Local Fields Example Sheet 2

1. $v_\pi(x) = \infty \iff x = 0$ by definition

$x, y \in \mathcal{O}_K \overset{x \neq 0 \neq y}{\implies} e_\pi(xy\,\mathcal{O}_K) =$

$= e_\pi(x\mathcal{O}_K) + e_\pi(y\mathcal{O}_K)$,

so $v_\pi(xy) = v_\pi(x) + v_\pi(y)$

If one of x and y is zero,

~~[illegible]~~ we have $v_\pi(xy) = v_\pi(x) +$
$+ v_\pi(y)$

since $\infty = n + \infty \;\; \forall n \in \mathbb{Z} \cup \{\infty\}$.
(by definition).

$x, y \in \mathcal{O}_K$ ~~[illegible]~~. Then $\pi^e \mid x\mathcal{O}_K, y\mathcal{O}_K$

$\Rightarrow \pi^e \mid (x+y)\mathcal{O}_K$

(recall that $I \mid J \iff I \supseteq J$).

Thus $e_{\mathfrak{p}}((x+y)\mathcal{O}_K) \geq \min(e_{\mathfrak{p}}(x\mathcal{O}_K),$
$e_{\mathfrak{p}}(y\mathcal{O}_K))$

so $v_{\mathfrak{p}}(x+y) \geq \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$

(you can go through and check that everything works if one of x, y or $x+y$ is 0).

$v_{\mathfrak{p}}$ is discrete by construction,

and $x \in \mathfrak{p} \implies v_{\mathfrak{p}}(x) > 0$.

Therefore $v_{\mathfrak{p}}|_{\mathbb{Z}_p}$ is a non-archimedean valuation on $\mathbb{Z}_p$ such that $v_{\mathfrak{p}}(p) > 0$

It follows that $v_{\mathfrak{p}}|_{\mathbb{Z}_p}$ is equivalent to v_p by Q14, Example Sheet 1.

2. We set $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$.

We have $5\mathcal{O}_L = (2+i)\mathcal{O}_L \cdot (2-i)\mathcal{O}_L$

and the latter are distinct prime ideals.

Set $\mathfrak{p}_1 = (2+i)\mathcal{O}_L$, $\mathfrak{p}_2 = (2-i)\mathcal{O}_L$.

Then $v_{\mathfrak{p}_1}(2-i) = 0 = v_{\mathfrak{p}_2}(2+i)$ and

so $v_{\mathfrak{p}_1}(2+i) = 1 = v_{\mathfrak{p}_2}(2-i)$,

so $v_{\mathfrak{p}_1}$ and $v_{\mathfrak{p}_2}$ are inequivalent

(they violate condition (ii) of Q10, Ex Sheet 1)

but both restrictions to $\mathbb{Z}$ are equivalent to v_5, by Q1 on this sheet.

In fact, both restrict to v_5 on the nose, as $v_{\mathfrak{p}_1}(5) = 1 = v_{\mathfrak{p}_2}(5)$.

(of course there are infinitely many more examples along these lines!)

3. Let $I = (x_1, \dots, x_n) \subseteq \mathcal{O}_K$ $\cancel{x}\ 0$.

Let v be a valuation on K in the given equivalence class.

WLOG $v(x_1) \leq v(x_2), \dots, v(x_n)$.

Then $v(x_1^{-1} x_i) = v(x_i) - v(x_1) \geq 0$ for $i = 2, \dots, n$, so

$$x_1^{-1} x_i \in \mathcal{O}_K \implies x_i \in x_1 \mathcal{O}_K.$$

$\therefore\ I = (x_1)$.

~~For~~ Second part:

By above, $\mathcal{O}_K$ Noetherian $\Rightarrow$ $\mathcal{O}_K$ PID.

Moreover, $\mathcal{O}_K$ has a unique maximal ideal (any valuation ring does), so $\mathcal{O}_K$ is a DVR and K is discretely valued.

The converse was proved in lectures.

4. Let $f(x) = g_1(x) \cdots g_m(x)$

be a factorization of $f(x)$ into

irreducible polynomials in $K[x]$.

In lectures, we showed that all roots ~~each~~ of g_i have the same

valuation.

