Last time:

K complete, non-arch. valued,

$f \in K[x]$ primitive if $f \in \mathcal{O}_K[x]$ and

$f \not\equiv 0 \mod \mathfrak{m}_K$,

Set $k := \mathcal{O}_K / \mathfrak{m}_K$

Prop. (Hensel's la): $f \in K[x]$ primitive,

$\bar{f} = g_0 \cdot h_0$ with $g_0, h_0 \in k[x]$

$(g_0, h_0) = (1)$ in $k[x]$

Then $f = g \cdot h$ with $g, h \in \mathcal{O}_K[x]$,

$\deg g = \deg g_0$, $\deg h = \deg h_0$

& $g \equiv g_0$, $h \equiv h_0$ in $k[x]$

Moreover, g, h are unique up to multiplication by elts in $\mathcal{O}_K^\times$.

Typical application:

$K/\mathbb{Q}$ finite, fix prime p. $\quad \mathbb{Z}_{(p)} = \{ \frac{m}{n} \in \mathbb{Q} \mid p \nmid n \}$

Assume $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} \simeq \mathbb{Z}_{(p)}[x]/f(x)$

$$f(x) \in \mathbb{Z}_{(p)}[x]$$

Write $\mathcal{O}_K/p \simeq \mathbb{F}_p[x]/f(x) = \prod_{i=1}^{g} \mathbb{F}_p[x]/\overline{h}_i(x)^{e_i}$

with $\overline{h}_i$ irreducible, $\deg \overline{h}_i = f(\mathfrak{p}_i|p)$,

and $\overline{h}_i, \overline{h}_j$ coprime for $i \neq j$

$\mathfrak{p}_i = (p,$ any lift of $\overline{h}_i)$

$\Rightarrow$ in $\mathbb{Z}_p[x]$: $\quad f(x) = \prod_{i=1}^{g} f_i(x)$ $\leftarrow$ monic

Hensel's lla

with $\bar{f}_i = h_i(x)^{e_i}$ $\left[\begin{array}{l}\text{still know} \\ (f(x)) = (\prod f_i) \\ \quad\uparrow \\ \text{in } \mathbb{Z}_p[x]\end{array}\right]$

$$\Rightarrow \quad \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \prod_{i=1}^{g} \underbrace{\mathbb{Z}_p[x] / f_i(x)}_{\text{finite free}/\mathbb{Z}_p \text{ of rank } e_i \cdot f(\mathfrak{p}_i|p)}$$

$$\Rightarrow \quad K \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p\left[\frac{1}{p}\right]$$

$$= \prod_{i=1}^{g} K_i \quad , \quad K_i/\mathbb{Q}_p = \mathbb{Q}_p[x]/f_i(x)$$

We'll see K_i are fields, actually $K_{\mathfrak{p}_i} \leftarrow$ completion of K w.r.t. to $\mathfrak{p}_i$-adic add. valuation

This should be compared to

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

$$\cong \mathbb{Q}[x]/f(x) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[x]/f(x)$$

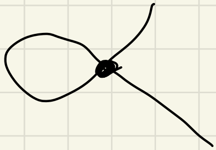
⚠ R int. domain, $I \subseteq R$ ideal

$\Rightarrow$ $\hat{R}_I$ need not be an integral domain

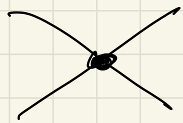
E.g. 1) $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \overset{\text{Exercise}}{=} p \cdot \mathcal{O}_K$-adic completion of $\mathcal{O}_K$ & p slits in at least two primes

2) Geometric example:

$R = k[x,y]/y^2 - x^3 - x^2$, char $k \neq 2$



and the (x,y)-adic completion of R is isomorphic to $k[[v,w]]/_{v\cdot w}$



Thm: K complete, non-arch. valued field, L/K algebraic ext., $|\cdot| : K \to \mathbb{R}_{\geq 0}$

$\Rightarrow \exists!$ ext. $|\cdot|_L : L \to \mathbb{R}_{\geq 0}$ of $|\cdot|$ to L

In part., $|\cdot|_L$ is stable under $\mathrm{Aut}(L/K)$

Moreover, if L/K is finite, $n := [L:K]$

$\Rightarrow |x|_L = |N_{L/K}(x)|^{\frac{1}{n}}$

$x \in L$

& L is complete for $|\cdot|_L$

Rmk: 1) Wrong without completeness,
$K/\mathbb{Q}$ finite, $p \in \mathbb{Z}$ prime

& $\exists\, \mathfrak{P}_1, \mathfrak{P}_2 \subseteq \mathcal{O}_K$ over (p),
$\mathfrak{P}_1 \neq \mathfrak{P}_2$

$\Rightarrow$ $v_{\mathfrak{P}_1}, v_{\mathfrak{P}_2}$ define inequivalent ext. of v_p

2) Stronger statement is true:
If $|\cdot|_{L,1}, |\cdot|_{L,2} : L \to \mathbb{R}_{\geq 0}$, s.t.

their restrictions to K are equivalent to $|\cdot|$, then $|\cdot|_{L,1} \sim |\cdot|_{L,2}$.

