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

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

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

Summary

- $\sim 8k$ 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

1. Project at a glance

2. 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

1. $v(0) = 0$;
2. $v(1) = 1_\Gamma$;
3. $v(x + y) \leq \max\{v(x), v(y)\}$ for all $x, y \in R$;
4. $v(xy) = v(x)v(y)$ for all $x, y \in R$.

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 $\perp = 0 \notin \Gamma$) such that

1. $v(0) = 0$;
2. $v(1) = 1_\Gamma$;
3. $v(x+y) \leq \max\{v(x), v(y)\}$ for all $x, y \in R$;
4. $v(xy) = v(x)v(y)$ for all $x, y \in R$.

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

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

Example 1: the p-adic valuation

- 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 $a_p(r) := \max\{\, n \in \mathbb{Z} \mid p^n$ divides $r \,\}$. Set $a_p(0) = \infty$.

Example 1: the p-adic valuation

- 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 $a_p(r) := \max\{\, n \in \mathbb{Z} \mid p^n$ divides $r \,\}$. Set $a_p(0) = \infty$.
- Extend it to an additive valuation on $\mathbb{Q}$ via $a_p(\frac{r}{s}) = a_p(r) - a_p(s)$.

Example 1: the p-adic valuation

- 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 $v_p \colon \mathbb{Q} \to p^{\mathbb{Z}} \cup \{0\} \cong \mathbb{Z} \cup \{\perp\}$ given by $v_p(x) = p^{-a_p(x)}$ and $v_p(0) = 0$, is a valuation on $\mathbb{Q}$.

Example 1: the p-adic valuation

- 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 $a_p(r) := \max\{\, n \in \mathbb{Z} \mid p^n$ 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 $v_p \colon \mathbb{Q} \to p^{\mathbb{Z}} \cup \{0\} \cong \mathbb{Z} \cup \{\perp\}$ given by $v_p(x) = p^{-a_p(x)}$ and $v_p(0) = 0$, is a valuation on $\mathbb{Q}$.
- **Examples**: $v_3(18) = 1/9$, $v_3(5/54) = 27$, $v_{37}(31/101) = 1$.

Example 1: the p-adic valuation

- 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 $a_p(r) := \max\{\, n \in \mathbb{Z} \mid p^n$ 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 $v_p \colon \mathbb{Q} \to p^{\mathbb{Z}} \cup \{0\} \cong \mathbb{Z} \cup \{\perp\}$ 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

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

Example 2: the X-adic valuation

- If $R = \mathbb{F}_q[X]$, then

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

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

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

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

The type $\mathbb{Z}_{\mathtt{m0}}$

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 $\mathbb{Z}_{\mathtt{m0}} =$ `WithZero (Multiplicative ℤ)` is $p^{\mathbb{Z}} \cup \{0\}$ without p.

The type $\mathbb{Z}_{\mathrm{m0}}$

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 $\mathbb{Z}_{\mathrm{m0}} =$ `WithZero (Multiplicative ℤ)` is $p^{\mathbb{Z}} \cup \{0\}$ without p.

```
def Multiplicative (α : Type u) := α

def ofAdd : α ≃ Multiplicative α :=
  ⟨fun x => x, fun x => x, fun _ => rfl, fun _ => rfl⟩

theorem ofAdd_add : ofAdd (x + y) = ofAdd x * ofAdd y := rfl
```

Examples:

- $(1 : \mathbb{Z}_{\mathrm{m0}}) = \mathtt{ofAdd}(0 : \mathbb{Z})$;
- $(0 : \mathbb{Z}_{\mathrm{m0}}) \neq \mathtt{ofAdd}(n : \mathbb{Z})$ for all $n \in \mathbb{Z}$;
- $\mathtt{ofAdd}(1 : \mathbb{Z}) = \mathtt{ofAdd}(1 : \mathbb{Z}) \ldots \to$ This is just *a* generator of $\mathbb{Z}_{\mathrm{m}}$;
- $\mathtt{ofAdd}(-1 : \mathbb{Z})$ is another one...;
- $(0 : \mathbb{Z}_{\mathrm{m0}}) < (\mathtt{ofAdd}(-1 : \mathbb{Z}) : \mathbb{Z}_{\mathrm{m0}}) < (1 : \mathbb{Z}_{\mathrm{m0}}) < (\mathtt{ofAdd}(37 : \mathbb{Z}) : \mathbb{Z}_{\mathrm{m0}})$.