It follows that

$$f_r(x) = \prod_{\substack{g_i \text{ has} \\ \text{all roots of} \\ \text{valuation } r}} g_i(x)$$

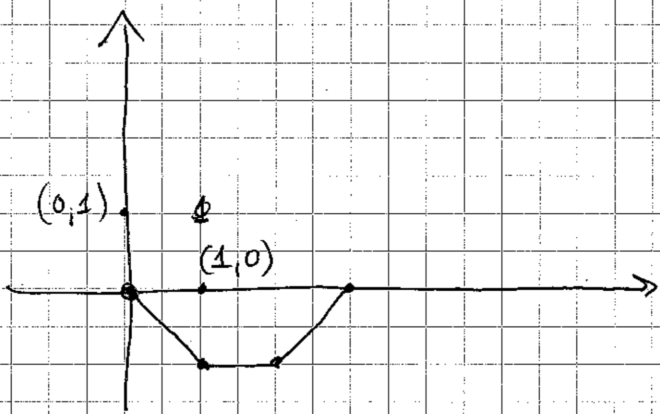
and hence $f_r(x) \in K[x]$.

The last part is then immediate since

the line segment of the Newton

polygon correspond to the possible valuations of the roots.

5. (i)



By Q4 on this sheet, the cubic $f(x)$ has three linear factors over $\mathbb{Q}_2$, hence three roots (of valuations $-1, 0, 1$).

Second part:

Multiply by 8: $8x^3 - 4x^2 - 4x + 8$

Set $y = 2x$: $y^3 - y^2 - 2y + 8$.

Quick way ("cheating")

Note that $y=-2$ is a root & factor it out. Then apply Hensel's Lemma to the other factor y^2-3y+4.

Long way

$$g(y)=y^3-y^2-2y+8 \equiv y^3-y^2 \equiv y^2(y-1) \mod 2$$

Hensel $\Rightarrow$ g has a root $\alpha \in \mathbb{Z}_2$ of valuation 0.

Let β, γ be the other roots. Then

$$\begin{cases} v_2(\alpha\beta\gamma) = v_2(\beta\gamma) = v_2(8) = 3, \\ v_2(\alpha\beta+\alpha\gamma+\beta\gamma) \\ v_2(\beta),\ v_2(\gamma) \geq 0 \end{cases}$$

$\Rightarrow$ $v_2(\beta)=1$ and $v_2(\gamma)=2$ (or the other way around).

$\Rightarrow$ $v_2(\beta+\gamma)=1$, $v_2(\beta\gamma)=3$

So $(y-\beta)(y-\gamma) = y^2 - 2uy + 8v$

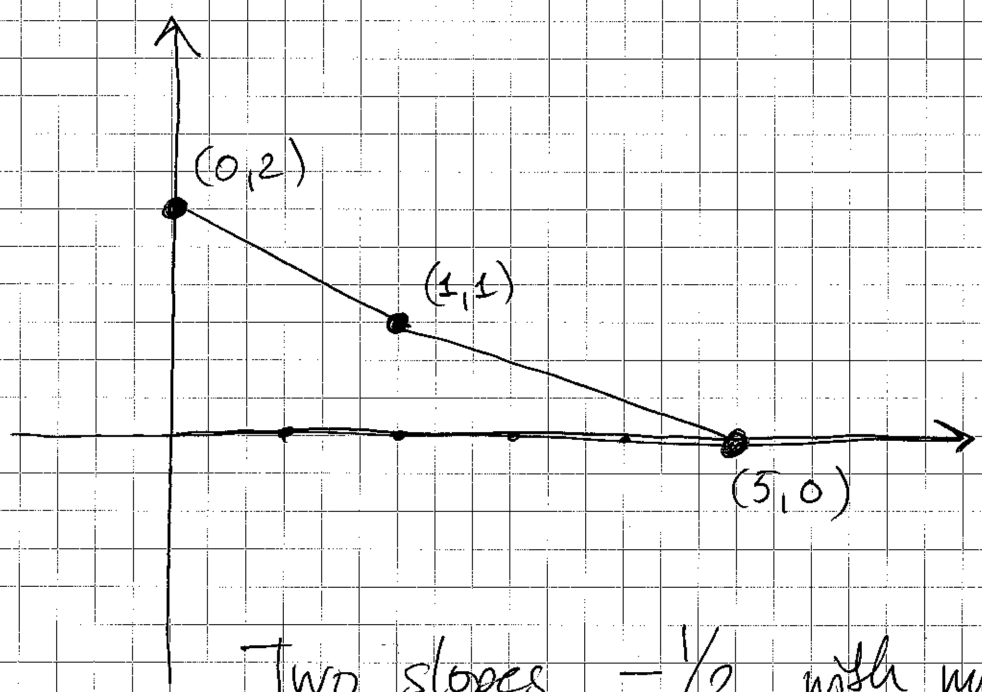
for some $u, v \in \mathbb{Z}_2^\times$.