3) $n \geq 1$

$\Rightarrow \exists !$ add. val. $v' : \mathbb{Q}_p(p^{\frac{1}{n}}) \to \frac{1}{n}\mathbb{Z} \cup \{\infty\}$

s.t. $v^{*}(p) = 1$

$\Rightarrow \bigcup_{n \geq 0} \mathbb{Q}_p(p^{\frac{1}{n}})$ is of infinite degree over $\mathbb{Q}_p$

Proof of thm:

Suff. to assume L/K is finite

Set $|x|_L := |N_{L/K}(x)|^{\frac{1}{n}}, x \in L$

Clear: 1) $|x|_L = 0 \Leftrightarrow N_{L/K}(x) = 0$
$\Leftrightarrow x = 0$

2) $|x|_L \cdot |y|_L = |x \cdot y|_L$ for $x, y \in L$

3) $|x|_L = |x|$ for $x \in K$

Set $A \subseteq L$ be the integral closure of $\mathcal{O}_K$

$\Rightarrow A \cap K = \mathcal{O}_K$ as $\mathcal{O}_K$ is int. closed

Claim: $A = \{x \in L \mid |x|_L \leq 1\}$

Prf of claim:

$$A = \{x \in L \mid \text{min. polynomial of } x \text{ has coeff. in } \mathcal{O}_K\}$$

$$= \{x \in L \mid \max\{\underbrace{|1|}_{=1}, |N_{L/K}(x)|\} \leq 1\} = (*)$$

[Last time:

Cor. (Hensel's la): $f \in K[x]$ irred., $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$

$\Rightarrow \|f\| = \max_{i=0,\dots,n} |a_i|$

$= \max(|a_0|, |a_n|)$]

$(*) = \{x \in L \mid |x|_L \leq 1\}$ $\triangleright$ claim

Claim: $|x+y|_L \leq \max(|x|_L, |y|_L)$ $\forall x, y \in L$

Prf: Assume $|x|_L \leq |y|_L$, $x, y \neq 0$

$\Rightarrow$ STS: $\left|1+\frac{x}{y}\right| \leq 1$, i.e.

$$|1+x| \leq 1 \quad \forall x \in L, \ |x|_L \leq 1$$

$(\Leftrightarrow x \in A)$

But $A \subseteq L$ is a subring

$\Rightarrow 1+x \in A$ if $x \in A$ $\qquad$ $\square_{\text{claim}}$

Remains to see $|\cdot|_L$ is the unique ext. of $|\cdot|$ & L complete for $|\cdot|_L$.

Let $|\cdot|'$ be any extension to L, $\mathcal{O}_L$ corresp. val. ring

$\Rightarrow A \subseteq \mathcal{O}_L$ (as $\mathcal{O}_L$ int. closed)

$\Rightarrow$ $\qquad \mathcal{O}_L = A$ or $L = A$

A valuation ring "of rank 1" $\qquad$ ("valuation rings are maximal")

But $L = A$ is not possible

$\Rightarrow A = \mathcal{O}_L$

$\Rightarrow |\cdot|'$ equiv. to $|\cdot|_L$ as

A is the val. ring for $|\cdot|_L$

Completeness follows from gen. statement below

K complete, non-arch. valued field, $|\cdot| : K \to \mathbb{R}_{\geq 0}$

Def: V K-v.s. A (ultra metric) norm on V is a map

$$\|\cdot\| : V \to \mathbb{R}_{\geq 0}, \text{ s.t.}$$

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

2) $\|\lambda \cdot x\| = |\lambda| \cdot \|x\| \quad \forall \lambda \in K, x \in V$

3) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$

$\forall x, y \in V$

Note: V has basis of fund. system of open nbhds of open $\mathcal{O}_K$-submodules

$\|-\|_1, \|-\|_2$ equivalent if ex. $C_1, C_2 > 0$, s.t.

$$C_1 \|x\|_1 \leq \|x\|_2 \leq C_2 \|x\|_1 \quad \forall x \in V$$

La: Assume V f.d. K-v.s.

