Formalizing Mathematics in Lean.

4. Number Theory in Lean: an (Incomplete) Overview

María Inés de Frutos Fernández

Universidad Autónoma de Madrid

21/07/2023

6th EACA International School on Computer Algebra and its Applications

Santiago de Compostela

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, J. Xu, 2023).
- Group and Galois cohomology (A. Livingston, 2023; ongoing).
- Iwasawa Theory (A. Narayanan, 2023*).
- Norm extensions and $\mathbb{C}_p$ (M. I. de Frutos-Fernández, 2023).
- FLT for regular primes (R. Brasca et. al, 2023; ongoing).
- Local Class Field Theory (M. I. de Frutos-Fernández, F. Nuccio).
- Divided powers (A. Chambert-Loir, M. I. de Frutos-Fernández).
- ...

Outline

Norms and Valuations

Nonarchimedean norms

Let R be a ring.

A nonarchimedean multiplicative ring norm (or nonarchimedean 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. $|rs| = |r||s|$ for all r, s in R.

If R is a commutative ring with a (nonarchimedean) norm $|\cdot|$ and A is 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 $r \in R, a \in A$.

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

Example: the p-adic valuation

- If $R = \mathbb{Z}$ and p is a prime number, the additive p-adic valuation a_p of $r \in \mathbb{Z}$ is $a_p(r) := \max\{\, n \in \mathbb{Z} \mid p^n \text{ divides } r \,\}$.
- Extend to a valuation on $\mathbb{Q}$ as $a_p(\frac{r}{s}) = a_p(r) - a_p(s)$.
- Examples : $a_3(18) = 2$, $a_3(5/27) = -3$.
- 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 $\mathbb{Z}_{m0}$.

The p-adic Numbers

Reference: R. Lewis, *A Formal Proof of Hensel's Lemma over the p-Adic Integers* [5].

The p-Adic Numbers in Mathlib

The p-adic numbers are defined in Lean as the Cauchy completion ℚ_[p] of $\mathbb{Q}$ with respect to the p-adic norm.

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

instance field : Field ℚ_[p] := Cauchy.field
instance normedField : NormedField ℚ_[p] := ...
instance : CompleteSpace ℚ_[p] := ...
instance : CharZero ℚ_[p] := ...

theorem nonarchimedean (q r : ℚ_[p]) :
  ‖q + r‖ ≤ max ‖q‖ ‖r‖ := ...

theorem rat_dense (q : ℚ_[p]) {ε : ℝ} (hε : 0 < ε) :
  ∃ r : ℚ, ‖q - r‖ < ε := ...
```

The p-Adic Integers

The p-adic integers $\mathbb{Z}$_[p] are defined as the subtype of $\mathbb{Q}$_[p] consisting of p-adic numbers with norm ≤ 1.

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

def subring : Subring ℚ_[p] where
  carrier := { x : ℚ_[p] | ‖x‖ ≤ 1 }
  ...

instance completeSpace : CompleteSpace ℤ_[p] := ...
instance : NormedCommRing ℤ_[p] := ...
instance : DiscreteValuationRing ℤ_[p] :=
instance isFractionRing : IsFractionRing ℤ_[p] ℚ_[p]  := ...
```

Hensel's Lemma

```
theorem hensels_lemma {p : ℕ} [inst : Fact (Nat.Prime p)]
   {F : Polynomial ℤ_[p]} {a : ℤ_[p]}
   (hnorm : ‖F.eval a‖ < ‖F.derivative.eval a‖ ^ 2) :
   ∃ z : ℤ_[p],
     F.eval z = 0 ∧ ‖z - a‖ < ‖F.derivative.eval a‖ ∧
     ‖F.derivative.eval z‖ = ‖F.derivative.eval a‖ ∧
      ∀ z', F.eval z' = 0 → ‖z' - a‖ < ‖F.derivative.eval a‖ →
        z' = z :=
  if ha : F.eval a = 0 then ⟨a, a_is_soln hnorm ha⟩
  else by
    exact ⟨soln_gen hnorm, eval_soln hnorm,
      soln_dist_to_a_lt_deriv hnorm ha, soln_deriv_norm hnorm,
      fun z => soln_unique hnorm ha z⟩
-- The file containing the whole proof is ∼500 lines long
```

The p-adic Complex Numbers

Reference: M. I. de Frutos Fernández, *Formalizing Norm Extensions and Applications to Number Theory* [3].

