Formalizing Local Fields in Lean

Filippo A. E. Nuccio Mortarino Majno di Capriglio

Université Jean Monnet-Saint-Étienne (France)

joint work with

María Inés de Frutos-Fernández

University of Bonn

Lean for the Curious Mathematician 2025 ICTS, Bangalore April 25th, 2025



Outline

- Project at a glance
- Discrete Valuations and DVR's
 - Definitions
 - Relation between discrete valuations and DVR's
 - Complete discretely valued fields
- 3 Local Fields
 - Mixed characteristic
 - Equal characteristic
 - Unramified extensions

Main Goal & Ingredients

Main goal: make Lean understand the following

Definition

A (nonarchimedean) local field is a field complete with respect to a discrete valuation and with finite residue field.

Main Goal & Ingredients

Main goal: make Lean understand the following

Definition

A (nonarchimedean) local field is a field complete with respect to a discrete valuation and with finite residue field.

Main Ingredients:

- Discrete valuations;
- The unit ball w.r.t a discrete valuation is a DVR (already in Mathlib);
- Extensions of discrete valuations;
- \mathbb{Q}_p , $\mathbb{F}_p((X))$ and their finite extensions are local fields.

Main Goal & Ingredients

Main goal: make Lean understand the following

Definition

A (nonarchimedean) local field is a field complete with respect to a discrete valuation and with finite residue field.

Main Ingredients:

- Discrete valuations;
- The unit ball w.r.t a discrete valuation is a DVR (already in Mathlib);
- Extensions of discrete valuations;
- \mathbb{Q}_p , $\mathbb{F}_p((X))$ and their finite extensions are local fields.

Long-term goal: Formalize Local Class Field Theory, that describes explicitly the abelian extensions of local fields, in Lean.



Summary

- $\bullet \sim 8k$ lines of new Lean code, the PR process is in progress;
- we used algebra, topology, analysis, ... results from Mathlib;

Summary

- $\bullet \sim 8k$ lines of new Lean code, the PR process is in progress;
- we used algebra, topology, analysis, ... results from Mathlib;
- we also relied upon https://github.com/mariainesdff/norm_ extensions_lean_4/tree/master/NormExtensions;
- The whole project is available at

```
https://github.com/mariainesdff/LocalClassFieldTheory.
```

 The project has been described in the paper María Inés de Frutos-Fernández, F. N., A Formalization of Complete Discrete Valuation Rings and Local Fields. CPP 2024, https://dl. acm.org/doi/10.1145/3636501.3636942

Outline

- Project at a glance
- Discrete Valuations and DVR's
 - Definitions
 - Relation between discrete valuations and DVR's
 - Complete discretely valued fields
- 3 Local Fields
 - Mixed characteristic
 - Equal characteristic
 - Unramified extensions

Valuations

A valuation v on a ring R is a map $v\colon R\to \Gamma_0$ to a linearly ordered commutative group *with zero* Γ_0 (where $\bot=0\notin \Gamma$) such that

- v(0) = 0;
- ② $v(1) = 1_{\Gamma};$

Valuations

A valuation v on a ring R is a map $v\colon R\to \Gamma_0$ to a linearly ordered commutative group *with zero* Γ_0 (where $\bot=0\notin \Gamma$) such that

- v(0) = 0;
- ② $v(1) = 1_{\Gamma};$
- $v(x+y) \le \max\{v(x), v(y)\} \text{ for all } x, y \in R;$

The unit ball of a valuation $v \colon R \to \Gamma_0$ is the subring

$$R_0 := \{ x \in R \mid v(x) \le 1_{\Gamma} \}.$$

• If $R = \mathbb{Z}$ and p is a prime number, the additive p-adic valuation a_p of $r \in \mathbb{Z} \setminus \{0\}$ is $a_p(r) := \max\{ n \in \mathbb{Z} \mid p^n \text{ divides } r \}$. Set $a_p(0) = \infty$.

