Formalizing Local Fields in Lean

María Inés de Frutos-Fernández

Universidad Autónoma de Madrid

joint work with

Filippo A. E. Nuccio

Université Jean Monnet Saint-Étienne

8 February 2024

XVI Summer Workshop in Mathematics, Universidade de Brasília

Table of Contents

General motivation

Fermat's Last Theorem

- Last theorem on Freek's list.
- Formulated around 1637.
- Proven by Wiles and Taylor in 1995.
- Proof uses elliptic curves, modular forms, Galois representations, class field theory...

General motivation

Fermat's Last Theorem

- Last theorem on Freek's list.
- Formulated around 1637.
- Proven by Wiles and Taylor in 1995.
- Proof uses elliptic curves, modular forms, Galois representations, class field theory...

The Langlands Program

- Collection of deep conjectures relating number theory and geometry.
- One of the largest research programs in modern mathematics.

Number Theory in Lean

- p-adic numbers (R. Lewis, 2019).
- Perfectoid spaces (J. Commelin, K. Buzzard, P. Massot, 2020)
- Witt vectors (J. Commelin, R.Lewis, 2021).
- Dedekind domains and class groups (A. Baanen, S. Dahmen, A. Narayanan, F. Nuccio, 2021).
- Adèles and idèles (M. I. de Frutos-Fernández, 2022).
- Modular forms (C. Birkbeck, 2022).
- Elliptic curves (D. Angdinata, K. Buzzard, J. Xu, 2023).
- Group and Galois cohomology (A. Livingston, 2023/Ongoing).
- Iwasawa Theory (A. Narayanan, 2023).
- FLT for regular primes (R. Brasca et. al., 2023).
- Local Class Field Theory (M. I. de Frutos-Fernández, F. Nuccio).
- Divided powers (A. Chambert-Loir, M. I. de Frutos-Fernández).
- ...

Motivation (I)

Example

Find the integral solutions to $X^2 + Y^2 + Z^2 = 0$.

- Positivity $\implies$ $(0,0,0)$ unique solution in $\mathbb{R}$ $\implies$ $(0,0,0)$ unique solution in $\mathbb{Z}$.

Motivation (II)

Example

Find the integral solutions to $X^2 + Y^2 - 3Z^2 = 0$.

- It has nontrivial solutions in $\mathbb{R}$, e.g, $(\pm\sqrt{3}, 0, 1)$, $(0, \pm\sqrt{3}, 1)$, ...
- Case analysis $\implies$ no nontrivial solutions in $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.
- Therefore, no nontrivial solutions in $\mathbb{Z}$.

Motivation (III)

Example

Let $(a, b, c) \in \mathbb{Z}^3$ be a solution of $X^2 + Y^2 = Z^2$.
Then abc is a multiple of 4.

- Case analysis in $\mathbb{Z}/4\mathbb{Z}$ (mod 4) does not help.
- Case analysis in $\mathbb{Z}/8\mathbb{Z}$ (mod 8) works.

Upshot

Sometimes working mod p is not enough
$\rightsquigarrow$ we need to consider mod p^2, mod p^3, ...
$\rightsquigarrow$ use the p-adic numbers.

The p-adic numbers.

- $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$.

The p-adic numbers.

- $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$.
- For each prime p, we get a p-adic absolute value $|\cdot|_p$ ("$p^n \longrightarrow 0$ when $n \longrightarrow \infty$").

The p-adic numbers.

- $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$.
- For each prime p, we get a p-adic absolute value $|\cdot|_p$ ("$p^n \longrightarrow 0$ when $n \longrightarrow \infty$").
- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

The p-adic numbers.

- $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$.
- For each prime p, we get a p-adic absolute value $|\cdot|_p$ ("$p^n \longrightarrow 0$ when $n \longrightarrow \infty$").
- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.
- $\mathbb{Q}_p$ is a local field.

Table of Contents

Mixed Characteristic Local Fields

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

```
class mixed_char_local_field (p : out_param(ℕ))
[fact(nat.prime p)] (K : Type*) [field K]
extends algebra (Q_p p) K :=
[to_finite_dimensional : finite_dimensional (Q_p p) K]
```

Equal Characteristic Local Fields

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

```
class eq_char_local_field (p : out_param(ℕ))
[fact(nat.prime p)] (K : Type*) [field K]
extends algebra 𝔽_[p]((X)) K :=
[to_finite_dimensional : finite_dimensional 𝔽_[p]((X)) K]
```

Local Fields

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

Lemma

A mixed characteristic local field is a local field.