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".

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 Γˣ] [Nontrivial Γˣ] : Prop where
  exists_generator_LTOne :
   ∃ (γ : Γˣ), Subgroup.zpowers γ = ⊤ ∧ γ < 1 ∧ ↑γ ∈ 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 "K₀" => v.ValuationSubring

instance isDVR_of_isDiscrete : IsDiscreteValuationRing K₀ 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 $v(\pi) = (\top$: Subgroup $\Gamma^{\times}$).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 $v(\pi) = (\top$: Subgroup $\Gamma^\times)$.genLTOne;
- the valuation is discrete if and only if there exists a uniformizer for v.

```
def IsUniformizer (π : K) : Prop :=
  v π = (⊤ : Subgroup Γˣ).genLTOne

structure Uniformizer where
  val : v.integer -- an element of the unit ball
  valuation_eq_gen : IsUniformizer v val

lemma isDiscrete_of_exists_Uniformizer {π : K}
    (hπ : IsUniformizer v π) : IsDiscrete v := ...

lemma exists_Uniformizer_ofDiscrete [IsDiscrete v] :
    ∃ π : K₀, IsUniformizer v (π : 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

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

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

lemma pow_Uniformizer {r : K₀} (hr : r ≠ 0)
  (π : Uniformizer v) :
  ∃ n : ℕ, ∃ u : K₀ˣ, r = (π.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

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

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

lemma pow_Uniformizer {r : K₀} (hr : r ≠ 0)
   (π : Uniformizer v) :
   ∃ n : ℕ, ∃ u : K₀ˣ, r = (π.1 ^ n).1  * u.1 := ...
```

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

```
lemma Uniformizer_is_generator (π : Uniformizer v) :
  maximalIdeal v.ValuationSubring = Ideal.span {π.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.

```
variable (R : Type u) [CommRing R] [IsDomain R] [IsDiscreteValuationRing R]

instance : Valued (FractionRing R) ℤₘ₀ := (maximalIdeal R).adicValued

instance : IsDiscrete (R := FractionRing R) Valued.v :=
 isDiscreteOfExistsUniformizer Valued.v
 (valuation_exists_uniformizer (FractionRing R)
  (maximalIdeal R)).choose_spec
```

Complete fields (I)

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

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

Complete fields (I)

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;
- $\operatorname{Frac} \mathbb{Z}_{(p)} = \mathbb{Q}$ admits valuations v_ℓ for every prime ℓ: p and R are lost!

Complete fields (I)

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

- v defined using $\mathfrak{m}_R$, and R local: essentially unique;
- ☡ $\operatorname{Frac}\mathbb{Z}_{(p)} = \mathbb{Q}$ 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 $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;

Complete fields (I)

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;
- ☡ $\operatorname{Frac}\mathbb{Z}_{(p)} = \mathbb{Q}$ 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 $3\cdot\mathbb{Z}[\sqrt{7}] = \mathfrak{p}\cdot\overline{\mathfrak{p}}$;
- Solution to both problems: consider complete fields.

Complete fields (I)

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;
- ☡ $\operatorname{Frac}\mathbb{Z}_{(p)} = \mathbb{Q}$ 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 $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;
- $v\colon R \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$ 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.

Complete fields (I)

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;
- ☡ $\operatorname{Frac}\mathbb{Z}_{(p)} = \mathbb{Q}$ 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 $3\cdot\mathbb{Z}[\sqrt{7}] = \mathfrak{p}\cdot\overline{\mathfrak{p}}$;
- $v\colon R \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$ 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.

Complete fields (I)

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;
- ⫽ $\operatorname{Frac}\mathbb{Z}_{(p)} = \mathbb{Q}$ 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 $3 \cdot \mathbb{Z}[\sqrt{7}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$;
- $v\colon R \twoheadrightarrow \mathbb{Z}_{m0}$ 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 $w\colon L \to \mathbb{Z}_{m0}$ 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 $\mathbb{Z}_p = \widehat{\mathbb{Z}_{(p)}}$;*
- *$\mathbb{F}_q(\!(X)\!)$ is the completion of $\mathbb{F}_q(X)$ w.r.t $v_X^{(q)}$, with unit ball $\mathbb{F}_q[\![X]\!]$.*

Complete fields (II)

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.

- $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} : K \twoheadrightarrow \mathbb{Z}_{\mathtt{m0}}$;

Some formalization pain

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

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

Some formalization pain

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

- $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} : K \twoheadrightarrow \mathbb{Z}_{\mathrm{m}0}$;
- $v_{\mathfrak{p}}$ extends to $\widehat{v_{\mathfrak{p}}} : K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathrm{m}0}$ 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 $v_{\hat{\mathfrak{p}}} : \Big(K_{\mathfrak{p}}\Big)_0 \twoheadrightarrow \mathbb{Z}_{\mathrm{m}0}$, that can be extended to the fraction field to get $v_{\hat{\mathfrak{p}}} : K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathrm{m}0}$.

Some formalization pain

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

- $K = \operatorname{Frac} R$;
- $\mathfrak{p} \subseteq R$ a maximal ideal that induces $v_{\mathfrak{p}} : K \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$;
- $v_{\mathfrak{p}}$ 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 $v_{\hat{\mathfrak{p}}} : K_{\mathfrak{p}} \twoheadrightarrow \mathbb{Z}_{\mathtt{m}0}$.
- "Obviously" $\widehat{v_{\mathfrak{p}}} = v_{\hat{\mathfrak{p}}}$ ...

Some formalization pain

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

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