Set $2z = y$ and divide by 4 to get

$$h(z) = z^2 - uz + 2v \equiv z(z-1) \mod 2$$

Thus $\alpha, \beta \in \mathbb{Z}_2$ by Hensel, and one can ~~follow~~ back track to show that f has three roots, of the desired valuations.

(ii)



Two slopes $-1/2$ with multiplicity 2

$-1/3$ with multiplicity 3

By Q4 on this sheet

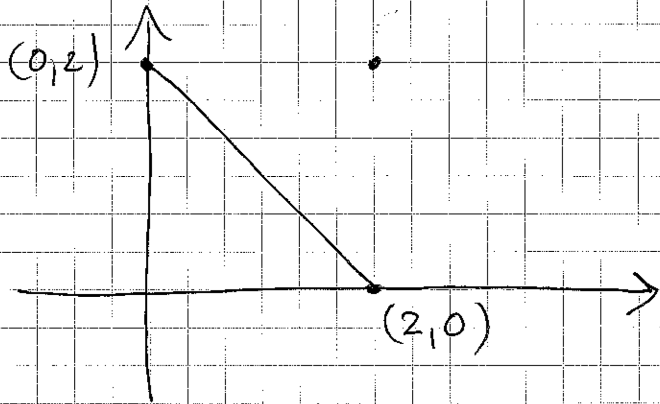
$$g(x) = g_{1/2}(x)\, g_{1/3}(x)$$

where $g_{1/2}(x) \in \mathbb{Q}_2[x]$ is quadratic with roots of valuation $1/2$, and $g_{1/3}(x) \in \mathbb{Q}_2[x]$ is cubic with roots of valuation $1/3$.

Neither $g_{1/2}(x)$ nor $g_{1/3}(x)$ have roots in $\mathbb{Q}_2$ (since $1/2, 1/3 \notin v_2(\mathbb{Q}_p)$) so they have to be irreducible.

iii) $h(x) = x^2 - 4 = (x+2)(x-2)$

has Newton polygon



6. The top coefficent of f_n is the top coefficient of $(x+1)^{p^{n-1}(p-1)}$, i.e $\underline{1}$.

The constant coefficient is

$$f_n(0) = \Phi_{p^n}(1) = p \, .$$

The roots of f_n are $\zeta_{p^n}^i - 1$, $i \in (\mathbb{Z}/p^n)^\times$, note that

$$\#(\mathbb{Z}/p^n)^\times = p^{n-1}(p-1)$$

Since Φ_{p^n} is irreducible, so is f_n and hence $w(\zeta_{p^n}^i - 1) = w(\zeta_{p^n}^j - 1)$ for all $i, j \in (\mathbb{Z}/p^n)^\times$.

It follows that

$$w(\zeta_{p^n}^i - 1) = \left(\sum_{j \in (\mathbb{Z}/p^n)^\times} w(\zeta_{p^n}^j - 1)\right) \Big/ p^{n-1}(p-1) =$$

$$= \frac{w\left(\prod_{j \in (\mathbb{Z}/p^n)^\times} \zeta_{p^n}^j - 1\right)}{p^n(p-1)} = \frac{w(p)}{p^n(p-1)} = \frac{1}{p^n(p-1)} .$$

7. $f(x) = x^3 + 4x + 7$

$\Delta f(x) = f(x+1) - f(x) = 3x^2 + 3x + 5$

$\Delta^2 f(x) = 6x + 6$

$\Delta^3 f(x) = 6$, $\Delta^n f(x) = 0 \quad \forall n \geq 4$.

so $a_0(f) = f(0) = 7$,

$a_1(f) = \Delta f(0) = 5$

$a_2(f) = \Delta^2 f(0) = 6$

$a_3(f) = \Delta^3 f(0) = 6$

$a_n(f) = 0 \quad \forall n \geq 4$.

