A Formalization of Complete Discrete Valuation Rings and Local Fields

María Inés de Frutos-Fernández, Filippo Alberto Edoardo Nuccio Mortarino Majno Di Capriglio

A Formalization of Complete Discrete Valuation Rings and Local Fields

María Inés de Frutos-Fernández*
Departamento de Matemáticas
Universidad Autónoma de Madrid
Madrid, Spain
maria.defrutos@uam.es

Filippo Alberto Edoardo Nuccio Mortarino Majno di Capriglio*
Institut Camille Jordan UMR 5208
Université Jean Monnet Saint-Étienne
Saint-Étienne, France
filippo.nuccio@univ-st-etienne.fr

Abstract

Local fields, and fields complete with respect to a discrete valuation, are essential objects in commutative algebra, with applications to number theory and algebraic geometry. We formalize in Lean the basic theory of discretely valued fields. In particular, we prove that the unit ball with respect to a discrete valuation on a field is a discrete valuation ring and, conversely, that the adic valuation on the field of fractions of a discrete valuation ring is discrete. We define finite extensions of valuations and of discrete valuation rings, and prove some localization results.

Building on this general theory, we formalize the abstract definition and some fundamental properties of local fields. As an application, we show that finite extensions of the field $\mathbb{Q}_p$ of p-adic numbers and of the field $\mathbb{F}_p((X))$ of Laurent series over $\mathbb{F}_p$ are local fields.

CCS Concepts: • **Theory of computation** → **Logic and verification**; **Proof theory**.

Keywords: formal mathematics, Lean, mathlib, algebraic number theory, local fields, discrete valuation rings.

ACM Reference Format:
María Inés de Frutos-Fernández and Filippo Alberto Edoardo Nuccio Mortarino Majno di Capriglio. 2024. A Formalization of Complete Discrete Valuation Rings and Local Fields. In *Proceedings of the 13th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP '24), January 15–16, 2024, London, UK*. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3636501.3636942

1 Introduction

The vague idea that geometric intuition and algebraic rigor can fruitfully interact is an old theme, certainly predating the modern approach by Descartes and subsequently by Newton and Leibniz. In contemporary commutative algebra, and especially after the advent of scheme theory by Grothendieck around 1960, this connection has become even tighter: geometric concepts and techniques are often borrowed for a wide range of applications. In this work we are concerned with the concept of *local field*, a fundamental notion in algebraic number theory whose origin, and still many applications, comes from geometry and diophantine questions. Suppose, for instance, that one is interested in the integral solutions (a_1, a_2, a_3) to $X_1^2 + X_2^2 + X_3^2 = 0$: clearly, since for positivity reasons the only *real* solution is $(0, 0, 0)$, there cannot be any other integral solutions. On the other hand, $X_1^2+X_2^2-3X_3^2 = 0$ certainly has real solutions, yet has no non-trivial solutions in $\mathbb{F}_3$, the field with 3 elements, as can be seen by analyzing the finitely many possibilities. Hence, if (a_1, a_2, a_3) is an integral solution to this equation, its reduction modulo 3 must be the trivial solution in $\mathbb{F}_3$, so that a_1, a_2 and a_3 are all divisible by 3. This implies $a_1 = a_2 = a_3 = 0$, since otherwise we would have an equality $a_1^2 + a_2^2 = 3a_3^2$, in which the highest power of 3 dividing the left hand side is even, while the highest power of 3 dividing the right hand side is odd, yielding a contradiction.

From a geometric perspective, one can regard the previous as a kind of "local analysis": interpreting the primes as the points of a geometric object attached to $\mathbb{Z}$, if a "global" solution $(a_1, a_2, a_3) \in \mathbb{Z}^3$ exists, then for each prime p, we obtain a solution $(\overline{a_1}, \overline{a_2}, \overline{a_3}) \in \mathbb{F}_p^3$ by reducing the coordinates modulo p — we can look at this as being a local solution "around the point p" — as well as the solution $((a_1 : \mathbb{R}), (a_2 : \mathbb{R}), (a_3 : \mathbb{R})) \in \mathbb{R}^3$ over the reals. In particular, if one of these local solutions fails to exists, this means that the equation cannot have a global solution. Yet, in this analogy, the fields $\mathbb{F}_p$ and $\mathbb{R}$ are very different: the former is finite, with trivial discrete geometry and of positive characteristic, while the latter has a rich metric structure and characteristic 0. Now, for every p, one can rather consider the field

*Both authors contributed equally to this research.

CPP '24, January 15–16, 2024, London, UK

ACM ISBN 979-8-4007-0488-8/24/01…$15.00
https://doi.org/10.1145/3636501.3636942

of p-adic numbers $\mathbb{Q}_p$ which is, in this perspective, a better analogue for $\mathbb{R}$ than $\mathbb{F}_p$: it has a metric with respect to which it is complete (Cauchy sequences converge), and it has characteristic 0 (so, in particular, it contains $\mathbb{Q}$). To define it, one observes that for every prime p there exists an absolute value $|\cdot|_p$ on $\mathbb{Q}$ for which numbers that are highly divisible by p are close to 0. Having an absolute value, it is possible to speak about convergence and about Cauchy sequences: exactly as for the euclidean absolute value, one can find Cauchy sequences that do not converge to any rational, and $\mathbb{Q}_p$ is defined as the *completion* of $\mathbb{Q}$ with respect to $|\cdot|_p$. It is the "smallest" field where all $|\cdot|_p$-Cauchy sequences converge. Crucially, it still bears strong connections with the prime p: for instance, if a monic polynomial in $\mathbb{Z}[X]$ has a simple root in $\mathbb{F}_p$, then it also has one in $\mathbb{Q}_p$.