$\mathbb{C}_p$ (I)

- $\mathbb{R}$ 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 $|\cdot|$.

$\mathbb{C}_p$ (I)

- $\mathbb{R}$ 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 have the p-adic norm $|\cdot|_p$ ("$p^n \longrightarrow 0$ when $n \longrightarrow \infty$").
- What is the p-adic analogue of $\mathbb{C}$?

$\mathbb{C}_p$ (II)

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

$\mathbb{C}_p$ (II)

- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.
- Consider $\mathbb{Q}_p^{\text{alg}}$:

$\mathbb{C}_p$ (II)

- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.
- Consider $\mathbb{Q}_p^{\text{alg}}$:
  - $\mathbb{Q}_p^{\text{alg}}$ is algebraically closed.
  - $|\cdot|_p$ **extends uniquely to** $\mathbb{Q}_p^{\text{alg}}$**.**
  - However, $\mathbb{Q}_p^{\text{alg}}$ is not complete with respect to $|\cdot|_p$.

$\mathbb{C}_p$ (II)

- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.
- Consider $\mathbb{Q}_p^{\text{alg}}$:
  - $\mathbb{Q}_p^{\text{alg}}$ is algebraically closed.
  - $|\cdot|_p$ **extends uniquely to** $\mathbb{Q}_p^{\text{alg}}$**.**
  - 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.

Strategy 1

Theorem

Let K be a field complete with respect to a discrete norm $|\cdot|_K$ and let L be a separable extension of K. Then $|\cdot|_K$ extends uniquely to a discrete absolute value $|\cdot|_L$ on L. If $n := [L : K] < \infty$, then

$$|x|_L := |Nm_{L/K}(x)|_K^{1/n}$$

Sketch of Proof.

- Reduce to case $n := [L : K]$ finite.
- $\{$Extensions of $|\cdot|_K\} \leftrightarrow \{$Ideals over maximal ideal$\}$
- Use Hensel's lemma to conclude uniqueness.
- For a Galois closure L' of L,

$$|Nm(x)|_K = \left|\prod \sigma(x)\right|_{L'} = |x|_L^n.$$

$\square$

Unique Extension Theorem

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 $|\cdot|_p$.

Ref: "Non-Archimedean Analysis" by Bosch, Güntzer, and Remmert (BGR).

The Spectral Norm (I)

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

- For each monic $q := X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$, 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.

The Spectral Norm (II)

```
variables {R : Type*} [semi_normed_ring R]

def spectral_value_terms (p : R[X]) : ℕ → ℝ :=
λ (n : ℕ), if n < p.nat_degree
 then ‖ p.coeff n ‖^(1/(p.nat_degree - n : ℝ)) else 0

def spectral_value (p : R[X]) : ℝ := supr (spectral_value_terms p)

variables (K L : Type*) [normed_field K] [field L] [algebra K L]

def spectral_norm (y : L) : ℝ := spectral_value (minpoly K y)
```

Proof of the extension theorems

- Described in Chapters 1–3 of BGR.
- Strategy:
  - Reduce to finite normal extensions.
  - Start with a candidate function for the extension norm and modify it (four times) to get a nonarchimedean K-algebra norm extending the norm on K.
- $\sim$5,000 lines of Lean code.

