Thm Let k be a field that has no nontriv. disc. val.
Then, the norm. disc. val. of $K = k(T)$ are:

- $f(T)$-adic val. for irred. $f(T) \in k[T]$
- $v_{\deg}$: $\frac{1}{T}$-adic val. $\left(\left(\frac{1}{T}\right) \subset k\left[\frac{1}{T}\right] \right)$.

Geometric intuition

Interpret any $g(T) \in k(T)$ as a "function" on the projective line $\mathbb{P}^1 = k \cup \{\infty\}$.

Then, $v_{X-a}(g) =$ order of vanishing of $g(T)$ at $T = a$
(< 0 if pole)

$v_{\infty}(g) = v_{\deg}(g) =$ order of vanishing of $g(T)$ at $T = \infty$.

<u>Pf</u> $v|_k$ is a disc. val. on k, so $v|_k$ is the triv. val.: $v(x) = 0 \ \forall x \in k^\times$.

$\Rightarrow k \subseteq \mathcal{O}_v$.

<u>Case 1: $v(T) \geq 0$</u>

$\Rightarrow k[T] \subseteq \mathcal{O}_v$.

Like in Thm 1.1. (for $\mathbb{Q}$), it follows that $v = v_{f(T)}$ for some irred. $f(T)$.

<u>Case: $v(T) < 0$</u>

$\Rightarrow k[\frac{1}{T}] \subseteq \mathcal{O}_v$

and $\mathfrak{p}_v \cap k[\frac{1}{T}] \subseteq k[\frac{1}{T}]$ prime ideal containing $\frac{1}{T}$.

$\Rightarrow \mathfrak{p}_v \cap k[\frac{1}{T}] = (\frac{1}{T})$.

Like in Thm 1.1., it follows that $v = v_{\deg}$.

$\square$

1.2. Topology

Let v be any valuation on K.

Fix any $\lambda > 1$. (If the res. field is $k_v = \mathbb{F}_q$, one usually picks $\lambda = q$.)

Then, $|x| = \lambda^{-v(x)}$ defines a norm on K:

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

b) $|xy| = |x| \cdot |y|$

c) $|x+y| \le \max(|x|, |y|)$

(stronger than the triangle inequality: $|x+y| \le |x| + |y|$.

$\leadsto$ <u>nonarchimedean</u> norm).

<u>Rmk</u> x close to y $\Leftrightarrow$ $v(x-y)$ large ($|x-y|$ small)

$\Leftrightarrow$ $x \equiv y \mod \mathfrak{p}^n$ for large n.

if $v = v_{\mathfrak{p}}$

<u>Rmk</u> The topology induced by $|\cdot|$ is indep. of λ.

Thm This makes K a <u>topological field</u>:

$$+ : K \times K \to K, \quad \times : K \times K \to K, \quad \cdot^{-1} : K^\times \to K^\times$$
$$(x,y) \mapsto x+y \qquad (x,y) \mapsto xy \qquad x \mapsto x^{-1}$$

are continuous.

1.3. Completion

Def/thm Let v be any norm. disc. val. on K. We call K <u>complete</u> w.r.t. v if every Cauchy seq. in K converges in K. The <u>completion</u> of K w.r.t. v is the field $\hat{K}_v$ consisting of Cauchy seq. in K modulo seq. converging to 0.

Extend $|\cdot|$ to $\hat{K}_v$ by $\left|\lim_{n\to\infty} a_n\right| := \lim_{n\to\infty} |a_n|$.

Extend v to a val. on $\hat{K}_v$ by

$$v\left(\lim_{n\to\infty} a_n\right) := \lim_{n\to\infty} v(a_n).$$

Note that v is still norm. disc. because $v(\hat{K}^\times) = \mathbb{Z}$ is discrete in $\mathbb{R}$.

We let $\hat{\mathcal{O}}_v := \{x \in \hat{K}_v \mid v(x) \geq 0\}$,

$$\hat{\mathfrak{p}}_v := \{x \in \hat{K}_v \mid v(x) > 0\}.$$

Lemma We have $\hat{\mathcal{O}}_v / \hat{\mathfrak{p}}_v^n \xleftarrow{\sim} \mathcal{O}_v / \mathfrak{p}_v^n$

$$x \longleftarrow\!\shortmid\; x$$

for all $n \geq 0$ and $\hat{\mathfrak{p}}_v = \mathfrak{p}_v \hat{\mathcal{O}}_v$.

Lemma Let $(a_n)_{n \geq 0}$ with $a_n \in \hat{K}_v$.

