Formalizing Norm Extensions and Applications to Number Theory

María Inés de Frutos-Fernández

Imperial College London/Universidad Autónoma de Madrid

February 16, 2023

Machine Assisted Proofs, IPAM

Outline

1. Motivation.
2. Norms and extensions.
3. Application: Fontaine's period rings.

Motivation for this project : $\mathbb{C}_p$.

- $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$.
- $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. It is complete with respect to $|\cdot|$.

Motivation for this project : $\mathbb{C}_p$.

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

Motivation for this project : $\mathbb{C}_p$.

- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Motivation for this project : $\mathbb{C}_p$.

- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.
- Is $\mathbb{Q}_p^{\text{alg}}$ the analogue of $\mathbb{C}$?

Motivation for this project : $\mathbb{C}_p$.

- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.
- Is $\mathbb{Q}_p^{\text{alg}}$ the analogue of $\mathbb{C}$?
  - $\mathbb{Q}_p^{\text{alg}}$ is algebraically closed.
  - $|\cdot|_p$ extends uniquely to $\mathbb{Q}_p^{\text{alg}}$ (more on this later).
  - However, $\mathbb{Q}_p^{\text{alg}}$ is not complete with respect to $|\cdot|_p$.

Motivation for this project : $\mathbb{C}_p$.

- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.
- Is $\mathbb{Q}_p^{\text{alg}}$ the analogue of $\mathbb{C}$?
  - $\mathbb{Q}_p^{\text{alg}}$ is algebraically closed.
  - $|\cdot|_p$ extends uniquely to $\mathbb{Q}_p^{\text{alg}}$ (more on this later).
  - However, $\mathbb{Q}_p^{\text{alg}}$ is not complete with respect to $|\cdot|_p$.
- Define $\mathbb{C}_p$ as the completion of $\mathbb{Q}_p^{\text{alg}}$ with respect to $|\cdot|_p$.
  - $\mathbb{C}_p$ is complete with respect to $|\cdot|_p$ and algebraically closed.

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).
- Elliptic curves (D. Angdinata, K. Buzzard, J. Xu).
- Modular forms (C. Birkbeck).
- Group and Galois cohomology (A. Livingston).
- Iwasawa Theory (A. Narayanan).
- FLT for regular primes (R. Brasca et. al.).
- Local Class Field Theory (M. I. de Frutos-Fernández, F. Nuccio).
- Divided powers (A. Chambert-Loir, M. I. de Frutos-Fernández).
- ...

Nonarchimedean norms

Let R be a ring.

A multiplicative ring norm (or absolute value) on R is a function $|\cdot| : R \to \mathbb{R}$ such that

1. $|r| \geq 0$ for all r in R,
2. $|r| = 0$ if and only if $r = 0$ for all r in R,
3. $|r + s| \leq |r| + |s|$ for all r, s in R, and
4. $|rs| = |r||s|$ for all r, s in R.

Nonarchimedean norms

Let R be a ring.

A nonarchimedean multiplicative ring norm on R is a function $|\cdot| : R \to \mathbb{R}$ such that

1. $|r| \geq 0$ for all r in R,
2. $|r| = 0$ if and only if $r = 0$ for all r in R,
3. $|r + s| \leq \max\{|r|, |s|\}$ for all r, s in R, and
4. $|rs| = |r||s|$ for all r, s in R.

Nonarchimedean norms

Let R be a ring.

A nonarchimedean ~~multiplicative~~ ring norm (or absolute value) on R is a function $|\cdot| : R \to \mathbb{R}$ such that

1. $|r| \geq 0$ for all r in R,
2. $|r| = 0$ if and only if $r = 0$ for all r in R,
3. $|r + s| \leq \max\{|r|, |s|\}$ for all r, s in R, and
4. $|rs| \leq |r||s|$ for all r, s in R.

A norm is power multiplicative if $|r^n| = |r|^n \ \forall r \in R, n \in \mathbb{N}_{\geq 1}$.

R-algebra norms

Let R be a commutative ring with a norm $|\cdot|$ and let A be an R-algebra.