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

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

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 := ...
```

Dedekind Domains and Class Groups

Reference: A. Baanen, S. R. Dahmen, A. Narayanan, and F. A. E. Nuccio, *A Formalization of Dedekind Domains and Class Groups of Global Fields* [1].

Dedekind domains

Three equivalent definitions:

```
class IsDedekindDomain (A : Type u_1) [inst : CommRing A]
   [inst : IsDomain A] : Prop where
  isNoetherianRing : IsNoetherianRing A
  dimensionLEOne : DimensionLEOne A
  isIntegrallyClosed : IsIntegrallyClosed A

def IsDedekindDomainInv (A : Type u_1) [inst : CommRing A]
   [inst : IsDomain A] : Prop :=
  ∀ (I) (_ : I ≠ (⊥ : FractionalIdeal A⁰ (FractionRing A))),
    I * I⁻¹ = 1

structure IsDedekindDomainDvr (A : Type u_1) [inst : CommRing A]
   [inst : IsDomain A] : Prop where
  isNoetherianRing : IsNoetherianRing A
  is_dvr_at_nonzero_prime :
    ∀ (P) (_ : P ≠ (⊥ : Ideal A)) (_ : P.IsPrime),
      DiscreteValuationRing (Localization.AtPrime P)
```

(Fractional) Ideals in Dedekind domains

Every nonzero ideal in a Dedekind domain is uniquely representable as a product of prime ideals (up to ordering).

```
instance Ideal.uniqueFactorizationMonoid {A : Type u_1}
   [inst : CommRing A] [inst : IsDomain A]
   [inst : IsDedekindDomain A]  :
  UniqueFactorizationMonoid (Ideal A) := ...
```

The ideal class group of a ring R is the group of invertible fractional ideals modulo the principal ideals.

```
def ClassGroup (R : Type u_1) [inst : CommRing R]
   [inst : IsDomain R] :=
(FractionalIdeal R⁰ (FractionRing R))ˣ / (toPrincipalIdeal R
    (FractionRing R)).range
```

Global Fields

Reference: A. Baanen, S. R. Dahmen, A. Narayanan, and F. A. E. Nuccio, *A Formalization of Dedekind Domains and Class Groups of Global Fields* [1].

Number Fields (I)

A number field is a field which has characteristic zero and is finite dimensional over $\mathbb{Q}$.

```
class NumberField (K : Type _) [Field K] : Prop where
  [to_charZero : CharZero K]
  [to_finiteDimensional : FiniteDimensional ℚ K]
```

The ring of integers of a number field K is the integral closure of $\mathbb{Z}$ in K.

```
def ringOfIntegers := integralClosure ℤ K

instance : IsDedekindDomain (𝒪 K) :=
IsIntegralClosure.isDedekindDomain ℤ ℚ K _

instance [NumberField K] : IsFractionRing (𝒪 K) K :=
integralClosure.isFractionRing_of_finite_extension ℚ _
```

Number Fields (II)

The class number of a number field is finite.

```
variable  (K : Type u_1) [inst : Field K] [inst : NumberField K]

instance : Fintype (ClassGroup (ringOfIntegers K)) :=
ClassGroup.fintypeOfAdmissibleOfFinite ℚ K
    AbsoluteValue.absIsAdmissible

noncomputable def classNumber : ℕ :=
Fintype.card (ClassGroup (ringOfIntegers K))
```

Function Fields

A function field is a finite field extension of $\mathbb{F}_p(X)$ for some prime p. In Mathlib's definition, $\mathbb{F}_p$ is replaced by any field.