The local analysis described before is an example of the "local-to-global" principle: to solve a problem in $\mathbb{Z}$, or $\mathbb{Q}$, one can try to solve it in $\mathbb{Q}_p$, for all p, and in $\mathbb{R}$. A famous application of the local-to-global principle is the Hasse–Minkowski Theorem, which states that if $Q(x)$ is a quadratic form with rational coefficients, then the equation $Q(x) = 0$ has a nontrivial solution over $\mathbb{Q}$ if and only if it has a nontrivial solution over $\mathbb{R}$ and over every $\mathbb{Q}_p$.

For another notorious example, it has long been known that the so-called "first case" of Fermat's Last Theorem can be solved using class field theory (see [17]), which is a deep theory where the global theorems are obtained by a beautiful patching of the local ones: we refer to [22] for an excellent account of this example. It should also be emphasized that ultimately Wiles' very proof of Fermat's Last Theorem makes heavy use of the local-to-global principle in the framework of Galois representations: we refer to [16] for a summary of this technique.

Before describing our work, let us mention two generalizations of the p-adic numbers that will guide our approach to the formalization. First of all, the field $\mathbb{Q}$ of rational numbers can be replaced by an arbitrary number field, or global field. We refer to [3, §2] for a brief overview of these notions in the context of formalization. Number fields are fields that can be obtained by adjoining roots of polynomials $f(X) \in \mathbb{Z}[X]$ to $\mathbb{Q}$, like $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{2}) = \{r+s\sqrt{2}, r, s \in \mathbb{Q}\}$. They are a key object of study in algebraic number theory and resemble in many perspectives the rational field. Every number field K can be realized as the field of fractions $K = \operatorname{Frac} O_K$ of a suitable subring $O_K \subseteq K$, in the same vein as $\mathbb{Q} = \operatorname{Frac}\mathbb{Z}$. These rings O_K are not principal, in general, but they are Dedekind domains (see Example 2.3 and the references *ibid.*): so, although we cannot in general define an absolute value $|\cdot|_\pi$ on O_K associated to elements $\pi \in O_K$, it is possible to define an absolute value $|\cdot|_\mathfrak{m}$ associated to every maximal ideal of O_K. The completion procedure discussed above can then be performed analogously, and the fields $\widehat{K}_\mathfrak{m}$ obtained in this way are all finite extensions of some $\mathbb{Q}_p$, and are the so-called mixed characteristic local fields. Analogous constructions exist when replacing $\mathbb{Q}$ by $\mathbb{F}_p(X)$, leading to equal characteristic local fields, and we refer to §3.1 for more details. There is also a more abstract definition of local fields, that includes the above two, that is recalled and formalized in Definition 3.1.

Secondly, unlike the euclidean metric, the p-adic one carries a strong discrete flavor, in that only integral powers of p can occur as values $|x|_p$ for $x \in \mathbb{Q} \setminus \{0\}$. This happens in other contexts, and the relevant notion is that of a discrete valuation ring; we will describe their theory in more detail in §2.3. Here we content ourselves with saying that they are a class of rings R endowed with a valuation map v to $\mathbb{Z}\cup\{\infty\}$ such that the arithmetic behavior of elements $r \in R$ can be read on the value $v(r)$. The relation of discrete valuation rings with local fields is deep: the completion of the fraction field of a discrete valuation ring with finite residue field (see §3) is a local field and, conversely, for every local field F the subset $\{x \in F \mid |x|_F \leq 1\}$ is always a discrete valuation ring, yet not every discrete valuation ring is of this form.

In this paper, we formalize in Lean 3 the definition and basic theory of local fields and their relation with discrete valuation rings. We provide both a concrete approach, defining mixed characteristic and equal characteristic local fields as finite field extensions of $\mathbb{Q}_p$ and $\mathbb{F}_p((X))$, and a more abstract definition of local field which comprises these two special cases.

The `mathlib` library provides a very complete theory of general valuations, as well as the basic theory of discrete valuation rings, but the connection between these two notions is largely missing. We formalize the definition of discrete valuation and greatly expand the available theory for discrete valuation rings, their fields of fractions, and their associated discrete valuations, including theorems about completions, extensions of valuations and localizations. To the authors' best knowledge, this work constitutes the first formalization of local fields and of extensions of discrete valuations in any proof assistant.

The Lean code for our formalization is available at a public GitHub repository. Inside the folder `from_mathlib` we gather files that are previous work of the authors, as well as a file due to Yaël Dillies, used in this project after securing permission from them. Everything else is new, original work of the authors of this paper, totaling about 8,000 lines of code. Some of the code excerpts below have been edited for clarity, but we also provide links to the corresponding results in our repository. In some code excerpts the so-called *dot notation* is exhibited: for example, the call `(ideal.is_prime I)` can be shortened to `I.is_prime`.

Throughout this paper, all rings are assumed to be commutative and unitary.