An *R-algebra norm* on A is a norm $\|\cdot\|$ on A such that $\|r \cdot a\| = |r| \cdot \|a\|$ for all $r \in R, a \in A$.

Question

The p-adic norm $|\cdot|_p$ on $\mathbb{Q}_p$ is a nonarchimedean multiplicative norm. We want to show that $|\cdot|_p$ extends uniquely to $\mathbb{Q}_p^{\text{alg}}$.

If K is a field with a nonarchimedean norm $|\cdot|$ and L/K is a field extension, can we extend $|\cdot|$ to L? Is this extension unique?

Question

The p-adic norm $|\cdot|_p$ on $\mathbb{Q}_p$ is a nonarchimedean multiplicative norm. We want to show that $|\cdot|_p$ extends uniquely to $\mathbb{Q}_p^{\text{alg}}$.

If K is a field with a nonarchimedean norm $|\cdot|$ and L/K is a field extension, can we extend $|\cdot|$ to L? Is this extension unique?

- Yes, under some conditions on $K, |\cdot|$, and L.
- Ref: "Non-Archimedean Analysis" by Bosch, Güntzer, and Remmert (BGR).

Extension Theorems (I)

Theorem (Extension Theorem, BGR 3.2.1/2)

Let K be a field with a nonarch. pow-mult. norm $|\cdot|$, L/K an algebraic extension, and $G(L/K)$ the group of K-algebra automorphisms of L.

- *The spectral norm $|\cdot|_{sp}$ on L is a nonarch. pow-mult. K-algebra norm on L extending the norm $|\cdot|$ on K.*
- *If L/K is finite and normal and $\|\cdot\|$ is a nonarch. pow-mult. K-algebra norm on L extending $|\cdot|$, then $|x|_{sp} = \max_{g \in G(L/K)} \|g(x)\|$ for all $x \in L$.*

Extension Theorems (II)

Theorem (Unique Extension Theorem, BGR 3.2.4/2)

Let K be a field that is complete with respect to a nonarchimedean multiplicative norm $|\cdot|$ and let L/K be an algebraic extension. Then the spectral norm on L is the unique multiplicative nonarchimedean norm on L extending the norm $|\cdot|$ on K.

$\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$, so $|\cdot|_p$ extends uniquely to $\mathbb{Q}_p^{\text{alg}}$.

$\mathbb{C}_p$ is defined as the completion of $\mathbb{Q}_p^{\text{alg}}$ with respect to $|\cdot|_p$.

The Spectral Norm

Let K be a field with a nonarchimedean norm $|\cdot|$, and let L/K be an algebraic extension.

- For each monic $q := X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$, define the spectral value $\sigma(q)$ of q as

$$\sigma(q) := \max_{0 \leq i < n} |a_i|^{1/(n-i)}.$$

- The spectral norm $|\cdot|_{\text{sp}}$ on L is the function $|\cdot|_{\text{sp}} : L \to \mathbb{R}_{\geq 0}$ given by $|y|_{\text{sp}} :=$ spectral value of the minimal polynomial of y over K.

Proof of the extension theorems (I)

Lemma

Let K be a field with a nonarch. pow.-mult. norm $|\cdot|$. Each finite extension L/K has at least one nonarch. pow.-mult. K-algebra norm extending $|\cdot|$.

Sketch of Proof.

- Define $\|\sum_{i=1}^{n} a_i e_i\| := \max_i |a_i|$, $\{e_1 = 1, \ldots, e_n\}$ fixed basis of L/K.
- Facts: $\|0\| = 0$, $\|x - y\| \leq \max\{\|x\|, \|y\|\}$, and $\exists M \in \mathbb{R}_{>0}$ s.t. $\|xy\| \leq M\|x\|\|y\|$ for all $x, y \in L$.
- Smoothing Step 1 (BGR Prop. 1.2.1/2): There exists a K-algebra norm on L extending $|\cdot|$.
- Smoothing Step 2 (BGR Prop. 1.3.2/1): There exists a power multiplicative K-algebra norm on L extending $|\cdot|$. Needs nonarchimedean $|\cdot|$.