The series $\sum_{n=0}^{\infty} a_n$ converges (in $\hat{K}_v$)

if and only if $a_n \xrightarrow[n \to \infty]{} 0$.

Pf "$\Leftarrow$" The partial sums $\sum_{n=0}^{M} a_n$ form a

Cauchy seq. because $\left| \sum_{n=N}^{M} a_n \right| \leq \max_{N \leq n \leq M} |a_n| \xrightarrow{N \to \infty} 0$.

"$\Rightarrow$" as for $\mathbb{R}$. $\square$

Lemma Let $S \subseteq \mathcal{O}_v$ be a set containing exactly one representative of each residue class in $\kappa_v = \mathcal{O}_v/\mathfrak{p}_v$. Then, each $x \in \hat{\mathcal{O}}_v$ can be written uniquely as

$$x = \sum_{i=0}^{\infty} a_i \pi_v^i \quad \text{with } a_i \in S.$$

"digits"

We have $x \in \hat{\mathcal{O}}_v^\times \Leftrightarrow a_0 \not\equiv 0 \bmod \mathfrak{p}_v$.

Each $x \in \hat{K}_v^\times$ can be written uniquely as

$$x = \sum_{i=-r}^{\infty} a_i \pi_v^i \text{ with } r \in \mathbb{Z},\ a_i \in S,$$
$$a_{-r} \not\equiv 0 \bmod \mathfrak{p}_v.$$

Pf For $x \in \hat{\mathcal{O}}_v$:

$$a_0 \equiv x \bmod \hat{\mathfrak{p}}_v$$

$$a_1 \equiv \frac{x - a_0}{\pi_v} \bmod \hat{\mathfrak{p}}_v$$

$$a_2 \equiv \frac{x - a_0 - a_1\pi_v}{\pi_v^2} \bmod \hat{\mathfrak{p}}_v$$

$$\vdots$$

$$x \in \hat{\mathcal{O}}_v^\times \Leftrightarrow v(x) = 0 \Leftrightarrow \overset{a_0}{\underset{|||}{x}} \not\equiv 0 \bmod \mathfrak{p}_v.$$

For $x \in \hat{K}_v^\times$, just look at $\frac{x}{\pi_v^{v(x)}} \in \hat{\mathcal{O}}_v^\times$.

$\square$

Ex $K = \mathbb{Q}$, $v = v_p$ (p-adic val.)

$\rightsquigarrow$ field of p-adic rationals $\mathbb{Q}_p = \hat{K}_v$

ring of p-adic integers $\mathbb{Z}_p = \hat{\mathcal{O}}_v$.

Let $S = \{0, \dots, p-1\}$ (repr. for el. of $\mathbb{Z}/p\mathbb{Z}$).

$$\Rightarrow \mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \;\middle|\; a_i \in \{0, \dots, p-1\} \right\}$$

$$= \{ \dots a_2 a_1 a_0 \mid \text{—"—} \}$$

Addition / mult. with carry like in $\mathbb{Z}$.

Unit $\Leftrightarrow$ last digit $a_0 \neq 0$.

For example,

$-1 = \dots 444$ in $\mathbb{Z}_5$

$\frac{1}{2} = \dots 223$ in $\mathbb{Z}_5$.

$\mathbb{Q}_p = \{ \dots a_2 a_1 a_0 . a_{-1} a_{-2} \dots a_{-r} \}$.

Ex k any field, $K = k(T)$, $v = v_T$ (T-adic val.)

$\Rightarrow \hat{\mathcal{O}}_v = k[[T]]$ ring of power series

$\hat{K}_v = k((T))$ field of Laurent series.

Pf The residue field is $\kappa_v = k[T]/(T) = k \subset K$, so take $S = \kappa_v$ and $\pi_v = T$.

$\Rightarrow$ Every elt. of $\hat{\mathcal{O}}_v$ is

$$\sum_{i=0}^{\infty} a_i T^i \text{ with } a_i \in k.$$

Every el. of $\hat{K}_v$ is

$$\sum_{i=-r}^{\infty} a_i T^i \text{ with } a_i \in k. \qquad \square$$

The def. of $\mathbb{Z}_p$ agrees with that given in section 0.2:

<u>Thm</u> Denote by $\varprojlim_n \mathcal{O}_v/\mathfrak{q}_v^n$ the

"inverse limit"

set of $(a_n)_{n\geq 0} \in \prod_{n\geq 0} \mathcal{O}_v/\mathfrak{q}_v^n$ such

that $a_n \equiv a_m \mod \mathfrak{q}_v^n$ for all $n \leq m$.
Equip each $\mathcal{O}_v/\mathfrak{q}_v^n$ with the discrete top.,
$\prod_{n\geq 0} \mathcal{O}_v/\mathfrak{q}_v^n$ with the prod. top.,
$\varprojlim \mathcal{O}_v/\mathfrak{q}_v^n$ with the subspace top.