```
class FunctionField [Algebra (RatFunc Fq) F] (Fq : Type)
   (F : Type) [inst : Field Fq] [inst : Field F]
   [inst : Algebra (RatFunc Fq) F] : Prop :=
  FiniteDimensional (RatFunc Fq) F
```

Analogous results to the number field case.

The Ring of Adèles of a Global Field

Reference: M. I. de Frutos Fernández, *Formalizing the Ring of Adèles of a Global Field* [2].

The Ring of Adèles of a Number Field (I)

- Let K be a number field. The ring of adèles of K is

$$\mathbb{A}_K := \prod_v{}' K_v := \{(x_v)_v \mid x_v \in \mathcal{O}_v \text{ a. e.}\},$$

  where v runs over all the places of K.
- We can separate archimedean and nonarchimedean places.
- $\mathbb{A}_K = \prod_{v \text{ nonarch.}}{}' K_v \times \prod_{v \text{ arch.}} K_v = \mathbb{A}_{K,f} \times \prod_{v \text{ arch.}} K_v = \mathbb{A}_{K,f} \times (\mathbb{R} \otimes_{\mathbb{Q}} K)$.

The Ring of Adèles of a Number Field (II)

- $\mathbb{A}_{K,f} = \prod_v' K_v \simeq K \otimes \prod_v \mathcal{O}_v \simeq \left(\prod_v \mathcal{O}_v\right)\left[\frac{1}{\mathcal{O}_K \setminus \{0\}}\right] \simeq K \otimes \mathbb{A}_{\mathbb{Q},f}$, where v runs over the maximal ideals of $\mathcal{O}_K$.

The Ring of Adèles of a Number Field (II)

- $\mathbb{A}_{K,f} = \prod_v' K_v \simeq K \otimes \prod_v \mathcal{O}_v \simeq \left(\prod_v \mathcal{O}_v\right)\left[\frac{1}{\mathcal{O}_K \setminus \{0\}}\right] \simeq K \otimes \mathbb{A}_{\mathbb{Q},f}$, where v runs over the maximal ideals of $\mathcal{O}_K$.

- With the 3^{rd} def., we get the topological ring structure 'for free'.

- However, it's easier to prove results using the 1^{st} definition.

The Ring of Adèles of a Number Field (II)

- $\mathbb{A}_{K,f} = \prod_v' K_v \simeq K \otimes \prod_v \mathcal{O}_v \simeq \left(\prod_v \mathcal{O}_v\right)\left[\frac{1}{\mathcal{O}_K \setminus \{0\}}\right] \simeq K \otimes \mathbb{A}_{\mathbb{Q},f}$, where v runs over the maximal ideals of $\mathcal{O}_K$.
- With the 3rd def., we get the topological ring structure 'for free'.
- However, it's easier to prove results using the 1st definition.
- Note: $\mathbb{A}_{R,f} := \prod_{v \text{ max.}}' F_v$ can be defined for any Dedekind domain R with field of fractions F.

Dedekind domains and valuations (I)

If R is a Dedekind domain of Krull dimension one, the maximal ideals are the nonzero prime ideals of R.

```
structure HeightOneSpectrum (R : Type u_1) [inst : CommRing R] where
  asIdeal : Ideal R
  isPrime : asIdeal.IsPrime
  ne_bot : asIdeal ≠ ⊥
```

We can define the v-adic valuation on $K := \mathrm{Frac}(R)$, the completion K_v and its ring of integers R_v.

```
variable {R : Type u_1} [inst : CommRing R] [inst : IsDomain R]
  [inst : IsDedekindDomain R] (K : Type u_2) [inst : Field K]
  [inst : Algebra R K] [inst : IsFractionRing R K]
  (v : IsDedekindDomain.HeightOneSpectrum R)
def adicValued : Valued K ℤm0 := Valued.mk' v.valuation
def adicCompletion :=
@UniformSpace.Completion K v.adicValued.toUniformSpace -- K_v
def adicCompletionIntegers : ValuationSubring (v.adicCompletion K) :=
Valued.v.valuationSubring -- R_v
```

Dedekind domains and valuations (II)

Every nonzero fractional ideal I of a Dedekind domain R can be factored as a product $\prod_v v^{n_v}$ over the maximal ideals of R, where the exponents n_v are integers.
If $I = a^{-1}J$ for $a \in R$ and J an ideal of R, then $n_v = val_v(J) - val_v(a)$.