1.1 Lean and `mathlib`

This project is formalized in the Lean 3 theorem prover [14], which is based on dependent type theory, with proof irrelevance, quotient types, and non-cumulative universes [9].

We build our work on top of the mathematical library `mathlib` of Lean 3, whose key properties are its unified approach to integrate different mathematical theories, and its decentralized nature, with over 300 contributors. One of the key tools for organizing mathematical hierarchies used both in Lean's core library and in `mathlib` is typeclass inference. By declaring certain terms as `instance`, Lean will automatically try to infer the relevant values during the unification procedure. We refer to [1] for a more detailed discussion of the role of `instance` parameters in Lean.

The formalization is in Lean 3 because at the time when we began it, almost none of its prerequisites were available in Lean 4. Now that the complete `mathlib` has been translated to Lean 4, we plan to port our work and start to integrate it in this library. All our future work related to this project will be directly implemented in Lean 4.

1.2 Paper outline

In §2, we treat the general theory of discrete valuations and discrete valuation rings: after presenting some background material in §2.1–§2.3, we describe our main results in §2.4, concerning completions, and §2.5, concerning extensions of valuations. In §3.1 we present our formalization of local fields, describing the equal and mixed characteristic cases in §3.1 and §3.2, respectively. We conclude in §4 with a description of future and related work and a discussion of some of our key design choices.

2 Discrete Valuation Rings

In this section we present our formalization of the theory of discretely valued fields and discrete valuation rings, including results about completions and extensions of valuations. As a technical prerequisite, we discuss in § 2.1 the definition and main properties of the `mathlib` type $\mathbb{Z}_{m0}$, where most of the valuations that we considered take their values.

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

There are several situations in mathematics in which additive structures get translated into multiplicative structures. For example, associated to each real number $n \neq 0$, there is an exponential map $\exp_n : \mathbb{R} \longrightarrow \mathbb{R}$ sending x to n^x. This map has the property that $\exp_n(x+y) = \exp_n(x) \cdot \exp_n(y)$ and, whenever $n > 1$, it preserves the order on $\mathbb{R}$.

A second example occurs in the theory of valuations. If $a : R \longrightarrow \mathbb{Z} \cup \{\infty\}$ is an additive valuation on a ring R (see Definition 2.1) and $n > 1$ is a real number, it is common to study the associated function $v : R \longrightarrow n^{\mathbb{Z}} \cup \{0\}$ sending r to $n^{-a(r)}$, with the convention that $n^{-\infty} = 0$. Here

$$n^{\mathbb{Z}} \cup \{0\} = \{n^a \mid a \in \mathbb{Z}\} \cup \{0\} \subseteq \mathbb{R}.$$

Some abstractions that can be used to formalize this kind of translations are available in `mathlib`. Given any type `A` endowed with an additive structure, `mathlib` provides a new type `multiplicative A` that is in bijection with `A` and carries a multiplicative structure, together with a map `of_add : A ⟶ multiplicative A` satisfying

$$\texttt{of\_add (x + y) = of\_add x * of\_add y}$$

for all `x, y : A`. If `A` is equipped with a preorder, then so is `multiplicative A`, and the map `of_add` is strictly monotone: `x ≤ y` is equivalent to `of_add x ≤ of_add y`. The map `to_add : multiplicative A ⟶ A` is inverse to `of_add`.

We are especially interested in the case `A` $= \mathbb{Z}$. As an additive group, $\mathbb{Z}$ is an infinite cyclic group generated by 1 or -1. Correspondingly, the elements `of_add(1)` and `of_add(-1)`, that do not bear a specific notation, are the only generators of the cyclic group `multiplicative` $\mathbb{Z}$. Since the map `of_add` preserves the unit element, we have that `of_add(0) = 1` is the unit, hence

$$(\texttt{1: multiplicative}\ \mathbb{Z}) \neq \texttt{of\_add(1:}\mathbb{Z}\texttt{)}.$$

Given two integers a, b, it holds that `of_add(a * b) = of_add(a)`^{b}`= of_add(b)`^{a}. In particular, we have the equality `of_add(±1)`^{n}`= of_add(±n)` for all `(n : ℤ)`.

A new type `with_zero (multiplicative ℤ)`, denoted $\mathbb{Z}_{m0}$, can be constructed from `multiplicative` $\mathbb{Z}$ by adding an extra term `0` to `multiplicative` $\mathbb{Z}$. The resulting type $\mathbb{Z}_{m0}$ still carries a multiplication, that extends the one on `multiplicative` $\mathbb{Z}$ and for which `0 * x = 0` for all `x`; moreover, setting `0 ≤ x` for all `x`, $\mathbb{Z}_{m0}$ is endowed with an order that extends the one on `multiplicative` $\mathbb{Z}$. The inclusion

$$\texttt{multiplicative}\ \mathbb{Z} \longrightarrow \mathbb{Z}_{m0}$$

is an order-preserving coercion that respects the multiplication on both sides, and we omit it from the notation.

The type $\mathbb{Z}_{m0}$ provides an abstraction of the structure on the set $n^{\mathbb{Z}} \cup \{0\}$ that does not require a choice of the base n, and it will be the codomain of most of the valuations that we consider in this paper.