Then, the map
$$\hat{\mathcal{O}}_v \longrightarrow \varprojlim_{n\to\infty} \mathcal{O}_v/\mathfrak{q}_v^n$$
$$x \longmapsto (x \bmod \mathfrak{q}_v^n)_n$$

is a homeomorphism.

REFERENCE: Neukirch, Algebraic Number Theory, Section II.

1.4. Nonarchimedean local fields

__Def__ A __(nonarch.) local field__ is a field K with a disc. val. v such that K complete w.r.t. v and the res. field κ_v is finite.

$\mathcal{O}_K := \mathcal{O}_v$, $\pi_K := \pi_v$, ---, $q_K := |\kappa_v|$.

$\kappa_v = \mathbb{F}_{q_K}$.

__Lemma__ If K is a nonarch. loc. field, then $\mathcal{O}_K$ is compact. (See also problem 5 on PSet 1.)

__Pf__ $\kappa_v = \mathbb{F}_q$. $\Rightarrow \#(\mathcal{O}_v/\mathfrak{p}_v^n) = q^n < \infty$

$\Rightarrow \mathcal{O}_v/\mathfrak{p}_v^n$ compact

$\Rightarrow \prod_{n \geq 0} \mathcal{O}_v/\mathfrak{p}_v^n$ compact

$\Rightarrow \mathcal{O}_v = \varprojlim \mathcal{O}_v/\mathfrak{p}_v^n$ compact.

$\uparrow$

$\varprojlim \mathcal{O}_v/\mathfrak{p}_v^n$ is a closed subset of $\prod \mathcal{O}_v/\mathfrak{p}_v^n$

$\square$

Lem $\mathfrak{p}_v^n$ is a compact open closed subset of K for all $n \in \mathbb{Z}$.

Pf $\mathfrak{p}_v^n = \{x \in K \mid v(x) \geq n\}$

$= \{x \in K \mid |x| \leq \lambda^{-n}\}$ closed

$= \{x \in K \mid |x| < R\}$ open

for R slightly larger than λ^{-n}.

$\mathcal{O}_v$ cpt., $\mathfrak{p}_v^n = \pi_v^n \cdot \mathcal{O}_v$

$\Rightarrow \mathfrak{p}_v^n$ cpt. $\square$

Lem K is locally cpt.

Pf For any $x \in K$, the set $x + \mathcal{O}_v$ is a cpt. open closed nbhd. of x. $\square$

Def The <u>archimedean local fields</u> are $\mathbb{R}$, $\mathbb{C}$.

1.5. Hensel's lemma

Let K be complete w.r.t. a disc. val. v.

Hensel's lemma (version 1) $V1$

Let $f(X) \in \mathcal{O}_v[X]$ and assume $\alpha \in \underset{\mathcal{O}_v/\varphi_v}{\overset{\shortparallel}{k_v}}$ is a simple root of $(f(X) \bmod \varphi_v) \in k_v[X]$.

Then, there is exactly one root $\beta \in \mathcal{O}_v$ of $f(X)$ such that $\beta \equiv \alpha \bmod \varphi_v$ (a lift of α).

Ex If $p \neq 2$ is a prime number and $a \not\equiv 0 \bmod p$ is a quadr. res. mod p, then $\sqrt{a} \in \mathbb{Z}_p$.

Pf (assuming V1)

$f(X) = X^2 - a$ has a root $\alpha \in \mathbb{F}_p$ mod p.

$f'(\alpha) = 2\alpha \not\equiv 0 \bmod p \Rightarrow$ simple root

$p \neq 2,\ \alpha \not\equiv 0$

$\Rightarrow f(X) = X^2 - a$ has a root in $\mathbb{Z}_p$. □

<u>Ex</u> $X^2 - 3$ has a (non-simple) root mod 3, but $\sqrt{3} \notin \mathbb{Z}_3$.

$X^2 - 3$ has a (non-simple) root mod 2, but no root mod 4.

$\Rightarrow \sqrt{3} \notin \mathbb{Z}_2$.