```
local notation "v_compl_of_adic" =>
  (Valued.v : Valuation K_v ℤₘ₀)
```

```
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

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.

```
class ValuedLocalField (K : Type*) [Field K] extends
      Valued K Γ where
  complete : CompleteSpace K
  isDiscrete : IsDiscrete <| Valued.v (R := K)
  finiteResidueField : Finite <| IsLocalRing.ResidueField
    (Valued.v (R := K)).valuationSubring
```

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 : 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 -- 𝒪_K

instance : IsDiscreteValuationRing 𝒪_K :=
  integralClosure.isDiscreteValuationRing_of_finite_extension
    (Q_p p) K
```

The p-adic numbers

`Mathlib`'s p-adic numbers:

```
def Padic (p : ℕ) [p.Prime] :=
CauSeq.Completion.Cauchy (padicNorm p) -- ℚ_[p]

def PadicInt (p : ℕ) [p.Prime] :=
{ x : ℚ_[p] // ‖x‖ ≤ 1 } -- ℤ_[p]
```

Our definition:

```
def Q_p : Type := adicCompletion ℚ (pHeightOneIdeal p)

def Z_p := (@Valued.v (Q_p p) _ ℤₘ₀ _ _).ValuationSubring
```

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

```
def padicEquiv : Q_p p ≃+* ℚ_[p] := ...

def padicIntEquiv : Z_p p ≃+* ℤ_[p] := ...
```

Equal Characteristic Local Fields

```
def FpXCompletion :=
(idealX 𝔽ₚ).adicCompletion (RatFunc 𝔽ₚ) -- 𝔽ₚ(X)^

def FpXIntCompletion :=
(idealX 𝔽ₚ).adicCompletionIntegers (RatFunc 𝔽ₚ) -- 𝔽ₚ[X]^
```

```
class EqCharLocalField (p : 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 : 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 : ℤ → R
  isPWO_support' : (Function.support coeff.support).IsPWO --
    PWO is Partially Well Ordered: every infinite sequence
    contains an infinite monotone subsequence.

def LaurentSeriesRingEquiv :
  LaurentSeries K ≃+* RatFuncAdicCompl K := ...