- If $R = \mathbb{Z}$ and p is a prime number, the additive p-adic valuation a_p of $r \in \mathbb{Z} \setminus \{0\}$ is $a_p(r) := \max\{ n \in \mathbb{Z} \mid p^n \text{ divides } r \}$. Set $a_p(0) = \infty$.
- Extend it to an additive valuation on \mathbb{Q} via $a_p(\frac{r}{s}) = a_p(r) a_p(s)$.

- If $R = \mathbb{Z}$ and p is a prime number, the additive p-adic valuation a_p of $r \in \mathbb{Z} \setminus \{0\}$ is $a_p(r) := \max\{ n \in \mathbb{Z} \mid p^n \text{ divides } r \}$. Set $a_p(0) = \infty$.
- Extend it to an additive valuation on \mathbb{Q} via $a_p(\frac{r}{s}) = a_p(r) a_p(s)$.
- The function $v_p \colon \mathbb{Q} \to p^{\mathbb{Z}} \cup \{0\} \cong \mathbb{Z} \cup \{\bot\}$ given by $v_p(x) = p^{-a_p(x)}$ and $v_p(0) = 0$, is a valuation on \mathbb{Q} .

- If $R = \mathbb{Z}$ and p is a prime number, the additive p-adic valuation a_p of $r \in \mathbb{Z} \setminus \{0\}$ is $a_p(r) := \max\{ n \in \mathbb{Z} \mid p^n \text{ divides } r \}$. Set $a_p(0) = \infty$.
- Extend it to an additive valuation on \mathbb{Q} via $a_p(\frac{r}{s}) = a_p(r) a_p(s)$.
- The function $v_p \colon \mathbb{Q} \to p^{\mathbb{Z}} \cup \{0\} \cong \mathbb{Z} \cup \{\bot\}$ given by $v_p(x) = p^{-a_p(x)}$ and $v_p(0) = 0$, is a valuation on \mathbb{Q} .
- **Examples**: $v_3(18) = 1/9$, $v_3(5/54) = 27$, $v_{37}(31/101) = 1$.

- If $R = \mathbb{Z}$ and p is a prime number, the additive p-adic valuation a_p of $r \in \mathbb{Z} \setminus \{0\}$ is $a_p(r) := \max\{ n \in \mathbb{Z} \mid p^n \text{ divides } r \}$. Set $a_p(0) = \infty$.
- Extend it to an additive valuation on \mathbb{Q} via $a_p(\frac{r}{s}) = a_p(r) a_p(s)$.
- The function $v_p \colon \mathbb{Q} \to p^{\mathbb{Z}} \cup \{0\} \cong \mathbb{Z} \cup \{\bot\}$ given by $v_p(x) = p^{-a_p(x)}$ and $v_p(0) = 0$, is a valuation on \mathbb{Q} .
- **Examples**: $v_3(18) = 1/9$, $v_3(5/54) = 27$, $v_{37}(31/101) = 1$.
- The unit ball is the subring

$$\mathbb{Z}_{(p)} = \left\{ \frac{r}{s} : p \nmid s \right\} \subseteq \mathbb{Q}$$

and its units are the multiplicative group

$$\mathbb{Z}_{(p)}^{\times} = \left\{ \frac{r}{s} : p \nmid s \text{ and } p \nmid r \right\} \subseteq \mathbb{Q}^{\times}$$



• If $R = \mathbb{F}_q[X]$, then

$$v_X^{(q)}(f/g) = q^{(\max_n \{X^n | g\} - \{\max_n (X^n | f\}))}$$

defines a $q^{\mathbb{Z}} \cup \{0\}) = (p^{f\mathbb{Z}} \cup \{0\})$ -valued valuation on $\operatorname{Frac} R = \mathbb{F}_q(X)$.