So

$$f(x) = 6\binom{x}{3} + 6\binom{x}{2} + 5\binom{x}{1} + 7\binom{x}{0}$$

$$g(x) = x^4 + 8x^3 + 6x^2 + 5$$

$\Delta g(x) = 4x^3 + 30x^2 + 40x + 15$

$\Delta^2 g(x) = 12x^2 + 72x + 74$

$$\Delta^3 g(x) = 24x + 84$$

$$\Delta^4 g(x) = 24$$

$$\Delta^4 g(x) = 0 \quad \forall n \geqslant 5, \text{ so}$$

$$g(x) = 24\binom{x}{4} + 84\binom{x}{3} + 74\binom{x}{2} + 15\binom{x}{1} + 5\binom{x}{0}.$$

---

8. i) The first part is just the binomial theorem.

Then we have

$$(1+a)^m(1+a)^n = (1+a)^{m+n}$$

for all $m, n \in \mathbb{Z}_{\geq 0}$

By density,

$$(1+a)^x(1+a)^y = (1+a)^{x+y}$$

$\forall x, y \in \mathbb{Z}_p$ since both sides are continuous functions in x and y.

Note that $(1+a)^x - 1 = \sum_{n=1}^{\infty} \binom{x}{n} a^n \in \mathfrak{m}_K$

for all a and x,

so $\left((1+a)^x\right)^y = \left(1 + \left((1+a)^x - 1\right)\right)^y$

makes sense.

We have $(1+a)^{mn} = \left((1+a)^m\right)^n$

for all $m, n \in \mathbb{Z}_{\geq 0}$, so we obtain

$(1+a)^{xy} = \left((1+a)^x\right)^y \;\; \forall x, y \in \mathbb{Z}_p$ by

density and continuity as before.

ii) By part i), we have, for $x, y \in \mathbb{Z}_p$,

$$(1+\lambda_i)^{x+p^n y} = (1+\lambda_i)^x \left((1+\lambda_i)^{p^n}\right)^y$$

Since $(1+\lambda_i)^{p^n} = \zeta_{p^n}^{ip^n} = 1$, we see

that $x \longmapsto (1+\lambda_i)^{x+p^n y}$ is

constant on cosets of $p^n\mathbb{Z}_p$.

It follows that

$$x \longmapsto \frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-mi} (1+\lambda_i)^x$$

is constant on cosets of $p^n \mathbb{Z}_p$.

Now let $x = j \in \{0, 1, \dots, p^n - 1\}$.

Then

$$\frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-mi} (1+\lambda_i)^j = \frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-mi+ji} =$$

$$= \begin{cases} 1 & \text{if } j = m \\ 0 & \text{if } j \neq m. \end{cases}$$

(iii) If $S \subseteq \mathbb{Z}_p$ is a subset, write

$$\mathbb{1}_S(x) = \begin{cases} 1, & x \in S \\ 0, & x \notin S \end{cases}$$

for the indicator function of S.

By ii)

$$\mathbb{1}_{m+p^n\mathbb{Z}_p}(x) = \frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-mi} (1+\lambda_i)^x =$$

$$= \frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-mi} \sum_{j=0}^{\infty} \binom{X}{j} \lambda_i^j =$$

$$= \sum_{j=0}^{\infty} \left(\frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-mi} \lambda_i^j \right) \binom{X}{j}$$

Set $\quad a_j(m,n) = \frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_{p^n}^{-mi} \lambda_i^j$

Then $a_j(m,n) \in \mathbb{Z}_p$. One way to see this is that the extension $\mathbb{Q}_p(\zeta_{p^n}) | \mathbb{Q}_p$ is Galois and ~~that~~ $\sigma(a_j(m,n)) = a_j(m,n)$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n}) | \mathbb{Q}_p)$.

Thus $\mathbb{1}_{m+p^n\mathbb{Z}_p}(X) = \sum_{j=0}^{\infty} a_j(m,n) \binom{X}{j}$

is the Mahler expansion of $\mathbb{1}_{m+p^n\mathbb{Z}_p}$.

Now let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be any arbitrary continuous function.

Fix $\varepsilon > 0$. By uniform continuity of f, we may find $n \geqslant 0$ and $c_0, \ldots, c_{p^n-1} \in \mathbb{Q}_p$ s.t if

$$g = \sum_{m=0}^{p^n-1} c_m \mathbb{1}_{m+p^n\mathbb{Z}_p},$$ then

$\|f-g\|_\infty \leqslant \varepsilon$ (note that g is continuous).