```
lemma fractional_ideal.factorization
  (I : fractional_ideal (non_zero_divisors R) K) (hI : I ≠ 0)
  {a : R} {J : ideal R}
  (haJ : I = fractional_ideal.span_singleton
    (non_zero_divisors R) ((algebra_map R K) a)⁻¹ * ↑J) :
  ∏ᶠ (v : height_one_spectrum R), (v.as_ideal : fractional_ideal
      (non_zero_divisors R) K)^
    ((associates.mk v.as_ideal).count (associates.mk J).factors -
    (associates.mk v.as_ideal).count (associates.mk
      (ideal.span{a})).factors : ℤ) = I :=
```

The finite adèle ring of a Dedekind domain.

- $\mathbb{A}_{R,f} := \prod_v' K_v := \left\{ x := (x_v)_v \in \prod_v K_v \,\middle|\, x_v \in R_v \text{ a. e.} \right\}.$

```
def ProdAdicCompletions :=
∀ v : HeightOneSpectrum R, v.adicCompletion K
def IsFiniteAdele (x : K_hat R K) :=
∀ᶠ v : HeightOneSpectrum R in Filter.cofinite, x v ∈
    v.adicCompletionIntegers K
def finiteAdeleRing : Subring (K_hat R K) where
  carrier := {x : K_hat R K | x.IsFiniteAdele}
  ...
```

- $\forall^f$ `... in filter.cofinite` : syntax for restricted product.
- Generating set : $\{\prod_v U_v \mid U_v \text{ open and } U_v = R_v \text{ for almost all } v\}$.
- I check that it is a commutative topological ring.

The finite idèle group.

- The finite idèle group $\mathbb{I}_{R,f}$ of R is the unit group of $\mathbb{A}_{R,f}$.
- It is a topological group with the topology induced by the map $\mathbb{I}_{R,f} \to \mathbb{A}_{R,f} \times \mathbb{A}_{R,f}$ sending $x \mapsto (x, x^{-1})$.

```
def finite_idele_group := units (finite_adele_ring R K)
instance : topological_group (finite_idele_group R K) :=
units.topological_group
```

The adèle ring of a global field.

- For a number field K, define $\mathbb{A}_K := \mathbb{A}_{K,f} \times (\mathbb{R} \otimes_{\mathbb{Q}} K)$.

```
variables (K : Type) [field K] [number_field K]
def A_K_f := finite_adele_ring (ring_of_integers K) K
def A_K := (A_K_f K) × (ℝ ⊗[ℚ] K)
```

- We get a topological ring structure.
- We define the group of (finite) idèles $\mathbb{I}_K$:

```
def I_K_f := units (A_K_f K)
def I_K := units (A_K K)
```

- And the idèle class group $C_K := \mathbb{I}_K / K^*$:

```
def C_K := (I_K K) / (inj_units_K.group_hom K).range
```

- The function field case is similar.

Stating the Main Theorem of Global Class Field Theory

Theorem (Main Theorem of Global Class Field Theory)

Let K be a number field. Denote by $\pi_0(C_K)$ the quotient of C_K by the connected component of the identity. There is an isomorphism of topological groups $\pi_0(C_K) \simeq G_K^{ab}$.

- $G_K := \mathrm{Gal}_{\bar{K}/K}$ is a topological group with the profinite topology (in `mathlib`, by S. Monnet).
- $G_K^{\mathrm{ab}} := G_K/\overline{[G_K, G_K]}$ with the quotient topology (now in `mathlib`: the topological closure of a normal subgroup is a normal subgroup).
- $\pi_0(C_K)$ has the quotient topology (now in `mathlib`: the connected component of the identity is a subgroup).

Proving that C_K surjects onto the ideal class group $\mathrm{Cl}(K)$

Proposition

There is a continuous surjective homomorphism from $\mathbb{I}_K$ to the group of invertible fractional ideals of K, sending $(x_v)_v$ to $\prod_{v \text{ fin.}} v^{v_v(x_v)}$.

Its kernel is the set $\mathbb{I}_{K,\infty}$ of elements $(x_v)_v$ in $\mathbb{I}_K$ having additive valuation zero at all finite places.

Corollary

There is a continuous surjection $C_K \to \mathrm{Cl}(K)$ with kernel $\mathbb{I}_{K,\infty}K^*/K^*$.

Local Fields

Reference: M. I. de Frutos Fernández and F. A. E. Nuccio,
https://github.com/mariainesdff/local_class_field_theory [4]

Discrete valuations

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

```
class is_discrete (v : valuation A 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.*

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

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

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)
```

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

Uniformizers (II)

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

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

```
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 the unit ball of the valuation v is generated by any uniformizer.