2.2 Valuations

Definition 2.1 ([6, Chapitre VI, §3, n°1, Définition 1])**.** Let R be a ring. A function $a : R \longrightarrow \mathbb{Z} \cup \{\infty\}$ is an *additive valuation* on R if

i) $a(r) = \infty$ if and only if $r = 0$;
ii) $a(r \cdot s) = a(r) + a(s)$ for all r, s in R;
iii) $a(r+s) \geq \min\{a(r), a(s)\}$ for all r, s in R.

Given an additive valuation a on R, we can define an associated function $v : R \longrightarrow \mathbb{Z}_{m0}$ by sending 0 to 0 and $r \neq 0$ to `of_add(-`a`(r))`. From the definition of a, it is easy to deduce that v satisfies the properties of a multiplicative valuation, as in the following definition:

Definition 2.2. A *multiplicative valuation* on a ring R is a function $v : R \longrightarrow \mathbb{Z}_{m0}$ satisfying the properties

i) $v(0) = 0$;
ii) $v(1) = 1$;
iii) $v(x \cdot y) = v(x) \cdot v(y)$ for all $x, y \in R$;
iv) $v(x + y) \leq \max\{v(x), v(y)\}$ for all $x, y \in R$.

Note that an element $r \in R$ has additive valuation 1 if and only if it has multiplicative valuation `of_add(-1)`. Elements of multiplicative valuation `of_add(-1)` will play a prominent role in §2.3.

For example, let $R = \mathbb{Z}$ be the ring of integers, and fix a prime number p. Then, thanks to unique factorization, we can define an additive valuation $a_p \colon \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ by sending an integer z to the number of times that p appears in the factorization of z. We can extend the function a_p to $\mathbb{Q}$ by defining $a_p(r/s) := a_p(r) - a_p(s)$. Then a_p is an additive valuation on $\mathbb{Q}$, called the *additive p-adic valuation* on $\mathbb{Q}$. The corresponding multiplicative valuation $v_p \colon \mathbb{Q} \to \mathbb{Z}_{\mathrm{m}0}$ is called the *p-adic valuation.*

Example 2.3 (The $\mathfrak{m}$-adic valuation)**.** We will often consider the following generalization of the p-adic valuation. If R is a Dedekind domain (see [6, Chapitre VII, §2]) which is not a field, then every nonzero ideal of R can be factored as a product of maximal ideals, uniquely up to reordering. Therefore, for every maximal ideal $\mathfrak{m}$ of R, we can follow an analogous construction to define an additive valuation $a_{\mathfrak{m}} : R \to \mathbb{Z} \cup \{\infty\}$ on R by sending 0 to ∞ and any nonzero $r \in R$ to the number of times that $\mathfrak{m}$ appears in the factorization of the principal ideal (r). We extend $a_{\mathfrak{m}}$ to the fraction field K of R by the formula $a_{\mathfrak{m}}(r/s) := a_{\mathfrak{m}}(r) - a_{\mathfrak{m}}(s)$. The corresponding multiplicative valuation $v_{\mathfrak{m}} = \texttt{of\_add} \circ (-a_{\mathfrak{m}}) \colon K \to \mathbb{Z}_{\mathrm{m}0}$ on K is called the *$\mathfrak{m}$-adic valuation.* This valuation was formalized in [12], and is available in `mathlib` as the declaration `is_dedekind_domain.height_one_spectrum.valuation` .

While in most number theory references it is more common to work with additive valuations than with multiplicative ones, for historical reasons `mathlib` follows the opposite convention, and it provides a much more complete API for multiplicative valuations. Hence we use multiplicative valuations in our formalization and, throughout the paper, whenever we use the term "valuation" without further adjectives, we mean "multiplicative valuation".

Remark 2.4. (For experts) More generally, the codomain $\mathbb{Z}_{\mathrm{m}0}$ in the definition of a (multiplicative) valuation can be replaced by $\Gamma_0 = \Gamma \cup \{0\}$, where Γ is a linearly ordered commutative group. The order on Γ is extended to Γ_0 analogously as we did for $\mathbb{Z}_{\mathrm{m}0}$. Structures like Γ_0 are called "groups with zero".

An example of this situation occurs when starting with a *local* Dedekind domain R, with unique maximal ideal $\mathfrak{m}_R$ and field of fractions K. In this setting one can prove that the quotient map

$$v \colon K \to K/R^\times$$

is a valuation, where the quotient $K/R^\times$ is ordered by reverse divisibility. The group with zero $K/R^\times = K^\times/R^\times \cup \{0\}$ is called the value group[1] of R. The value group is implemented in `mathlib` as `valuation_ring.value_group`, but we mostly stick to $\mathbb{Z}_{\mathrm{m}0}$-valued valuations in our work.

We represent valuations using the `valuation` structure available in `mathlib`, which encodes Definition 2.2. A valuation on a ring R induces a topology that is homogeneous with respect to addition (see [5, Chapitre III,§1]: every neighborhood $\Omega \subseteq R$ is of the form $\Omega = x + \Omega_0$ where Ω_0 is a neighborhood of 0 and $x \in \Omega$. In other words, addition (and subtraction) are homeomorphisms of the ring into itself. This property shows that to characterize the topology it is enough to describe the neighborhoods of 0.