Lemma

An equal characteristic local field is a local field.

Table of Contents

Valuations

A valuation v on a ring R is a map $v : R \to \Gamma_0$ to a linearly ordered commutative group with zero Γ_0 such that

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

Example: 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 to a valuation on $\mathbb{Q}$ as $a_p(\frac{r}{s}) = a_p(r) - a_p(s)$.
- Examples : $a_3(18) = 2$, $a_2(5/16) = -4$.
- The function $v_p : \mathbb{Q} \to p^{\mathbb{Z}} \cup \{0\}$ given by $v_p(x) = p^{-a_p(x)}$ is a valuation on $\mathbb{Q}$.
- In Mathlib, we work with an abstraction of $p^{\mathbb{Z}} \cup \{0\}$, the type `with_zero (multiplicative ℤ)`, denoted $\mathbb{Z}_{m0}$.

Discrete valuations

A discrete valuation is a surjective valuation $v\colon K \to \mathbb{Z}_{m0}$ on a field K.

```
class is_discrete (v : valuation K ℤm0) : Prop :=
(surj : function.surjective v)
```

Examples

- *The p-adic valuation on $\mathbb{Q}$ is discrete.*
- *The X-adic valuation on $\mathbb{F}_q(X)$ is discrete.*

Uniformizers (I)

Let K be a field with a valuation $v : K \to \mathbb{Z}_{m0}$.
A uniformizer for the valuation v is an element $\pi \in K$ with additive valuation 1.

```
variables {K : Type*} [field K] (vK : valuation K ℤₘ₀)

def is_uniformizer (π : K) : Prop :=
vK π = (multiplicative.of_add (- 1 : ℤ) : ℤₘ₀)

structure uniformizer :=
(val : vK.integer) -- an element of the unit ball
(valuation_eq_neg_one : is_uniformizer vK val)
```

Uniformizers (II)

A valuation $v : K \to \mathbb{Z}_{m0}$ on a field K is discrete if and only if there exists a uniformizer for v.

```
variables {K : Type*} [field K] (v : valuation K ℤₘ₀)
local notation ‘K₀‘ := v.valuation_subring

lemma is_discrete_of_exists_uniformizer {π : K}
  (hπ : is_uniformizer v π) :
  is_discrete v := ...

lemma exists_uniformizer [is_discrete v] :
  ∃ π : K₀, is_uniformizer v (π : K) := ...
```

Uniformizers (III)

Given a valuation $v : K \to \mathbb{Z}_{m0}$ with a uniformizer π, any nonzero element $r \in K_0$ can be written in the form

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

```
variables {K : Type*} [field K] (v : valuation K ℤₘ₀)
lemma pow_uniformizer {r : K₀} (hr : r ≠ 0)
  (π : uniformizer v) :
  ∃ n : ℕ, ∃ u : K₀ˣ, r = π.1^n * u := ...
```

The maximal ideal of K_0 is generated by any uniformizer.

```
lemma uniformizer_is_generator (π : uniformizer v) :
maximal_ideal v.valuation_subring = ideal.span {π.1} := ...
```

Local Fields

A local field K is a field complete with respect to a discrete valuation and with finite residue field.

- The discrete valuation on K induces a topology.
- K is complete (Cauchy sequences converge).

The unit ball

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

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

Example

- The unit ball of $\mathbb{Q}$ with the p-adic valuation is
$$\left\{ \frac{r}{s} \in \mathbb{Q} \,\middle|\, (r, s) = 1 \land p \nmid s \right\}.$$
- The unit ball of $\mathbb{Q}_p$ is $\mathbb{Z}_p$, the ring of p-adic integers.
- The unit ball of $\mathbb{F}_q(\!(X)\!)$ is $\mathbb{F}_q[\![X]\!]$.