def powerSeriesRingEquiv : PowerSeries K ≃+*
   (Polynomial.idealX K).adicCompletionIntegers (RatFunc K) :=
```

Unramified extensions of local fields

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

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

Unramified extensions of local fields

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

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

$$\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & L_0 \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & \kappa_L \arrow[d, dash, dashed] \\
E \arrow[r, shift left, "(-)_0"] \arrow[d, dash, dashed] & E_0 \arrow[l, shift left, "\mathrm{Frac}"] \arrow[d, dash, dashed] & \kappa_E \arrow[d, dash, dashed] \\
K \arrow[r, leftrightarrow] & K_0 \arrow[r, leftrightarrow] & \kappa_K
\end{tikzcd}$$

Unramified extensions of local fields

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

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

$$
\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & L_0 \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & \kappa_L \arrow[d, dash, dashed] \\
E \arrow[r, shift left, "(-)_0"] \arrow[d, dash, dashed] & E_0 \arrow[l, shift left, "\mathrm{Frac}"] \arrow[d, dash, dashed] & \kappa_E \arrow[d, dash, dashed] \\
K \arrow[r, leftrightarrow] & K_0 \arrow[r, leftrightarrow] & \kappa_K
\end{tikzcd}
$$

```
structure IntClosedSubalgebra extends Subalgebra K₀ L₀ where
    is_int_closed : IsIntegrallyClosed toSubalgebra
```

Unramified extensions of local fields

Recall: a Galois connection is a pair of maps l and u s. t. $l(a) \leq b \Leftrightarrow a \leq u(b)$:

$$\begin{tikzcd}
L \arrow[rr, leftrightarrow] \arrow[d, dash, dashed] & & L_0 \arrow[d, dash, dashed] \\
E \arrow[rr, shift left, "(-)_0"] \arrow[d, dash, dashed] & & E_0 \arrow[ll, shift left, "\mathrm{Frac}"] \arrow[d, dash, dashed] \\
K \arrow[rr, leftrightarrow] & & K_0
\end{tikzcd}$$

Unramified extensions of local fields

Recall: a Galois connection is a pair of maps l and u s. t. $l(a) \leq b \Leftrightarrow a \leq u(b)$:

$$\begin{tikzcd}
L \arrow[rr, leftrightarrow] \arrow[d, dash, dashed] & & L_0 \arrow[d, dash, dashed] \\
E \arrow[rr, shift left, "(-)_0"] \arrow[d, dash, dashed] & & E_0 \arrow[ll, shift left, "\mathrm{Frac}"] \arrow[d, dash, dashed] \\
K \arrow[rr, leftrightarrow] & & K_0
\end{tikzcd}$$

```
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) := ...
```

Unramified extensions of local fields

Recall: a Galois connection is a pair of maps l and u s. t. $l(a) \leq b \Leftrightarrow a \leq u(b)$:

$$\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & L_0 \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & \kappa_L \arrow[d, dash, dashed] \\
E \arrow[r, shift left, "(-)_0"] \arrow[d, dash, dashed] & E_0 \arrow[l, shift left, "\mathrm{Frac}"] \arrow[r, shift left, "\texttt{LocalRing.ResidueField}"] \arrow[d, dash, dashed] & \kappa_E \arrow[l, shift left, "\texttt{unramifiedSubalgebra}"] \arrow[d, dash, dashed] \\
K \arrow[r, leftrightarrow] & K_0 \arrow[r, leftrightarrow] & \kappa_K
\end{tikzcd}$$

```
def unramifiedSubalgebra :
   (IntermediateField (ResidueField K₀) (ResidueField L₀))
      → (IntClosedSubalgebra K w_L) := ...
```

Unramified extensions of local fields

Recall: a Galois connection is a pair of maps l and u s. t. $l(a) \leq b \Leftrightarrow a \leq u(b)$:

$$
\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & L_0 \arrow[r, leftrightarrow] \arrow[d, dash, dashed] & \kappa_L \arrow[d, dash, dashed] \\
E \arrow[r, shift left, "(-)_0"] \arrow[d, dash, dashed] & E_0 \arrow[l, shift left, "\mathrm{Frac}"] \arrow[r, shift left, "\texttt{LocalRing.ResidueField}"] \arrow[d, dash, dashed] & \kappa_E \arrow[l, shift left, "\texttt{unramifiedSubalgebra}"] \arrow[d, dash, dashed] \\
K \arrow[r, leftrightarrow] & K_0 \arrow[r, leftrightarrow] & \kappa_K
\end{tikzcd}
$$

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

def unramifiedSubalgebra_gi (Etale K₀ L₀) : 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`

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