Note that $a_j(m,n) \longrightarrow 0$ as $j \to \infty$ for all m,n. It follows that $\exists N$ s.t

$j \geqslant N \Rightarrow |a_j(g)|_p \leqslant \varepsilon$

Then, for $j \geqslant N$,

$$\|\Delta^j f - \Delta^j g\|_\infty \leqslant \|f-g\|_\infty \leqslant \varepsilon,$$

and hence

$$|a_j(f)|_p = |\Delta^j f(0)|_p \leqslant |\Delta^j g(0)|_p + |\Delta^j f(0) - \Delta^j g(0)|_p \leqslant 2\varepsilon.$$

Here $a_j(f) \to 0$ as $j \to \infty$.

9. We have

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

$$= \left|\sum_{j=0}^{n-1} (b_j-a_j)\alpha^j\right| \leqslant$$

$$\leqslant \max_{j=0,\dots,n-1} \left(|b_j-a_j|\,|\alpha|^j\right).$$

If $|\alpha-\beta_i| > \max_{j=0,\dots,n-1} \left(|b_j-a_j|^{1/n}\,|\alpha|^{j/n}\right)$

for all i, this would be a contradiction.

10. Let L be the Galois closure of $K(\alpha,\beta)$ over $K(\beta)$, and let $\sigma \in \mathrm{Gal}(L/K(\beta))$.

(note that α seperable $\Rightarrow$ $L|K(\beta)$ Galois)

Then

since $\beta = \sigma(\beta)$

$$|\alpha - \sigma(\alpha)| = |\alpha - \beta + \beta - \sigma(\alpha)| =$$

$$= |\alpha - \beta + \sigma(\beta - \alpha)| \leq$$

$$\leq \max\left(|\alpha - \beta|, |\sigma(\beta - \alpha)| \right) =$$

$$= |\alpha - \beta|$$

since σ is an isometry.

It follows that $|\alpha - \sigma(\alpha)| < |\alpha - \alpha_i|$ $\forall i = 2, \dots, n$, by assumption.

But $\sigma(\alpha)$ is a $K(\beta)$-conjugate of α, hence a K-conjugate of α, so $\sigma(\alpha) \in \{\alpha, \alpha_2, \dots, \alpha_n\}$.

It follows that we must have $\sigma(\alpha) = \alpha$.

Since this holds for all $\sigma \in Gal(L/K(\beta))$, $\alpha \in K(\beta)$ and hence $K(\alpha) \subseteq K(\beta)$.

11. Let α be a primitive element of $L/\mathbb{Q}_p$. Fix an algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ containing L, ~~and~~.

Put $n = [L:\mathbb{Q}_p]$ and let $\alpha_2, \dots, \alpha_n$ be the $\mathbb{Q}_p$-conjugates in $\overline{\mathbb{Q}_p}$ of α.

Let $f(x) \in \mathbb{Q}_p[x]$ be the minimal polynomial of $\alpha / \mathbb{Q}_p$.

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we may find a monic degree n polynomial $g(x) \in \mathbb{Q}[x]$ with a root $\beta \in \overline{\mathbb{Q}_p}$ s.t $|\alpha - \beta| < |\alpha - \alpha_i|$ for $i = 2, \dots, n$, by Q9 on this sheet.

By Krasner's Lemma (Q10),
$L = \mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta)$.

Since $\deg g = n$, we have

$$[\mathbb{Q}_p(\beta):\mathbb{Q}_p] \leq n = [L:\mathbb{Q}_p]$$

and hence $L = \mathbb{Q}_p(\beta)$,

moreover g is irreducible over $\mathbb{Q}_p$ and hence over $\mathbb{Q}$.

Put $K = \mathbb{Q}(\beta)$; this is an extension of $\mathbb{Q}$ of degree n.

Since

$$K = \bigoplus_{i=0}^{n-1} \mathbb{Q}\beta^i \subseteq \bigoplus_{i=0}^{n-1} \mathbb{Q}_p\beta^i = L$$

we ~~deas~~ see that K is dense in L.

K is a valued field by restricting the absolute value $|\cdot|$ on L to K, and L is the completion of K.

To finish, we need to show that $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}}$ for some maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ containing p.

(here $\mathcal{O}_K$ is the ring of integers of K
and <u>not</u> the valuation ring for $|\cdot|$).

<u>CLAIM</u>: Let $|\cdot|$ be any non-archimedean absolute value on K s.t $|p| < 1$. Then $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}}$ for some $\mathfrak{p}$ containing p.