The unit ball is a DVR

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

Proposition (Serre's Local Fields, 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.

```
instance dvr_of_is_discrete : discrete_valuation_ring K₀ :=
{ to_is_principal_ideal_ring := integer_is_principal_ideal_ring v,
  to_local_ring := infer_instance,
  not_a_field' := by rw [ne.def, ← is_field_iff_maximal_ideal_eq];
  exact not_is_field v }
```

The maximal ideal of the unit ball

Given a discrete valuation $v : K \to \Gamma_0$, the maximal ideal of K_0 is

$$\mathfrak{m}_v := \{ x \in K \mid v(x) < 1 \}.$$

Example

- The maximal ideal of $\mathbb{Z}_p$ is (p).
- The maximal ideal of $\mathbb{F}_q[\![X]\!]$ is (X).

The fraction field of a DVR

Conversely, the fraction field of a discrete valuation ring A is discretely valued.

```
variables (A : Type*) [comm_ring A] [is_domain A] [discrete_valuation_ring A]

instance : valued (fraction_ring A) ℤₘ₀ :=
(maximal_ideal A).adic_valued

instance : is_discrete (@valued.v (fraction_ring A) _ ℤₘ₀ _ _) :=
 is_discrete_of_exists_uniformizer valued.v
 (valuation_exists_uniformizer (fraction_ring A)
  (maximal_ideal A)).some_spec
```

Local Fields

A local field K is a field complete with respect to a discrete valuation and with finite residue field.

- The residue field $K_0/\mathfrak{m}_v$ of K is finite.

```
class local_field (K : Type*) [field K] extends valued K ℤm0 :=
(complete : complete_space K)
(is_discrete : is_discrete (@valued.v K _ ℤm0 _ _))
(finite_residue_field : fintype (local_ring.residue_field
    ((@valued.v K _ ℤm0 _ _).valuation_subring))
```

Complete fields (I)

Proposition

If K is complete with respect to a discrete valuation v and if L/K is a finite extension, then L has a unique discrete valuation $w\colon L \to \mathbb{Z}_{m0}$ inducing v and L is complete with respect to w.

Proof sketch.

- L has a unique valuation $w' : L \to \mathbb{R}_{\geq 0}$ extending v.
- "w' takes values in $\mathbb{Z}_{m0}^{q}$ for some $q \in \mathbb{Q}^{\times}$".
- So we can normalize w' to obtain $w : L \to \mathbb{Z}_{m0}$.

$\square$

Complete fields (II)

Proposition

If K is complete with respect to a discrete valuation v and if L/K is a finite extension, then the integral closure of K_0 inside L coincides with L_0 and so, in particular, it is a discrete valuation ring.

```
lemma integral_closure_eq_integer [finite_dimensional K L] :
  (integral_closure hv.v.valuation_subring L).to_subring =
  (extension K L).valuation_subring.to_subring := ...
instance discrete_valuation_ring_of_finite_extension
    [finite_dimensional K L] :
 discrete_valuation_ring (integral_closure
   hv.v.valuation_subring L) := ...
```

The ring of integers (I)

We define the ring of integers of a mixed characteristic local field K as the integral closure of $\mathbb{Z}_p$ in K.

```
variables (p : ℕ) [fact(nat.prime p)]
(K : Type*) [field K] [mixed_char_local_field p K]

def ring_of_integers := integral_closure (Z_p p) K -- 𝒪 p K
```

Recall that we have shown that this ring of integers is isomorphic to the unit ball K_0 of K, and that it is a discrete valuation ring.

The ring of integers (II)

We define the ring of integers of an equal characteristic local field K as the integral closure of $\mathbb{F}_p[\![X]\!]$ in K.

```
variables (p : ℕ) [fact(nat.prime p)]
(K : Type*) [field K] [eq_char_local_field p K]

def ring_of_integers := integral_closure 𝔽_[p]⟦X⟧ K -- 𝒪 p K
```

Again, the ring of integers is a discrete valuation ring.

Localization (I)

Let R be a Dedekind domain (that is not a field), $K = \mathrm{Frac}(R)$, $\mathfrak{p}$ a maximal ideal of R.

- E. g., $R = \mathbb{Q}$, $\mathbb{F}_p(X)$, a number field, a function field...

The completion $K_{\mathfrak{p}}$ has a discrete valuation extending the valuation $v_{\mathfrak{p}}$.