$\Rightarrow$ Any two norms on V are equivalent, and V is complete (for top. induced by any norm)

Proof: $(v_1, \dots, v_n)$ basis of V over K.

Set $\|\sum_{i=1}^{n} a_i v_i\| := \max_{i=1,\dots,n} |a_i|$

$\Rightarrow$ V complete for $\|-\|$.

STP: Any norm $\|\cdot\|'$ on V is equiv.

to $\|\cdot\|$

Set $C_2 := \max_{i=1,\dots,n} \|v_i\|'$

$$\Rightarrow \quad \|\underbrace{\sum_{i=1}^{n} a_i v_i}_{=:x}\|' \leq C_2 \cdot \max_{i=1,\dots,n} |a_i| \leq C_2 \cdot \|x\|$$

Claim: $\exists\, C_1 > 0$, s.t. $\|x\|' \geq C_1 \cdot \|x\|$
$\forall x \in V$

Prf: Ind. on n

Clear if $n=1$ as $V = K \cdot v_1$

For $i = 1, \dots, n$, set

$V_i = \langle v_1, \dots, \hat{v}_i, \dots, v_n \rangle$

omitted

$\Rightarrow$ $V_i \leq V$ $\Rightarrow$ $V_i \leq V$ closed

Ind. complete for $\|\cdot\|'$ for $\|\cdot\|'$-top

$\Rightarrow \bigcup_{i=1}^{n} v_i + V_i \subseteq V$ closed, does not contain 0

$\Rightarrow \exists\, \varepsilon > 0$, s.t. $\{x \in V \mid \|x\|' < \varepsilon\}$

$\subseteq V \setminus \bigcup_{i=1}^{n} v_i + V_i$

Take any $x \in V$, $x = \sum_{i=1}^{n} a_i v_i$, $x \neq 0$

Pick j, s.t. $a_j \neq 0$, $|a_j| = \|x\|$

$$\Rightarrow \|x\|' = |a_j| \cdot \|\underbrace{\frac{a_1}{a_j} \cdot v_1 + \dots + v_j + \dots + \frac{a_n}{a_j} \cdot v_n}_{\in v_j + V_j}\|$$

$\geq |a_j| \cdot \varepsilon = \varepsilon \cdot \|x\| \Rightarrow$ Take $C_1 = \varepsilon$ $\square$

Prop: K compl, discrete valued field, L/K field of degree n

$\Rightarrow \mathcal{O}_L$ is free over $\mathcal{O}_K$

Necessarily, $\mathrm{rk}_{\mathcal{O}_K} \mathcal{O}_L = n$ (as $\mathcal{O}_L \otimes_{\mathcal{O}_K} K = L$)

Rmk: $\mathcal{O}_K$ PID $\Rightarrow$ the case L/K sep. has been dealt with using the trace bilinear form

Prf: Let $\pi \in \mathcal{O}_K$ be a uniformizer.
Let $\bar{x}_1, \dots, \bar{x}_m \in \mathcal{O}_L/\pi\mathcal{O}_L$ be a basis over $k := \mathcal{O}_K/\mathfrak{m}_K = \mathcal{O}_K/\pi$
Let $x_1, \dots, x_m \in \mathcal{O}_L$ be lifts
Consider $\psi: \mathcal{O}_K^m \to \mathcal{O}_L$, $(a_i)_i \mapsto \sum_{i=1}^m a_i x_i$

Claim: ψ is an isomorphism.

Use lemma:

$f: M \to N$ morph. of $\mathcal{O}_K$-modules,

1) If M is π-adically complete, i.e. $M \simeq \varprojlim_n M/\pi^n M$, N is π-adic. separated, i.e. $\bigcap_{n \geq 0} \pi^n N = \{0\}$,

& $\bar{f}: M/\pi \to N/\pi$ is surjective

$\Rightarrow$ f surjective

2) If M is π-adically sep,

N is π-torsionfree

& $\bar{f}: M/\pi \to N/\pi$ injective

$\Rightarrow$ f injective

(1) + 2) $\Rightarrow$ ψ iso., as $\bar{\psi}$ is an iso.)

G profinite, $H \subseteq G$ finite index

$\not\Rightarrow$ H open in G

Ex: $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

$$\Rightarrow \text{ ex. surj. } G \twoheadrightarrow \prod_{p \text{ primes}} \mathbb{Z}/2 =: X$$

$\mathbb{F}_2$

has many finite index subgroups which are not open

$$X \supseteq Y := \bigoplus_{p \text{ primes}} \mathbb{Z}/2$$

any preimage of a finite index subgrp in $\underbrace{X/Y}_{\mathbb{F}_2\text{-v.s. of infinite dimension}}$ will do