseteq$" By proposition, every element $x \in \mu_{f,n}$ is a form of $a \cdot_{F_f} \alpha$ for some $a \in \mathcal{O}_K$. (as $\alpha \in (\mu_{f,n} \setminus \mu_{f,n-1})$)

$K(\alpha)$ is complete, and $[a]_{F_f}(x) \in \mathcal{O}_K[[x]]$

$\Rightarrow$ $x = [a]_{F_f}(\alpha) \in K(\alpha)$

$\Rightarrow$ $K(\alpha) \supseteq K(\mu_{f,n})$

Proof scheme: (fill later).

Week 8 lec 3

K a local field. $|k| = q$, π a unif. f- Lubin-Tate series $\pi x + x^q$.

thm 20.7 Isomorphism between Lubin-Tate extension and quotients

There are isomorphisms

$$\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\simeq} \left(\mathcal{O}_K/\pi^n\mathcal{O}_K\right)^\times$$

determined by

$$(*) \quad \psi_n(\sigma) \cdot_{F_f} x = \sigma(x), \ \forall x \in \mu_{f,n}, \ \sigma \in \mathrm{Gal}(K_{\pi,n}/K).$$

ψ_n does not depend on f.

Proof:

let $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$

then σ preserves $\mu_{f,n}$ torsion and act continuously on $K(\mu_{f,n}) = K_{\pi,n}$.

Since $F_f(X,Y) \in \mathcal{O}_K[[X,Y]]$, and, $[a]_{F_f} \in \mathcal{O}_K[[X]]$. for all $a \in \mathcal{O}_K$, we have continuity for σ.

Continuity for σ $\Rightarrow$ $\begin{cases} \sigma(x \cdot_{F_f} y) = \sigma(x) +_{F_f} \sigma(y) & \forall x,y \in \mu_{f,n} \\ \sigma(a \cdot_{F_f} x) = a_{F_f}\, \sigma(x) & \forall x \in \mu_{f,n},\ a \in \mathcal{O}_K \end{cases}$

Thus $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n}) \longleftarrow$ Aut as an $\mathcal{O}_K$-module.

This indues a group homomorphism

$$\mathrm{Gal}(K_{\pi,n}/K) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,n})$$

this is injective since $K_{\pi,n} = K(\mu_{f,n})$. $\boxed{\text{Why injective ?}}$

Since $\pi_{f,n} \cong \mathcal{O}_K/\pi^n$ as an $\mathcal{O}_K$ module.

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

(this is because $\mathrm{Aut}_R(M) = R^\times$ for M free rank 1 module over R)

??

Obtain $\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \hookrightarrow (\mathcal{O}_K/\pi^n)^\times$ defined by

$\psi_n(\sigma) \in (\mathcal{O}_K/\pi)^\times$ be unique element s.t.

$\psi_n(\sigma) \cdot_{F_f} x = \sigma(x) \quad \forall x \in \mu_{f,n}$.

$[K_{\pi,n} : K] = q^{n-1}(q-1) = |(\mathcal{O}_K/\pi^n)^\times| \Rightarrow \psi_n$ Surjective by counting.

Now, let g be another Lubin-Tate series, we obtain

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

let $\theta : F_f \to F_g$ be iso of formal $\mathcal{O}_K$-modules (prop 19.2 $\Rightarrow$ this) thus indues isomorphism

$\theta : \mu_{f,n} \xrightarrow{\sim} \mu_{g,n}$ of $\mathcal{O}_K$-modules.

here for $x \in \mu_{f,n}$, $\theta(\psi_n(\sigma) \cdot_{F_f} x) = \psi_n(\sigma) \cdot_{F_g} \theta(x)$

But $\theta \in \mathcal{O}_K[[x]]$ has coefficient in $\mathcal{O}_K$,

$\Rightarrow \theta(\sigma(x)) = \sigma(\theta(x))$ (continuity) $\forall x \in \mu_{f,n}$

$\Rightarrow \theta(\psi_n(\sigma) \cdot_{F_f} x) = \theta(\sigma(x)) = \sigma(\theta(x)) = \psi_n'(\sigma) \cdot_{F_g} \theta(x)$

$\Rightarrow \psi_n(\sigma) = \psi_n'(\sigma)$ ▨

Proof scheme: (fill later).