In particular, $K_{\mathfrak{p}0}$ is a discrete valuation ring.

Localization (II)

```
variables (R : Type*) [comm_ring R] [is_domain R] [is_dedekind_domain R]
(K : Type*) [field K] [algebra R K] [is_fraction_ring R K]
(v : height_one_spectrum R)

local notation `R_v` :=
is_dedekind_domain.height_one_spectrum.adic_completion_integers K v
local notation `K_v` :=
is_dedekind_domain.height_one_spectrum.adic_completion K v

lemma valuation_completion_integers_exists_uniformizer :
∃ (π : R_v), valued.v (π : K_v) = (multiplicative.of_add ((-1 : ℤ))) := ...

instance : is_discrete (@valued.v K_v _ ℤₘ₀ _ _) :=
is_discrete_of_exists_uniformizer _
(valuation_completion_integers_exists_uniformizer R K v).some_spec

instance : discrete_valuation_ring R_v :=
disc_valued.discrete_valuation_ring K_v
```

Localization (III)

$K_{\mathfrak{p}}$ has a valuation extending the valuation on K.

```
local notation ‘v_compl_of_adic‘ :=
(valued.v : valuation K_v ℤm0)
```

Since $K_{\mathfrak{p}0}$ is a discrete valuation ring, we can also endow $K_{\mathfrak{p}}$ with the adic topology generated by the maximal ideal of $K_{\mathfrak{p}0}$.

```
local notation ‘v_adic_of_compl‘ :=
is_dedekind_domain.height_one_spectrum.valuation K_v
    (max_ideal_of_completion R v K)
```

We prove that both valuations agree:

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

Table of Contents

Project at a glance

- Master's level number theory results.
- $\sim 8k$ lines of Lean 3 code.
- We used algebra, topology, analysis, ... results from `mathlib`.
- Now being ported to Lean 4.

The p-adic numbers

Mathlib's p-adic numbers:

```
def padic (p : ℕ) [fact p.prime] :=
@cau_seq.completion.Cauchy _ _ _ _ (padic_norm p) _ -- ℚ_[p]
def padic_int (p : ℕ) [fact p.prime] :=
{x : ℚ_[p] // ‖x‖ ≤ 1} -- ℤ_[p]
```

Our definition:

```
def Q_p : Type* := adic_completion ℚ (p_height_one_ideal p)
def Z_p := (@valued.v (Q_p p) _ ℤₘ₀ _ _).valuation_subring
```

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

```
def padic_equiv : (Q_p p) ≃+* ℚ_[p] := ...
def padic_int_ring_equiv : (Z_p p) ≃+* ℤ_[p] := ...
```

Laurent Series

```
variables (p : ℕ) [fact(nat.prime p)]
def FpX_completion :=
(ideal_X 𝔽_[p]).adic_completion (ratfunc 𝔽_[p]) -- 𝔽_[p]((X))
def FpX_int_completion := -- 𝔽_[p]⟦X⟧
(ideal_X 𝔽_[p]).adic_completion_integers (ratfunc 𝔽_[p])
```

We provide an isomorphism between $K((X))$ and the field `laurent_series K`.

```
def laurent_series_ring_equiv :
(completion_of_ratfunc K) ≃+* (laurent_series K) := ...
```

Extensions and valued instances

If K is complete with respect to a discrete valuation v and L/K is a finite extension, we have defined a discrete valuation on L.

We do not turn it into a `valued L` $\mathbb{Z}_{m0}$ instance to avoid diamonds.

```
lemma trivial_extension_eq_valuation :
  extended_valuation K K = hv.v :=
```

We make exceptions for mixed/equal characteristic local fields.

Table of Contents

Local Class Field Theory

Local class field theory: branch of number theory that studies the abelian extensions of a local field.

Used in the proof of Fermat's Last Theorem.

First case of the Langlands conjectures.

Proof uses ramification theory, cohomology theory, class formations, ...

Thanks for listening! Questions?

María Inés de Frutos-Fernández, Filippo Alberto Edoardo Nuccio Mortarino Majno Di Capriglio, “A Formalization of Complete Discrete Valuation Rings and Local Fields”. CPP 2024. https://doi.org/10.1145/3636501.3636942

https://github.com/mariainesdff/local_class_field_theory