When R is a Dedekind domain and $v = v_{\mathfrak{m}}$ is the topology associated to a maximal ideal $\mathfrak{m}$, as defined in Example 2.3, a basis for the neighborhoods of 0 is provided by the sets

$$U_\gamma = \{r \in R \big| v_{\mathfrak{m}}(r) \leq \gamma\} \quad \text{for} \quad \gamma \colon \mathbb{Z}_{\mathrm{m}0},\ \gamma \neq 0.$$

In particular, two elements r_1, r_2 are "close to each other" if their difference lies in a sufficiently deep neighborhood of 0, meaning that $v_{\mathfrak{m}}(r_1 - r_2) \leq \gamma$ for a suitable $\gamma \colon \mathbb{Z}_{\mathrm{m}0}, \gamma \neq 0$. Given the definition of $v_{\mathfrak{m}}$ this translates into the fact that the principal ideal $(r_1 - r_2)$ is divisible by a high power of $\mathfrak{m}$.

Actually, the above topology is of a special kind, because the valuation defines a structure of *uniform space* on R, as explained in [6, Chapitre VI, §5] and in the references *ibid*. This is a simultaneous generalization of the structure of metric space and of topological group and the topology is induced by the uniform structure. Our main reference for uniform structures is [5, Chapitre II]; for a throughout discussion of the formalization of uniform spaces, we urge the reader to consult the beautifully written [8], in particular its §5.

The `mathlib` library also provides the class `valued`, which bundles together a ring R endowed with a uniform space structure and a distinguished valuation inducing it. Given a term (`hv : valued R` $\mathbb{Z}_{\mathrm{m}0}$), these can be accessed through `hv.to_uniform_space` and `hv.v`, respectively.

This class is designed for rings in which there is a preferred valuation. Recall from Example 2.3 that on a Dedekind domain R, there is a valuation for each maximal ideal, and it can be shown that any nontrivial valuation on R is of this form. Hence, if R is local, then the only nontrivial valuation on R is the $\mathfrak{m}_R$-adic valuation associated to its unique maximal ideal, and we declare a `valued` instance on R. If R is not local, given any maximal ideal $\mathfrak{m} \subseteq R$ we can still define a term (`hv`$_{\mathfrak{m}}$`: valued R` $\mathbb{Z}_{\mathrm{m}0}$) representing the $\mathfrak{m}$-adic valuation and allowing us to access the whole `valued` API locally. Yet, we would not declare this as a global `valued` instance

[1] We translate in this way the term *groupe des valeurs* from [6, Chapitre VI, §3, n°2].

on R, since none of the $\mathfrak{m}$-adic valuations on R is preferred over the others.

Given a ring R with a valuation v, we can consider the *unit ball* of R, that is the subring R° of elements with valuation less than or equal to $(1 \colon \mathbb{Z}_{\mathrm{m}0})$. This subring is called `v.integer` in `mathlib`. When K is a field, the subring K° is a *valuation subring*, meaning that for every $\alpha \in K$, either $\alpha \in K^\circ$ or $\alpha^{-1} \in K^\circ$: in particular, $K \cong \operatorname{Frac}(K^\circ)$. Since the definition of valuation subring involves taking inverses, it is only available for fields. Hence, when working with a general ring R, we formalize R° as `v.integer`, but when working with a field we use the richer structure `v.valuation_subring`, which gives us access to results about valuation subrings available in `mathlib`.

2.3 Discrete Valuation Rings

Our general references for the theory of discrete valuation rings are [20, Chapitres I–II] and [6, Chapitre VI]. One notable difference with our language is that both references consider additive valuations, whereas we stick to the multiplicative convention introduced in §2.2, which is the approach chosen in `mathlib`. Mathematically, the two points of view are equivalent: one just needs to keep in mind the translation between $\mathbb{Z} \cup \{\infty\}$ and $\mathbb{Z}_{\mathrm{m}0}$. Finally, we refer to [7], in particular to [7, Chapitre IV], for the main results about ring theory and commutative algebra that we will need.

Let R be a ring, as above assumed commutative and unitary. We begin by recalling the following equivalence:

Theorem 2.5 ([6, Chapitre VI, §3, n°6, Proposition 9])**.** *Suppose R is a Noetherian local ring that is not a field. The following properties are equivalent:*

1. *The maximal ideal $\mathfrak{m}_R$ of R is principal;*
2. *R is a principal ideal domain (PID);*
3. *R is an integral domain that coincides with the unit ball of its fraction field* $\operatorname{Frac}(R)$ *with respect to a valuation* $v \colon \operatorname{Frac} R \longrightarrow \mathbb{Z}_{\mathrm{m}0}$.

Remark 2.6. In [6, Chapitre VI, §3, n°6, Proposition 8] and in [20, Chapitre I, §2, Proposition 2] other equivalences are proved, but we will not need them.