<u>Proof</u>: Let $\mathcal{O}_K$ be the ring of integers of K. Every $x \in \mathcal{O}_K$ is integral over $\mathbb{Z}$ (by definition), so we must have $|x| \leq 1$. (since $|\mathbb{Z}| \leq 1$).

Let $\mathfrak{p} = \{ x \in \mathcal{O}_K \mid |x| < 1 \}$.

We have $p \in \mathfrak{p}$, and one checks that $\mathfrak{p}$ is a non-zero prime ideal, hence maximal.

We wish to show that $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}}$.

Let $S = \mathcal{O}_K \setminus \mathfrak{p}$. Note that, by construction of $\mathfrak{p}$ and $|\cdot|_{\mathfrak{p}}$, we have $x \in S \iff |x| = 1 \iff |x|_{\mathfrak{p}} = 1$, for $x \in \mathcal{O}_K$. S is multiplicatively closed since ~~Consider the subring~~ $\mathfrak{p}$ is a prime ideal.

Consider the subring

$$\mathcal{O}_{K,\mathfrak{p}} = \left\{ \frac{a}{b} \in K \;\middle|\; a \in \mathcal{O}_K,\ b \in S \right\} \subseteq K.$$

We claim that $\mathcal{O}_{K,\mathfrak{p}}$ is a discrete valuation ring, with maximal ideal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$.

Before proving this, note that this would imply that $|\cdot|$ and $|\cdot|_{\mathfrak{p}}$ are equivalent. Indeed, both are ≤ 1 on $\mathcal{O}_{K,\mathfrak{p}}$ and $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = \{ x \in \mathcal{O}_{K,\mathfrak{p}} \mid |x| < 1 \} =$

$$= \{ x \in \mathcal{O}_{K,\mathfrak{p}} \mid |x|_{\mathfrak{p}} < 1 \}$$

So if $\pi \mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$, then

$|\cdot| = |\ |_{\mathfrak{p}}^{s}$, where s is such that

$|\pi| = |\pi|_{\mathfrak{p}}^{s}$.

<u>$\mathcal{O}_{K,\mathfrak{p}}$ is a DVR</u>

<u>Step 1</u>: If $I \subseteq \mathcal{O}_{K,\mathfrak{p}}$ is an ideal, then $(I \cap \mathcal{O}_K) \cdot \mathcal{O}_{K,\mathfrak{p}} = I$.

<u>Pf</u>: $(I \cap \mathcal{O}_K) \cdot \mathcal{O}_{K,\mathfrak{p}} \subseteq I$, is clear.

If $\frac{a}{s} \in I$, then $a \in I \cap \mathcal{O}_K$ and hence $\frac{a}{s} = \frac{1}{s} a \in (I \cap \mathcal{O}_K) \cdot \mathcal{O}_{K,\mathfrak{p}}$, proving the reverse ~~⊆~~ inclusion.

<u>Step 2</u>: If $I \subseteq \mathcal{O}_{K,\mathfrak{p}}$ is a nonzero ideal, then $I = \mathfrak{p}^n \mathcal{O}_{K,\mathfrak{p}} = (\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^n$ for some $n \geq 0$.

<u>Pf</u>: We use some basic ~~s~~ facts about $\mathcal{O}_K$.

First, $\mathcal{O}_K$ is Noetherian $\Rightarrow$ $\mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}} = (\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^n$ $\forall n \geq 0$ (both ideals have the same generators).

Next, write $I \cap \mathcal{O}_K = \mathfrak{p}^n \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where ~~no~~ $n, e_1, \dots, e_r \geq 0$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are non-zero prime ideals of $\mathcal{O}_K$ distinct from $\mathfrak{p}$.

By Step 1, we have

$$I = (I \cap \mathcal{O}_K) \cdot \mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n \mathfrak{p}_1^{e_r} \cdots \mathfrak{p}_r^{e_r} \mathcal{O}_{K,\mathfrak{p}} =$$

$$= (\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^n (\mathfrak{p}_1\mathcal{O}_{K,\mathfrak{p}})^{e_1} \cdots (\mathfrak{p}_r\mathcal{O}_{K,\mathfrak{p}})^{e_r}.$$

It remains to show that if $\mathfrak{q} \neq \mathfrak{p}$ is a maximal ideal, then $\mathfrak{q}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$.