- Examples:
 - $v_X^{(q)}(X^2/(X+1)) = 1/q^2;$
 - $v_X^{(q)}((X-1)/(X^2-X))=q.$
- The unit ball is the subring

$$K_0 = \left\{ \frac{f(X)}{g(X)} : g(0) \neq 0 \right\}.$$



The type \mathbb{Z}_{m0}

Both for v_p and $v_X^{(q)}$, the base of the exponential — transforming (+) into (*) — is irrelevant: what matters is the structure of $p^{\mathbb{Z}}=\langle p\rangle_*\cong \mathbb{Z}=\langle 1\rangle_+$.

The type $\mathbb{Z}_{\mathtt{m}0}=$ WithZero (Multiplicative \mathbb{Z}) is $p^{\mathbb{Z}}\cup\{0\}$ without p.

The type \mathbb{Z}_{m0}

Both for v_p and $v_X^{(q)}$, the base of the exponential — transforming (+) into (*) — is irrelevant: what matters is the structure of $p^{\mathbb{Z}}=\langle p\rangle_*\cong \mathbb{Z}=\langle 1\rangle_+$.

The type $\mathbb{Z}_{\mathtt{m}0} = \mathtt{WithZero}$ (Multiplicative \mathbb{Z}) is $p^{\mathbb{Z}} \cup \{0\}$ without p.

```
def Multiplicative (\alpha : Type u) := \alpha def ofAdd : \alpha \simeq Multiplicative \alpha := \langle \text{fun x => x, fun x => x, fun } \rangle theorem ofAdd_add : ofAdd (x + y) = ofAdd x * ofAdd y := rfl
```

Examples:

- $\bullet (1:\mathbb{Z}_{\mathtt{m}0}) = \mathtt{ofAdd}(0:\mathbb{Z});$
- ullet $(0:\mathbb{Z}_{\mathtt{m}0})
 eq \mathtt{ofAdd}(n:\mathbb{Z}) \ \mathsf{for \ all} \ n \in \mathbb{Z};$
- ofAdd $(1:\mathbb{Z})=$ ofAdd $(1:\mathbb{Z})\ldots \to$ This is just a generator of $\mathbb{Z}_{\mathfrak{m}};$
- ullet of $Add(-1:\mathbb{Z})$ is another one...;
- $\bullet \ (0:\mathbb{Z}_{\mathtt{m}0}) < (\mathtt{ofAdd}(-1:\mathbb{Z}):\mathbb{Z}_{\mathtt{m}0}) < (1:\mathbb{Z}_{\mathtt{m}0}) < (\mathtt{ofAdd}(37:\mathbb{Z}):\mathbb{Z}_{\mathtt{m}0}).$

Discrete valuations

Pen & Paper Math: A discrete valuation on a field K is a non-trivial valuation $v: K \to ?^{\mathbb{Z}} \cup \{0\}$. Upon rescaling, it can be normalized so that it is surjective and "we will tacitly assume it is surjective henceforth".

Discrete valuations

Pen & Paper Math: A discrete valuation on a field K is a non-trivial valuation $v \colon K \to ?^{\mathbb{Z}} \cup \{0\}$. Upon rescaling, it can be normalized so that it is surjective and "we will tacitly assume it is surjective henceforth".

Lean: A discrete valuation on a field K is a valuation $v \colon K \to \Gamma$ to a linearly ordered commutative group with zero Γ satisfying

```
class IsDiscrete [IsCyclic \Gamma^{\times}] [Nontrivial \Gamma^{\times}] : Prop where exists_generator_LTOne : \exists \ (\gamma : \Gamma^{\times}), Subgroup.zpowers \gamma = \top \land \gamma < 1 \land \uparrow \gamma \in \text{range v}
```

Example

- The p-adic valuation v_p on $\mathbb Q$ is discrete: $v_p(p) = \mathtt{ofAdd}(-1:\mathbb Z)$
- The X -adic valuation $v_X^{(q)}$ on $\mathbb{F}_q(X)$ is discrete: $v_q(X) = \mathtt{ofAdd}(-1:\mathbb{Z})$.