A ring satisfying the equivalent properties of Theorem 2.5 is called a discrete valuation ring (often shortened as DVR). The nomenclature is motivated by point 3. *ibid.*: given a DVR R, it is possible to find a valuation

$$v \colon \operatorname{Frac}(R) \longrightarrow \mathbb{Z}_{\mathrm{m}0}$$

such that $R = (\operatorname{Frac} R)^\circ$: yet this valuation is not unique. Indeed, the definition of the action of $\mathbb{Z}$ on $\mathbb{Z}_{\mathrm{m}0}$ shows that replacing a valuation v by a power v^e for $e \in \mathbb{Z}_{>0}$ leaves the unit ball unchanged. For each of these valuations, the image $\operatorname{Im}(v) \subseteq \mathbb{Z}_{\mathrm{m}0}$ is the free group with zero generated by $v(r)$, where r is any generator of the maximal ideal $\mathfrak{m}_R$ of R. Upon replacing v by $v^{1/a(r)}$ for some generator r of $\mathfrak{m}_R$, where a denotes the additive valuation associated to v, we can assume that the image is the whole $\mathbb{Z}_{\mathrm{m}0}$: in this case the valuation is said to be *normalized*, and the elements of valuation equal to (`of_add`(-1) : $\mathbb{Z}_{\mathrm{m}0}$) are called *uniformizers*.

One basic result is that, for a normalized valuation on a DVR, the uniformizers are exactly the set of generators of $\mathfrak{m}_R$, because properties ii) and iii) of Definition 2.2 show that an element $u \in R$ is a unit if and only if $v(u) = 1 =$ (`of_add 0`). In particular, there exists a unique normalized valuation on a DVR, since the same argument shows that every valuation is uniquely determined by its value on one, or any, generator of $\mathfrak{m}_R$. Moreover, as explained in Example 2.3, any such valuation can uniquely be extended to $\operatorname{Frac}(R)$. We denote this normalized valuation by $v_{0,R}$ — or simply by v_0 when the DVR R can be understood.

Assume now that R is any integral domain (not necessarily a DVR) and that K is a field of fractions for R. The points of view taken in [20, Chapitre I] and in [6, Chapitre VI, §3, n°6] concerning valuations on K are not identical: in the former, the valuations occurring in point 3. of Theorem 2.5 take values in $\mathbb{Z} \cup \{\infty\}$ (or $\mathbb{Z}_{\mathrm{m}0}$, up to our translation), whereas in the latter they are valued in $K^\times/R^\times \cup \{\infty\}$, that translates to the value group $K/R^\times = K^\times/R^\times \cup \{0\}$ in our language, but under the assumption that there is an isomorphism $K^\times/R^\times \cong \mathbb{Z}$. In both cases they are called "discrete"; they are said to be normalized, as above, when they are surjective. Often results are stated assuming that the valuation is normalized, relying on the possibility of achieving this normalization simply by rescaling, so that the theory of discrete valuations is essentially the theory of *normalized* discrete valuations.

In the setting of a formalization work, the ambiguities described above concerning the group (with zero) Γ_0 and the normalization of the valuation call for more attention than in pen-and-paper mathematics. It is in principle possible to let Γ_0 vary, including it as a (perhaps implicit) variable: yet one must stipulate the existence of an isomorphism $\Gamma_0 \cong \mathbb{Z}_{\mathrm{m}0}$, adding one more variable, so that we rather find it more convenient to consider only valuations that are $\mathbb{Z}_{\mathrm{m}0}$-valued, in line with the choice made when defining the adic valuation attached to a height-one prime of a Dedekind domain. Even with this choice, the above discussion about different possible normalizations of a $\mathbb{Z}_{\mathrm{m}0}$-valued valuations, all leading to the same mathematical object, suggests that the focus should be put on *normalized* valuations, rather than general ones. With this in mind, we call a valuation "discrete" when it is $\mathbb{Z}_{\mathrm{m}0}$-valued and *also* normalized, encoding this notion in the following class:

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

Code excerpt 1. Definition of discrete valuation.

Observe that when the domain R is endowed with a discrete valuation in the above sense, then it is necessarily a field. Henceforth we change perspective a bit and we focus on a topological field K endowed with a valuation v, letting K° be its unit ball: as discussed at the end of §2.2 this is implemented by putting a `valued` instance `hv` on `K` and by setting

```
K₀ = hv.v.valuation_subring
```

Now, with our definition, a valuation is discrete only if it takes values in the type $\mathbb{Z}_{m0}$ and if there exists a uniformizer, and this we prove in the following form:

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

The lemma `exists_uniformizer_of_discrete` provides the reverse implication. Similarly, the aforementioned correspondence between uniformizers for a normalized valuation and generators of $\mathfrak{m}_R$ takes the form

```
lemma uniformizer_is_generator
  (π : uniformizer v) :
  maximal_ideal K₀ = ideal.span {π.1}
```

and the declaration `is_uniformizer_of_generator` represents the reverse implication. From now on, we call a valued field whose valuation is discrete a *discretely valued field.*

The next result that we want to discuss is the formalization of [20, Chapitre I, §1, Proposition 1], stating that the unit ball of a discretely valued field is a DVR. The notion of DVR was already in `mathlib` at the time of our project, implemented through the class `discrete_valuation_ring` — this corresponds to property 2. in Theorem 2.5. Our result takes the following form:

```
instance dvr_of_is_discrete [is_discrete v] :
  discrete_valuation_ring K₀
```

Code excerpt 2. The unit ball is a DVR if the valuation is discrete.

Suppose now that R is a DVR, and let K be a field of fractions for R. By Theorem 2.5, R is a local ring that is a PID, so in particular R is a Dedekind domain, and one can consider the adic valuation associated to its unique maximal ideal $\mathfrak{m}_R$, as defined in Example 2.3. Now, Baanen *et al.* formalized in [2] and [3] the general theory of Dedekind domains, and de Frutos-Fernández formalized in [12] the main properties of adic valuations on Dedekind domains.