But $\mathfrak{q} \neq \mathfrak{p} \Rightarrow \mathfrak{q} \cap S \neq \emptyset$, so $\mathfrak{q}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$.

<u>Step 3</u>: $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is principal.

<u>Pf</u>: We may find $\pi \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \setminus \mathfrak{p}^2\mathcal{O}_{K,\mathfrak{p}}$

(for example, take $\pi \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ s.t $|\pi|$ is maximal).

Then $\pi\mathcal{O}_{K,\mathfrak{p}} \neq \mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}}$ for $n \geq 2$, so by Step 2 we must have $\pi\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$.

Step 2 & 3 then imply that the nonzero ideals of $\mathcal{O}_{K,\mathfrak{p}}$ are $\pi^n\mathcal{O}_{K,\mathfrak{p}}$, $n \geq 0$, so $\mathcal{O}_{K,\mathfrak{p}}$ is a PID with a unique maximal ideal, i.e a DVR.

12. We are going to use the following equivalent formulation of the Baire category theorem:

Let X be a metric. Assume that there exists closed, nowhere dense subsets $F_1, F_2, \ldots$ such that $X = \bigcup_{i=1}^{\infty} F_i$

Then X is not complete.

A set $S \subseteq X$ is called nowhere dense if $U \not\subseteq S$ for every open set $U \subseteq X$.

(This formulation is roughly the contrapositive of the formulation in the exercise).

Now consider $\overline{\mathbb{Q}_p}$. Let $K \subseteq \mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$. Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ inside $\overline{\mathbb{Q}_p}$.

~~We have $\mathbb{Q}$~~

By the first part in the pf of Q11, $\exists \alpha \in \overline{\mathbb{Q}}$ s.t. $K = \mathbb{Q}_p(\alpha)$.

It follows that $\overline{\mathbb{Q}_p} = \bigcup_{\alpha \in \overline{\mathbb{Q}}} \mathbb{Q}_p(\alpha)$.

We claim that $\mathbb{Q}_p(\alpha) \subseteq \overline{\mathbb{Q}_p}$ is closed and nowhere dense.

First, it is complete, hence closed.

Second, $\overline{\mathbb{Q}_p}$ is infinite dimensional over $\mathbb{Q}_p$ (for example, there is an unramified ext^n of every degree $n \in \mathbb{Z}_{\geq 1}$);

and in any normed space V, if a linear subspace W contains an open set, then $V = W$.

Thus, since $\mathbb{Q}_p(\alpha) \neq \overline{\mathbb{Q}_p}$, $\mathbb{Q}_p(\alpha)$ is nowhere dense.

Since $\overline{\mathbb{Q}}$ is countable, it follows ~~that~~ from the Baire category thm that $\overline{\mathbb{Q}_p}$ is not complete.

13. Let $\overline{\mathbb{Q}_p}$ be an algebraic closure of $\mathbb{C}_p$. Take $\alpha \in \overline{\mathbb{C}_p}$ and consider $\mathbb{C}_p(\alpha)$.

Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{C}_p[x]$ be the minimal polynomial of α, and let $\alpha_2, \dots, \alpha_n$ be the other roots of f.

Since $\overline{\mathbb{Q}_p}$ is dense in $\mathbb{C}_p$, we may find $g(x) = x^n + b_{n-1}x^{n-1} + \dots + a_0 \in \overline{\mathbb{Q}_p}[x]$ with a root β s.t

$$|\alpha - \beta| < |\alpha - \alpha_i|, \quad i = 2, \dots, n,$$

, using Q9 on this sheet.

By Krasner's Lemma (Q10), we have $\mathbb{C}_p(\alpha) \subseteq \mathbb{C}_p(\beta)$.

But $\overline{\mathbb{Q}_p}$ is algebraically closed, so $\beta \in \overline{\mathbb{Q}_p} \subseteq \mathbb{C}_p$. Thus $\mathbb{C}_p(\alpha) = \mathbb{C}_p$ so $\alpha \in \mathbb{C}_p$, and $\mathbb{C}_p$ is algebraically closed.

14. i) Let $v \in V$ and let $(e_i)_{i \in I}$ be an orthonormal basis for V.