Proof of the extension theorems (II)

Proof of the Extension Theorem.

- We may assume L/K is finite and normal (e.g., to check $|xy|_{\mathrm{sp}} \leq |x|_{\mathrm{sp}}|y|_{\mathrm{sp}}$, we can work on the normal closure of $K(x, y)$).
- By the previous Lemma, $\exists$ pow.-mult. K-algebra norm $\|\cdot\|$ on L extending $|\cdot|$.
- Smoothing Step 3: Define $|y|_G := |y|_{G(L/K)} := \max_{g \in G(L/K)} \|g(y)\|$.
- $|y|_G$ is a pow.-mult. K-algebra norm $\|\cdot\|$ on L extending $|\cdot|$.
- All $g \in G(L/K)$ are isometries with respect to $|\cdot|_G$.
- The minpoly q_y of $y \in L$ is of the form $q_y = \prod (X - g(y))^{p^e}$.
- Use BGR Prop. 3.1.2/1 to conclude $|y|_G = |y|_{\mathrm{sp}}$.

Proof of the extension theorems (III)

Proof of the Unique Extension Theorem.

Check uniqueness:

- Let $\|\cdot\|$ be a pow.-mult. K-algebra norm on L extending $|\cdot|$. By BGR Prop. 3.1.5/1, it suffices to check $\|\cdot\|$ and $|\cdot|$ are equivalent on each $K(y), y \in L$.
- This follows from K complete and $K(y)$ finite dimensional over K.

Check $|\cdot|_{\mathrm{sp}}$ is multiplicative:

- Fix $y \in L$.
- Smoothing Step 4 (BGR Prop 1.3.2/2): There is a pow.-mult. K-algebra norm $|\cdot|_y$ on L such that y is multiplicative for $|\cdot|_y$.
- Hence $|\cdot|_{\mathrm{sp}} = |\cdot|_y$, so y is multiplicative for $|\cdot|_{\mathrm{sp}}$.

Unbundling (semi)norms

In our discussion, K has a preferred norm, so we can use `mathlib`'s class `normed_field`.

```
variables {K : Type*} [normed_field K]
```

However, we need to consider several norms on L. I introduced new unbundled versions of norms (and seminorms): `ring_norm`, ring_seminorm, etc.

```
variables {L : Type*} [field L] (f g : mul_ring_norm L)
```

Relating norms and valuations (I)

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

We say that $v : R \to \Gamma_0$ has rank 1 if it is nontrivial and there exists an injective morphism of linear ordered groups with zero $\Gamma_0 \to \mathbb{R}_{\geq 0}$.

Relating norms and valuations (II)

Nontrivial nonarchimedean norms correspond to rank 1 valuations.

I created a translation between both notions in Lean:

```
def normed_field.to_valued {K : Type*} [normed_field K]
  (h : is_nonarchimedean (norm : K → ℝ)) : valued K ℝ≥0 := ...
```

```
def valued_field.to_normed_field {L : Type*} [field L]
  {Γ₀ : Type*} [linear_ordered_comm_group_with_zero Γ₀]
  [val : valued L Γ₀] [hv : is_rank_one val.v] :
  normed_field L := ...
```

Galois Representations

Let K be a p-adic field (e.g., $K = \mathbb{Q}_p$) and denote $G_K := \mathrm{Gal}(K^{\mathrm{alg}}/K)$.
A p-adic Galois representation is a continuous group homomorphism $\rho : G_K \to \mathrm{GL}(V)$, where V is a finite dim. $\mathbb{Q}_p$-vector space.

- E.g., $H^i_{\text{ét}}(X_{K^{\mathrm{alg}}}, \mathbb{Q}_p)$ for X/K a proper, smooth variety.

Galois Representations

Let K be a p-adic field (e.g., $K = \mathbb{Q}_p$) and denote $G_K := \mathrm{Gal}(K^{\mathrm{alg}}/K)$.
A p-adic Galois representation is a continuous group homomorphism $\rho : G_K \to \mathrm{GL}(V)$, where V is a finite dim. $\mathbb{Q}_p$-vector space.