Discrete valuation rings

An integral domain is a discrete valuation ring (DVR) if it is a local principal ideal domain which is not a field.

```
class IsDiscreteValuationRing (R : Type U) [CommRing R]
  [IsDomain R] extends IsPrincipalIdealRing R, LocalRing R
  where
  not_a_field' : maximalIdeal R ≠ ⊥
```

Given its name, it'd better be related to discrete valuations...

The unit ball is a DVR

Proposition (Serre's Corps Locaux, Proposition I.1.1)

If K is a field with a discrete valuation v, then its unit ball K_0 is a discrete valuation ring.

```
variable (K:Type u) [Field K] (v:Valuation K Γ) [IsDiscrete v]

local notation "K<sub>0</sub>" => v.ValuationSubring

instance isDVR_of_isDiscrete: IsDiscreteValuationRing K<sub>0</sub> where
toIsPrincipalIdealRing := integer_isPrincipalIdealRing v
toLocalRing := inferInstance
not_a_field' := by
   rw [Ne.def, ← isField_iff_maximalIdeal_eq]
   exact not_isField v
```

Uniformizers (I)

Let K be a field with a valuation $v: K \to \Gamma$.

- A uniformizer is a $\pi \in K$ such that $v(\pi) = (\top : \text{Subgroup } \Gamma^{\times}).\text{genLTOne};$
- the valuation is discrete if and only if there exists a uniformizer for v.

Uniformizers (I)

Let K be a field with a valuation $v: K \to \Gamma$.

- A uniformizer is a $\pi \in K$ such that $v(\pi) = (\top : \text{Subgroup } \Gamma^{\times}).\text{genLTOne};$
- ullet the valuation is discrete if and only if there exists a uniformizer for v.

```
def IsUniformizer (\pi : K) : Prop :=
  v \pi = (T : Subgroup \Gamma^{\times}).genLTOne
structure Uniformizer where
  val: v.integer -- an element of the unit ball
  valuation_eq_gen : IsUniformizer v val
lemma isDiscrete_of_exists_Uniformizer \{\pi : K\}
   (h\pi : IsUniformizer v \pi) : IsDiscrete v := ...
lemma exists Uniformizer of Discrete [IsDiscrete v]:
   \exists \pi : K_0, IsUniformizer v (\pi : K) := ...
```

Uniformizers (II)

If $u \in K$ satisfies $v(u) = (1:\Gamma^\times)$, then $u \cdot \pi$ is again a uniformizer, and $u \in K_0^\times$.

Since every uniformizer is sent to a generator, (\Leftarrow discrete valuation...) each $0 \neq r \in K_0$ can be uniquely written in the form

```
r = \pi^n \cdot u, with n \in \mathbb{N}, u \in K_0^{\times}.
```

```
variables {K : Type u} [Field K] (v : Valuation K \Gamma)

lemma pow_Uniformizer {r : K_0} (hr : r \neq 0)

(\pi : Uniformizer v) :

\exists n : \mathbb{N}, \exists u : K_0^{\times}, r = (\pi.1 ^n).1 * u.1 := ...
```

Uniformizers (II)

If $u \in K$ satisfies $v(u) = (1 : \Gamma^{\times})$, then $u \cdot \pi$ is again a uniformizer, and $u \in K_0^{\times}$.

Since every uniformizer is sent to a generator, (\Leftarrow discrete valuation...) each $0 \neq r \in K_0$ can be uniquely written in the form

```
r = \pi^n \cdot u, with n \in \mathbb{N}, u \in K_0^{\times}.
```

```
variables {K : Type u} [Field K] (v : Valuation K \Gamma)

lemma pow_Uniformizer {r : K<sub>0</sub>} (hr : r \neq 0)

(\pi : Uniformizer v) :

\exists n : \mathbb{N}, \exists u : K_0^{\times}, r = (\pi.1 ^ n).1 * u.1 := ...
```

It follows that the maximal ideal of K_0 is generated by any uniformizer:

```
lemma Uniformizer_is_generator (\pi : Uniformizer v) : maximalIdeal v.ValuationSubring = Ideal.span {\pi.1} := ...
```