Then, writing $v = \sum a_i e_i$

$$\|v\| = \max_{i \in I} |a_i|_p \in \{p^n \mid n \in \mathbb{Z}\} \cup \{0\}.$$

Moreover, $\|p^{-n} e_i\| = |p^{-n}| = p^n \ \forall n \in \mathbb{Z}$ and $\|0\| = 0$, so we have equality.

ii) Let $V^0 = \{v \in V \mid \|v\| \leq 1\}$.

We have $$V = \bigcup_{n \in \mathbb{Z}} p^n V^0 = \bigcup_{n \in \mathbb{Z}} \{v \in V \mid \|v\| \leq p^{-n}\}$$

~~Set ||v||' = p^{−sup{n | v∈}~~

Set $$\|v\|' = p^{-\sup\{n \in \mathbb{Z} \mid v \in p^n V^0\}},$$

where $\sup\{n \in \mathbb{Z} \mid v \in p^n V^0\} = \infty$ if $v \in p^n V^0 \ \forall n$, i.e. if $v = 0$, and

$p^{-\infty} := 0$.

One checks that this is a $\mathbb{Q}_p$-norm on V

and that $||V||' = |\mathbb{Q}_p|_p$.

Moreover, one checks that

$$p^{-1}||v||' \leq ||v|| \leq ||v||',$$

so $||\cdot||'$ and $||-||$ are equivalent.

iii) Consider $V^0 = \{v \in V \mid ||v|| \leq 1\}$.

This is a $\mathbb{Z}_p$-module, and the quotient V^0/pV^0 is an $\mathbb{F}_p$-vector space.

Take a set of elements $(e_i)_{i \in I}$ in V^0 such that the reductions $\overline{e_i} \in V^0/pV^0$ form an $\mathbb{F}_p$-basis for V^0/pV^0.

<u>Claim</u> $(e_i)_{i \in I}$ is an orthonormal basis for V.

Pf: First, $e_i \in V^\circ \setminus pV^\circ \Rightarrow$

$\overset{p^{-1}\not<}{\Longrightarrow} \|e_i\| \leq 1 \Rightarrow \|e_i\| = 1$.

"Linear independence" / Uniqueness

Assume that $0 = \sum a_i e_i$, with $a_i \to 0$. Assume that not all a_i are 0. Then, since the a_i are bounded, we may scale them so that $|a_i|_p \leq 1 \ \forall i$ and $\exists i: |a_i|_p = 1$.

Then, reducing mod pV°, we get a nontrivial equation $0 = \sum \bar{a}_i \bar{e}_i$, which is a contradiction, since the $\bar{e}_i$ form a basis for V° / pV°.

Existence & norm equality

Let $v \neq 0$ be in V. By scaling, it suffices to prove the following:

If $\|v\|=1$, then $\exists a_i$ s.t

$\sum a_i e_i = v$, and $\max_i |a_i|_p = 1$.

not needed

(For each $n \geq 0$, we have an isomorphism

$$V^0 / p V^0 \longrightarrow p^n V^0 / p^{n+1} V^0$$
$$v \longmapsto p^n v$$

of $\mathbb{F}_p$-vector spaces.)

Now, consider $\overline{v} =$ v mod pV^0, and choose

$a_{i,0} \in \{0, \dots, p-1\}$ s.t

$$\overline{v} = \sum_{i \in I} \overline{a_{i,0}}\, \overline{e_i}.$$

Then $v - \sum_{i \in I} a_{i,0} e_i \in pV^0$, so take

$a_{i,1} \in \{0, \dots, p-1\}$ s.t

$$\overline{\frac{1}{p}\left(v - \sum a_{i,0} e_i\right)} = \sum_{i \in I} \overline{a_{i,1}}\, \overline{e_i}.$$

Then $v - \sum (a_{i,0} + p a_{i,1}) e_i \in p^2 V^0$

Continuing in this way, we find

$$a_{i,0}, \ldots, a_{i,n}, \ldots \in \{0, \ldots, p-1\} \text{ s.t.}$$

$$v - \sum \left(a_{i,0} + p a_{i,1} + \ldots + p^n a_{i,n}\right) e_i \in p^{n+1} V^0$$

$\forall n$.

Set $a_i = \sum_{n=0}^{\infty} a_{i,n} p^n$; it follows

that $v = \sum_{i \in I} a_i e_i$, $a_i \in \mathbb{Z}_p$.

Also, since $v \notin p V^0$, we must have an i such that $a_{i,0} \neq 0 \Rightarrow |a_i|_p = 1$ and hence $\max_{i \in I} |a_i|_p = 1$.