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

Discrete valuation rings

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

```
class discrete_valuation_ring (R : Type u) [comm_ring R]
  [is_domain R]
  extends is_principal_ideal_ring R, local_ring R : Prop :=
(not_a_field' : maximal_ideal R ≠ ⊥)
```

Conexion with discrete valuation rings

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 }
```

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

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 $w' : L \to \mathbb{R}_{\geq 0}$ exteding 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) := ...
```

Global to Local (I)

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

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.

Global to Local (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
```

Global to Local (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 := ...
```

Local Fields

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

```
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)))
```

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]
```

Lemma

A mixed characteristic local field is a local field.

```
instance (p : out_param ℕ) [fact(nat.prime p)] (K : Type*)
  [field K] [mixed_char_local_field p K] :
local_field K := ...
```

The ring of integers

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.

Equal Characteristic Local Fields

An equal characteristic local field is a finite field extension of the field $\mathbb{F}_p((X))$, 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]
```

Lemma

An equal characteristic local field is a local field.

```
instance (p : out_param ℕ) [fact(nat.prime p)] (K : Type*)
  [field K] [eq_char_local_field p K] :
  local_field K := ...
```

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 ring `laurent_series K`.

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

The ring of integers

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.

Local Class Field Theory

Theorem (Local Reciprocity Law)

For every local field K, there exists a homomorphism (local Artin map)

$$\phi_K : K^\times \to Gal(K^{ab}/K)$$

such that:

1. *for every uniformizer π of K, $\phi_K(\pi)_{|K^{un}} = Frob_K$,*
2. *for every finite abelian extension L of K, $Nm_{L/K}(L^\times)$ is contained in the kernel of $x \mapsto \phi_K(x)_{|L}$ and ϕ_K induces an isomorphism*

$$\phi_{L/K} : K^\times/Nm_{L/K}(L^\times) \to Gal(L/K).$$

LCFT Prerequitistes

- Ramification theory
- Group cohomology (Amelia Livingston)
- Galois cohomology
- Hilbert's Theorem 90 (Amelia Livingston)
- $\mathrm{inv}_K : H^2(\mathrm{Gal}(K^{\mathrm{al}}/K), (K^{\mathrm{al}})^\times) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$.
- Tate cohomology
- ...

References

Anne Baanen, Sander R. Dahmen, Ashvni Narayanan, and Filippo A. E. Nuccio.
A Formalization of Dedekind Domains and Class Groups of Global Fields.
In *ITP 2021*, pages 5:1–5:19, 2021.

María Inés de Frutos-Fernández.
Formalizing the Ring of Adèles of a Global Field.
In *ITP 2022*, pages 14:1–14:18, 2022.

María Inés de Frutos-Fernández.
Formalizing Norm Extensions and Applications to Number Theory.
In *ITP 2023*, pages 13:1–13:18, 2023.

María Inés de Frutos-Fernández and Filippo A. E. Nuccio.
Formalizing Local Fields (working title), 2023.
URL: https://github.com/mariainesdff/local_class_field_theory.

Robert Y. Lewis.
A Formal Proof of Hensel's Lemma over the p-Adic Integers.
In *CPP 2019*, pages 15—26, 2019.

Lean Meetings

Lean for the Curious Mathematician 2023 (Düsseldorf, 4–8 Sept. 2023):

- `https://lftcm2023.github.io/`

Lean for the Curious Mathematician 2024 (Marseille, 25–29 March 2024)

- `https://conferences.cirm-math.fr/2970.html`