- E.g., $H^i_{\text{ét}}(X_{K^{\mathrm{alg}}}, \mathbb{Q}_p)$ for X/K a proper, smooth variety.

Conjecture (Fontaine–Mazur)

Fix a number field F and a prime number p. Let V be a finite dimensional p-adic representation of $\mathrm{Gal}(F^{alg}/F)$ such that

1. *For almost all primes $\mathfrak{p} \in \mathcal{O}_F$, V is unramified at p.*
2. *For all primes $\mathfrak{p}$ above p, the representation $V_{|Gal(F^{alg}_{\mathfrak{p}}/F_{\mathfrak{p}})}$ is de Rham.*

Then V appears as a subquotient of some $H^i_{ét}(X_{F^{alg}}, \mathbb{Q}_p)(\chi^m_{cycl})$, where $i \in \mathbb{Z}_{\geq 0}$, X is a proper smooth variety over F and $m \in \mathbb{Z}$.

Fontaine's period rings

Fontaine's period rings are topological $\mathbb{Q}_p$-algebras B,

- with a continuous linear action of G_K,
- with some compatible additional structures (e.g. a Frobenius map, a filtration, etc.),
- such that B^{G_K} is a field, and
- the B^{G_K}-vector space $D_B(V) = (B \otimes_{\mathbb{Q}_p} V)^{G_K}$ is an interesting invariant of the Galois rep. V.

V is B-admissible if $\dim_{B^{G_K}} D_B(V) = \dim_{\mathbb{Q}_p} V$.

Fontaine's period rings: Examples ($K = \mathbb{Q}_p$)

1. $B = K^{\mathrm{alg}}$. Then V is K^{alg}-admissible $\iff$ the G_K action on V factors through a finite quotient.
2. $B = \mathbb{C}_p$. Then V is $\mathbb{C}_p$-admissible $\iff$ the action of I_K on V factors through a finite quotient.
3. $B = B_{\mathrm{HT}} := \mathbb{C}_p[X, X^{-1}]$. Then V is B_{HT}-admissible (or Hodge-Tate) $\iff$ $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V \equiv \mathbb{C}_p(\chi_{\mathrm{cycl}}^{n_1}) \oplus \cdots \oplus \mathbb{C}_p(\chi_{\mathrm{cycl}}^{n_d})$ for some $n_i \in \mathbb{Z}$.

```
@[derive comm_ring]
def Cp_x_y := mv_polynomial (fin 2) ℂ_[p]
def B_HT := (Cp_x_y  p) / (ideal.span {(X 0 * X 1 - 1)} :
    ideal (Cp_x_y  p))
```

4. $B = B_{\mathrm{dR}}$. V is de Rham if it is B_{dR}-admissible.

Definition of B_{dR} (I)

Define $E := \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/(p)$.

```
def E := ring.perfection (𝒪_ℂ_[p] / (ideal.span{p} : ideal 𝒪_ℂ_[p])) p
```

Let $A_{\mathrm{inf}} := W(E)$ be the ring of Witt vectors of E.

```
def A_inf := witt_vector p (E p)
```

$B^+_{\mathrm{inf}} := A_{\mathrm{inf}}[\frac{1}{p}]$

```
def B_inf_plus := localization.away (p : A_inf p)
```

Definition of B_{dR} (II)

There is a canonical surjective homomorphism $\theta : B_{\mathrm{inf}}^{+} \to \mathbb{C}_p$. B_{dR}^{+} is the completion of B_{inf}^{+} with respect to the ideal $\ker(\theta)$.

```
def B_dR_plus := adic_completion (theta p).ker (B_inf_plus p)
```

B_{dR} is the field of fractions of B_{dR}^{+}.

```
def B_dR := fraction_ring (B_dR_plus p)
```

Questions

Thanks for listening! Questions?

https://mariainesdff.github.io/