With these works at our disposal, our starting point is that the $\mathfrak{m}_R$-adic valuation $v_{\mathfrak{m}_R}$ associated to the maximal ideal $\mathfrak{m}_R$ coincides with the normalized valuation v_0 on K (since R is a domain, we directly extend these valuations to any of its fields of fractions). Although this is mathematically trivial, and the two functions $v_0, v_{\mathfrak{m}_R}$ are considered identical in pen-and-paper mathematics, they actually belong to different types and hence are different terms: in the `mathlib` formalization, the valuation v_0 takes values in the value group $K/R^\times$ (see Remark 2.4), while $v_{\mathfrak{m}_R}$ is $\mathbb{Z}_{m0}$-valued. Our approach to compare them is to show that the unit balls with respect to both coincide. To do so, it is enough to show that R is the unit ball of K when endowed with the valuation $v_{\mathfrak{m}_R}$, because this is tautologically true with respect to the valuation v_0. To prove the isomorphism $R \cong K^\circ$ we first provide the following

```
instance : valued K :=
(maximal_ideal R).adic_valued
```

Code excerpt 3. The `valued` instance on the field of frations of a DVR.

giving a `valued` structure on K by using the $\mathfrak{m}_R$-adic valuation $v_{\mathfrak{m}_R}$. With this definition, the whole library concerning adic valuations is at our disposal. We then show that the valuation $v_{\mathfrak{m}_R}$ is actually discrete (in our sense) by providing the

```
instance : is_discrete (valued.v K ℤₘ₀)
```

Code excerpt 4. The valuation on a DVR is discrete.

By combining this result with the above discussion we deduce that K° is itself a DVR, and we finally prove the isomorphism $R \cong K^\circ$ in the form of the following

```
def dvr_equiv_unit_ball :
  R ≃+* valued.v.valuation_subring
```

Remark 2.7. When implementing valuations on a discrete valuation ring R with field of fractions[2] K, we made the design choice to put an instance of the `valued` class on K, but not on the ring R itself. The reason is that, if needed, we can recover the uniform structure on R from the one on K, so we prefer not to duplicate this information. This choice is consistent with `mathlib`'s file `ring_theory.dedekind_domain .adic_valuation`, in which `valued` instances are only put on fields.

As illustrated in the Introduction, one application of the theory of DVR's to number theory comes from the fact that every maximal ideal $\mathfrak{m}$ in a Dedekind domain R induces a discrete valuation, with respect to which the unit ball is a DVR. In this context, we prove the following lemma:

```
lemma adic_valued_is_discrete
  [is_dedekind_domain R] [is_fraction_ring R K]
  (𝔪 : height_one_spectrum R) :
  is_discrete (adic_valued 𝔪).v
```

[2] See §4.3 for more details.

2.4 Complete Discrete Valuation Rings

One setting where the theory of DVR's becomes crucial — especially for its applications to algebraic number theory and algebraic geometry — is that of (adic) completions. The completion is a general procedure that can be performed on every uniform space T, as explained in [5, Chapitre II, §3]. We are not providing the exact definition here; the crucial property to retain is that it yields another uniform space $\widehat{T}$, containing T as a dense subspace, and such that every uniformly continuous function $f\colon T \longrightarrow Z$, valued in any complete, separated topological space Z can be extended *uniquely* to a function

$$\widehat{f}\colon \widehat{T} \to Z \tag{1}$$

(see [5, Chapitre II, §3, n°6, Théorème 2]). When T is a commutative topological group, it suffices that f is a continuous group homomorphism to admit a unique extension, because [5, Chapitre III, §3, n°1, Proposition 3] guarantees that it is automatically uniformly continuous; and the completeness on Z can be weakened as in [5, Chapitre I, §8, n°5, Théorème 1].

In the special case where $T = K$ is a field with a valuation v (endowed with the uniform structure induced by it as explained in §2.2), the completion $\widehat{K}$ is again a field. We refer to [6, Chapitre VI, §5, n°3] for the generalities concerning completions of valued fields, and to [20, Chapitre II, §1] for a shorter introduction. Applying[3] the universal property (1) to the valuation v yields a map $\widehat{v}\colon \widehat{K} \longrightarrow \mathbb{Z}_{m0}$ that is still a valuation. Completions of uniform spaces and uniform fields have been formalized[4], and the paper [8] contains an account of the formalization. The application of this construction in the setting of Dedekind domains is due to de Frutos-Fernández, see [12].

A prototypical example of a completion of a field is the field $\mathbb{Q}_p$ of p-adic numbers, that is defined as the completion of $\mathbb{Q}$ endowed with the p-adic valuation v_p. Another example arises when starting with the ring $K[X]$ of polynomials in one indeterminate over the field K: being a PID, it is a Dedekind domain and the construction of Example 2.3 defines a valuation $v\colon K(X) \longrightarrow \mathbb{Z}_{m0}$ attached to any maximal ideal $\mathfrak{m} \subseteq K[X]$. Take, for instance, $\mathfrak{m} = (X)$. Then the valuation v_X defines a uniform structure on the field

$$K(X) = \operatorname{Frac}(K[X]) = \left\{\frac{f}{g},\ f, g \in K[X] \text{ with } g \neq 0\right\}$$

of rational functions whose completion $\widehat{K(X)}$ is isomorphic to the field $K((X))$ of Laurent series: we discuss our formalization of this isomorphism in §3.1.1.