★ unfamiliar w/ this proof.

def $K_{\pi,\infty}$

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

$$\underbrace{\psi: \mathrm{Gal}(K_{\pi,\infty}/K)}_{\text{does not depend on the choice of Lubin Tate anymore}} \cong \varprojlim_n (\mathcal{O}_K/\pi^n)^\times \cong \mathcal{O}_K^\times$$

Thm (Generalized Kronecker - Weber)

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

pf: omit

Construction of the Artin map

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

Art_K is defined by:

$$K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times \longrightarrow \mathrm{Gal}(K^{ur}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{ab}/K)$$

$$\pi^n u \leftarrow (n,u) \longrightarrow \left(\mathrm{Fr}^n_{K^{ur}/K},\ \psi^{-1}(u)\right)$$

the image of Art_K lands in $W(K^{ab}/K)$, so $\mathrm{Art}_K: K^\times \xrightarrow{\cong} W(K^{ab}/K)$

image of Art_K equal to $W(K^{ab}/K)$

Remark: independent of choice of π.

End of Examinable Materials.

Local fields summary (important theorems)

- lemma: 4 equivalent conditions for v discrete:
  - ↳ v is discrete
  - ↳ $\mathcal{O}_K$ PID
  - ↳ $\mathcal{O}_K$ Noetherian
  - ↳ m is principal
- lemma: field to DVR, and DVR to field to $\mathcal{O}_K$.
- Prop: $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n \mathcal{O}_K$, every $x \in \mathcal{O}_K$ written uniquely as $\sum_{i=0}^{\infty} a_i \pi^i$, $a_i \in \mathcal{O}_K/\pi\mathcal{O}_K$.
- Thm: Hensel's lemma
- Thm: lifting root version of Hensel's lemma.
- Thm: Teichmuller lift thm.
- Thm: L/K finite then $|\cdot|$ extends uniquely to absolute values on L.

  $|\cdot|_L : L \to K$ $\quad |y|_L = |N_{L/K}(y)|^{1/n}$. L is complete w.r.t. $|\cdot|_L$.
- lem: $\mathcal{O}_K^{\text{int}(L)} = \mathcal{O}_L$
- Prop: $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n$ is iso
- Prop: finite extension of local field is local
- Thm: Ostrowski's theorem: Any nontrivial abs val on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or p-adic abs val for some p.
- Summary of classification of local fields: any LF is isomorphic to
  1) $\mathbb{R}, \mathbb{C}$ (Arch)
  2) $\mathbb{F}_{p^m}((t))$ (Non-arch, = char)
  2) finite ext of $\mathbb{Q}_p$ (non-arch, mixed char)
- Prop. Nearby polynomials define same extensions
- thm. Local fields are completion of global fields.
- Thm: DVR $\Leftrightarrow$ DDK dom w/ 1 prime ideal

  DDK localised is DVR
- Lem: integral closure of DDK is DDK.

- $\mathcal{O}_K$ DDK, $(x) = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_\mathfrak{p}(x)}$
- The absolute values of L extending $|\cdot|_\mathfrak{p}$ is $|\cdot|_\mathfrak{P}$ where $\mathfrak{P}$ lie over $\mathfrak{p}$.
- lem: $L \otimes_K K_\mathfrak{p} \twoheadrightarrow L_\mathfrak{P}$ is surjective

  $(l, k) \mapsto lk$
- Thm: $L \otimes_K K_\mathfrak{p} \to \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$ is an iso
- cor: $x \in L$, $N_{L/K}(x) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(x)$
- Thm: $D_{L/K} = \prod_{\mathfrak{P}} D_{L_\mathfrak{P}/K_\mathfrak{p}}$
- Cor: $d_{L/K} = \prod_{\mathfrak{P}} d_{L_\mathfrak{P}/K_\mathfrak{p}}$.
- Thm: $\sum_{i=1}^{r} e_i f_i = [L:K]$
- Prop: $\mathrm{Gal}(L/K)$ acts on $\mathfrak{P}_i$ transitively
- Thm: $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ prime.

  If $\mathfrak{p}$ ramifies in L, $\forall x_1, \cdots x_n \in L$, $\mathfrak{p} \mid \Delta(x_1, \cdots, x_n)$

  If $\mathfrak{p}$ is unram in L, $\forall x_1, \cdots x_n \in L$, $\mathfrak{p} \nmid \Delta(x_1, \cdots, x_n)$
- Thm: $N_{L/K}(D_{L/K}) = d_{L/K}$
- Thm: finite separable extensions of local fields split into unram and totally ram.
- Thm: 3 properties about higher ramification groups:

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

  ii) $\bigcap_{s=0}^{\infty} G_s = \{1\}$

  iii) $s \in \mathbb{Z}_{\geq 0}$, $\exists$ injective group hom $G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$
- Cor. Galois ext of local fields is solvable and G_s/G_{s+1} has formulas.
- cor. L/K ext of number fields, $\mathfrak{P} \in \mathcal{O}_L$, $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, $e(\mathfrak{P}/\mathfrak{p}) > 1 \Leftrightarrow$ iff $\mathfrak{P} \mid D_{L/K}$
- <u>infinite Galois Theory</u> (week 7 & onwards, Review later)