The fraction field of a DVR

Using uniformizers, we can prove the converse of Serre's Proposition: the fraction field of a discrete valuation ring admits *a* discrete valuation.

```
\label{eq:commRingR} \begin{tabular}{ll} variable (R:Type u) [CommRing R] [IsDomain R] [IsDiscrete ValuationRing R] \\ instance: Valued (FractionRing R) <math>\mathbb{Z}_{m0} := (maximalIdeal\ R).adicValued \\ instance: IsDiscrete (R:=FractionRing\ R)\ Valued.v:= \\ isDiscrete 0f Exists Uniformizer\ Valued.v \\ (valuation\_exists\_uniformizer\ (FractionRing\ R) \\ (maximalIdeal\ R)).choose\_spec \end{tabular}
```

Let R be a DVR, $v \colon R \twoheadrightarrow \mathbb{Z}_{m0}$ "its" discrete valuation.

• v defined using \mathfrak{m}_R , and R local: essentially unique;

Let R be a DVR, $v \colon R \twoheadrightarrow \mathbb{Z}_{m0}$ "its" discrete valuation.

- v defined using \mathfrak{m}_R , and R local: essentially unique;
- $\mathbb{Z} \operatorname{Frac} \mathbb{Z}_{(p)} = \mathbb{Q}$ admits valuations v_{ℓ} for every prime ℓ : p and R are lost!

Let R be a DVR, $v \colon R \twoheadrightarrow \mathbb{Z}_{m0}$ "its" discrete valuation.

- v defined using \mathfrak{m}_R , and R local: essentially unique;
- $\mathbb{Z} \operatorname{Frac} \mathbb{Z}_{(p)} = \mathbb{Q}$ admits valuations v_{ℓ} for every prime ℓ : p and R are lost!
- **2** There are two ways of extending v_3 to $\mathbb{Q}(\sqrt{7})$, because $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;

Complete discretely valued fields

Let R be a DVR, $v: R \to \mathbb{Z}_{m0}$ "its" discrete valuation.

- v defined using \mathfrak{m}_R , and R local: essentially unique;
- $\mathbb{Z} \operatorname{Frac} \mathbb{Z}_{(p)} = \mathbb{Q}$ admits valuations v_{ℓ} for every prime ℓ : p and R are lost!
- **2** There are two ways of extending v_3 to $\mathbb{Q}(\sqrt{7})$, because $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;
- Solution to both problems: consider complete fields.

Let R be a DVR, $v: R \to \mathbb{Z}_{m0}$ "its" discrete valuation.

- v defined using m_R, and R local: essentially unique;
- $\mathbb{Z} \operatorname{Frac} \mathbb{Z}_{(p)} = \mathbb{Q}$ admits valuations v_{ℓ} for every prime ℓ : p and R are lost!
- Z There are two ways of extending v_3 to $\mathbb{Q}(\sqrt{7})$, because $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;
- $v : R \to \mathbb{Z}_{m0}$ defines a metric on $K = \operatorname{Frac} R$ with balls

$$\mathscr{B}(0,\rho)=\{x:K \text{ such that } v(x)<\rho\} \qquad (\text{say for } \rho:\mathbb{Z}_{\mathtt{m}0});$$

and we can consider the completion of K with respect to this metric.

Let R be a DVR, $v: R \to \mathbb{Z}_{m0}$ "its" discrete valuation.

- v defined using \mathfrak{m}_R , and R local: essentially unique;
- $\mathbb{Z} \operatorname{Frac} \mathbb{Z}_{(p)} = \mathbb{Q}$ admits valuations v_{ℓ} for every prime ℓ : p and R are lost!
- There are two ways of extending v_3 to $\mathbb{Q}(\sqrt{7})$, because $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;
- $v: R \to \mathbb{Z}_{m0}$ defines a metric on $K = \operatorname{Frac} R$ and we can consider the completion of K with respect to this metric.

Proposition

If K is complete w.r.t a discrete valuation v and L/K is a finite extension, then L has a unique discrete $w\colon L\to \mathbb{Z}_{\mathtt{m}0}$ inducing v and L is complete w.r.t. w.

Let R be a DVR, $v \colon R \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$ "its" discrete valuation.

- v defined using \mathfrak{m}_R , and R local: essentially unique;
- $\mathbb{Z} \operatorname{Frac} \mathbb{Z}_{(p)} = \mathbb{Q}$ admits valuations v_{ℓ} for every prime ℓ : p and R are lost!
- There are two ways of extending v_3 to $\mathbb{Q}(\sqrt{7})$, because $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;
- $v: R \to \mathbb{Z}_{m0}$ defines a metric on $K = \operatorname{Frac} R$ and we can consider the completion of K with respect to this metric.

Proposition

If K is complete w.r.t a discrete valuation v and L/K is a finite extension, then L has a unique discrete $w \colon L \to \mathbb{Z}_{\mathtt{m}0}$ inducing v and L is complete w.r.t. w.

Example

- \mathbb{Q}_p is the completion of \mathbb{Q} w.r.t v_p : complete, with unit ball $\mathbb{Z}_p = \widehat{\mathbb{Z}_{(p)}}$;
- ullet $\mathbb{F}_q(\!(X)\!)$ is the completion of $\mathbb{F}_q(X)$ w.r.t $v_X^{(q)}$, with unit ball $\mathbb{F}_q[\![X]\!]$.

Proposition

If K is complete w.r.t a discrete valuation v and L/K is a finite extension, the integral closure of K_0 in L coincides with L_0 and thus is a DVR.

```
variable {K L : Type u} [Field K] [Field L] [Algebra K L]
  [hv : Valued K Γ] [IsDiscrete hv.v] [CompleteSpace K]

lemma integralClosure_eq_integer [FiniteDimensional K L] :
  (integralClosure hv.v.ValuationSubring L).toSubring =
        (extendedValuation K L).ValuationSubring.toSubring := ...

instance isDiscreteValuationRing_of_finite_extension
  [FiniteDimensional K L] :
  IsDiscreteValuationRing
        (integralClosure hv.v.ValuationSubring L) := ...
```

Some formalization pain

Let R be a Dedekind domain: for our purposes, assume R not local.

- \bullet $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} \colon K \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$;

- $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} \colon K \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$;
- $v_{\mathfrak{p}}$ extends to $\widehat{v_{\mathfrak{p}}} \colon K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$ where $K_{\mathfrak{p}}$ is the completion of K w.r.t. $v_{\mathfrak{p}}$;

- $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} \colon K \twoheadrightarrow \mathbb{Z}_{m0}$;
- $v_{\mathfrak{p}}$ extends to $\widehat{v_{\mathfrak{p}}} \colon K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathtt{m0}}$ where $K_{\mathfrak{p}}$ is the completion of K w.r.t. $v_{\mathfrak{p}}$;
- in particular, $(K_{\mathfrak{p}})_0$ is a discrete valuation ring: get $v_{\hat{\mathfrak{p}}} \colon (K_{\mathfrak{p}})_0 \twoheadrightarrow \mathbb{Z}_{m0}$, that can be extended to the fraction field to get $v_{\hat{\mathfrak{p}}} \colon K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{m0}$.

- \bullet $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} \colon K \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$;
- $v_{\mathfrak{p}}$ extends to $\widehat{v_{\mathfrak{p}}} \colon K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathtt{m0}}$ where $K_{\mathfrak{p}}$ is the completion of K w.r.t. $v_{\mathfrak{p}}$;
- in particular, $(K_{\mathfrak{p}})_0$ is a discrete valuation ring: get $v_{\hat{\mathfrak{p}}} \colon K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$.
- ullet "Obviously" $\widehat{v_{\mathfrak{p}}}=v_{\hat{\mathfrak{p}}}$...

- \bullet $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} \colon K \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$;
- $v_{\mathfrak{p}}$ extends to $\widehat{v_{\mathfrak{p}}} : K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$ where $K_{\mathfrak{p}}$ is the completion of K w.r.t. $v_{\mathfrak{p}}$;
- in particular, $(K_{\mathfrak{p}})_0$ is a discrete valuation ring: get $v_{\hat{\mathfrak{p}}} \colon K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$.
- "Obviously" $\widehat{v_{\mathfrak{p}}} = v_{\hat{\mathfrak{p}}} \dots$ after 250 lines of code!

```
\begin{array}{lll} \textbf{local notation "v\_compl\_of\_adic"} & => \\ & (\texttt{Valued.v : Valuation K\_v } \mathbb{Z}_{m0}) \end{array}
```

```
local notation "v_adic_of_compl" =>
   IsDedekindDomain.HeightOneSpectrum.valuation (K := K_v)
      (maxIdealOfCompletion R v K)
```

```
lemma adic_of_compl_eq_compl_of_adic (x : K_v) :
   v_adic_of_compl x = v_compl_of_adic x := ...
```

Outline

- Project at a glance
- Discrete Valuations and DVR's
 - Definitions
 - Relation between discrete valuations and DVR's
 - Complete discretely valued fields
- 3 Local Fields
 - Mixed characteristic
 - Equal characteristic
 - Unramified extensions

Local Fields

Definition

A (nonarchimedean) local field is a field complete with respect to a discrete valuation and with finite residue field.

A mixed characteristic local field is a finite field extension of the field \mathbb{Q}_p of p-adic numbers, for some prime p.

An equal characteristic local field is a finite field extension of the field $\mathbb{F}_p((X))$, for some prime p.

Mixed Characteristic Local Fields

```
class MixedCharLocalField (p : N) [Nat.Prime p] (K : Type u)
   [Field K] extends Algebra (Q_p p) K where
   to_finiteDimensional : FiniteDimensional (Q_p p) K
```

Lemma

A mixed characteristic local field K is a local field.

```
instance (p : N) [Nat.Prime p] (K : Type u) [Field K]
[MixedCharLocalField p K] : LocalField K := ...
```

Mixed Characteristic Local Fields

```
class MixedCharLocalField (p : N) [Nat.Prime p] (K : Type u)
    [Field K] extends Algebra (Q_p p) K where
    to_finiteDimensional : FiniteDimensional (Q_p p) K
```

Lemma

A mixed characteristic local field K is a local field.

```
instance (p : \mathbb{N}) [Nat.Prime p] (K : Type u) [Field K]
[MixedCharLocalField p K] : LocalField K := ...
```

The ring of integers \mathcal{O}_K is the integral closure of \mathbb{Z}_p in K: it is a DVR.

```
def ringOfIntegers := integralClosure (Z_p p) K -- \mathcal{O}_K instance : IsDiscreteValuationRing \mathcal{O}_K := integralClosure.isDiscreteValuationRing_of_finite_extension (Q_p p) K
```

The *p*-adic numbers

Mathlib's p-adic numbers:

```
def Padic (p : \mathbb{N}) [p.Prime] := CauSeq.Completion.Cauchy (padicNorm p) -- \mathbb{Q} [p]

def PadicInt (p : \mathbb{N}) [p.Prime] := { x : \mathbb{Q}[p] // ||x|| \le 1 } -- \mathbb{Z}[p]
```

Our definition:

```
\operatorname{\mathsf{def}} Q_p : Type := adicCompletion \mathbb Q (pHeightOneIdeal p) \operatorname{\mathsf{def}} Z_p := (@Valued.v (Q_p p) _ \mathbb Z_{m0} _ _).ValuationSubring
```

We prove that they are isomorphic (as rings and as uniform spaces).

```
def padicEquiv : Q_p p \simeq+* Q_[p] := ... 
def padicIntEquiv : Z_p p \simeq+* Z_[p] := ...
```

Equal Characteristic Local Fields

```
def FpXCompletion := (idealX \mathbb{F}_p).adicCompletion (RatFunc \mathbb{F}_p) -- \mathbb{F}_p(X)^{\wedge} def FpXIntCompletion := (idealX \mathbb{F}_p).adicCompletionIntegers (RatFunc \mathbb{F}_p) -- \mathbb{F}_p[X]^{\wedge} class EqCharLocalField (p : \mathbb{N}) [Nat.Prime p] (K : Type*) [Field K] extends Algebra (FpXCompletion p) K where to finiteDimensional : FiniteDimensional (FpXCompletion p) K
```

Lemma

An equal characteristic local field is a local field.

```
instance (p : \mathbb{N}) [Nat.Prime p] (K : Type u) [Field K]
  [EqCharLocalField p K] : LocalField K := ...
```

Laurent Series

The fields LaurentSeries K and K((X)) are isomorphic (for every field K)

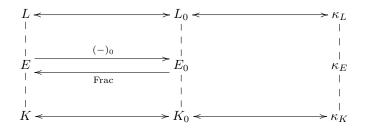
```
structure LaurentSeries (R : Type*) [Zero R] where
 coeff : \mathbb{Z} \to \mathbb{R}
  isPWO_support': (Function.support coeff.support).IsPWO
def LaurentSeriesRingEquiv :
  LaurentSeries K ≃+* RatFuncAdicCompl K := ...
def powerSeriesRingEquiv : PowerSeries K ≃+*
   (Polynomial.idealX K).adicCompletionIntegers (RatFunc K) :=
```

Let K be a (valued) local field, L/K a separable extension.

For every intermediate field L/E/K we have a diagram

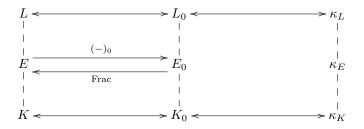
Let K be a (valued) local field, L/K a separable extension.

For every intermediate field L/E/K we have a diagram

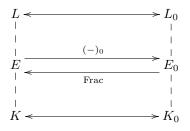


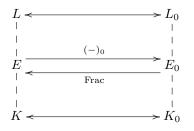
Let K be a (valued) local field, L/K a separable extension.

For every intermediate field L/E/K we have a diagram



structure IntClosedSubalgebra extends Subalgebra K_0 L_0 where is_int_closed : IsIntegrallyClosed toSubalgebra

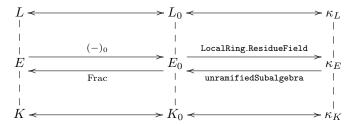




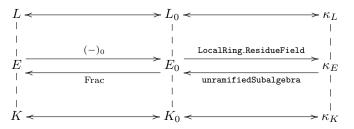
```
theorem fracField_gc : GaloisConnection
   (fracField K vL) (unitBall K vL) := ...

def fracField_gi :
    GaloisInsertion (fracField K vL) (unitBall K vL) := ...

def fracField_gci :
    GaloisCoinsertion (fracField K vL) (unitBall K vL) := ...
```



```
\begin{array}{l} \text{def unramifiedSubalgebra :} \\ \text{(IntermediateField (ResidueField } K_0) \ (\text{ResidueField } L_0))} \\ \rightarrow \text{(IntClosedSubalgebra K w_L) := } \dots \end{array}
```



```
theorem unramifiedSubalgebra_gc : GaloisConnection
   (unramifiedSubalgebra K L) (resField K L) :=

def unramifiedSubalgebra_gi (Etale K<sub>0</sub> L<sub>0</sub>) : GaloisInsertion
   (unramifiedSubalgebra K L) (resField K L) := ...

def unramifiedSubalgebra_gci : GaloisCoinsertion
   (unramifiedSubalgebra K L) (resField K L) := ...
```

Thank you

María Inés de Frutos-Fernández, Filippo A. E. Nuccio A Formalization of Complete Discrete Valuation Rings and Local Fields, CPP 2024

https://dl.acm.org/doi/10.1145/3636501.3636942

 $\verb|https://github.com/mariainesdff/LocalClassFieldTheory|\\$