When completing a field K endowed with a valuation v, the valuation $\widehat{v}$ is unique under the condition of extending the one on K, by (1). It follows that $\widehat{K}$ is always endowed with a global `valued` instance, even when K is not. This is for example the case with $\mathbb{Q}$ and $\mathbb{Q}_p$: the first has infinitely many non-equivalent valuations v_p, and thus no global `valued` instance is declared for it. On the other hand, each $\mathbb{Q}_p$ has a preferred valuation and is actually a valued field. More generally, given a maximal ideal $\mathfrak{m}$ of a Dedekind domain R, we can apply the above discussion to the valuation $v_{\mathfrak{m}}$ to obtain a complete valued field $\widehat{K}_{\mathfrak{m}}$.

We now go back to our discussion concerning DVR's. So, let R be a DVR with field of fractions K. We have seen in the code excerpt 3 that K, endowed with the valuation $v_{\mathfrak{m}_R}$, is valued and so is its completion $\widehat{K}_{\mathfrak{m}_R}$, denoted by `K_v` in our code. Moreover, the valuation on K is discrete (see the code excerpt 4) and the first result we obtain is that the same holds for the valuation $\widehat{v_{\mathfrak{m}_R}}$ on $\widehat{K}_{\mathfrak{m}_R}$, which takes the following form:

```
instance (R : Type*) [is_dedekind_domain R]
  (v : height_one_spectrum R) :
  is_discrete (valued.v K_v ℤₘ₀)
```

In particular, we can consider the ring $\left(\widehat{K}_{\mathfrak{m}_R}\right)^{\circ}$ (denoted by `R_v` in our code) to find, by the discussion in §2.3, that it is itself a DVR

```
instance : discrete_valuation_ring R_v :=
discrete_valuation.dvr_of_is_discrete _
```

with field of fractions $\widehat{K}_{\mathfrak{m}_R}$. Thus, $\left(\widehat{K}_{\mathfrak{m}_R}\right)^{\circ}$ is a local ring endowed with a maximal ideal, denoted $\widehat{\mathfrak{m}_R}$. It is therefore possible to once again apply de Frutos-Fernández' work and endow $\widehat{K}_{\mathfrak{m}_R} = \operatorname{Frac}\left(\left(\widehat{K}_{\mathfrak{m}_R}\right)^{\circ}\right)$ with the $\widehat{\mathfrak{m}_R}$-adic valuation $v_{\widehat{\mathfrak{m}_R}}$, which puts a (potentially) new `valued` structure on $\widehat{K}_{\mathfrak{m}_R}$.

Now, as the notation suggests, the maximal ideal $\widehat{\mathfrak{m}_R}$, which is in particular an abelian group, actually coincides with the completion (inside the larger space $\widehat{K}_{\mathfrak{m}_R}$) of the abelian group $\mathfrak{m}_R$. In our language, this reflects on the equality of the two valuations $\widehat{v_{\mathfrak{m}_R}}$ and $v_{\widehat{\mathfrak{m}_R}}$ on $\widehat{K}_{\mathfrak{m}_R}$, but this equality will clearly not be a definitional one, given the different constructions that led to the two valuations. Rather, it takes the following form:

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

In the above code excerpt, `v_adic_of_compl` represents the valuation $v_{\widehat{\mathfrak{m}_R}}$, while `v_compl_of_adic` is $\widehat{v_{\mathfrak{m}_R}}$.

[3] We do not describe here the topology on $\mathbb{Z}_{m0}$, suffices it to say that it mimics the discrete one on $\mathbb{Z}$. We refer the reader to the relevant `mathlib` file.

[4] Given a ring A, an ideal $I \subseteq A$ and an A-module M, `mathlib` contains the declaration `adic_completion I M`. This is defined purely algebraically as a module of "coherent sequences", a concrete incarnation of an inverse limit. A systematic comparison between this I-adic completion and the uniform one has not yet been formalized.

2.5 Extensions of Complete Discrete Valuation Rings

The goal of this section is to prove that if K is any field complete with respect to a discrete valuation v and L/K is a finite extension of fields, then there is a unique discrete valuation on L "extending" v. To explain our formalization, we first need to discuss the relation between valuations and norms.

Definition 2.8. A *nonarchimedean multiplicative norm* on a ring R is a function $|\cdot|: R \longrightarrow \mathbb{R}$ such that

i) $|r| = 0$ if and only if $r = 0$ for all $r \in R$;
ii) $|1| = 1$;
iii) $|r \cdot s| = |r| \cdot |s|$ for all r, s in R;
iv) $|r + s| \leq \max\{|r|, |s|\}$ for all r, s in R;
v) $|-r| = |r|$ for all r in R.

It follows from these conditions that $0 \leq |r|$ for all $r \in R$.

A valuation $v: R \longrightarrow \Gamma_0$ valued in a group with zero Γ_0 has *rank one* if it is nontrivial and there exists an injective morphism of linearly ordered groups with zero from Γ_0 to $\mathbb{R}_{\geq 0}$. In particular, any nontrivial valuation $v: R \longrightarrow \mathbb{Z}_{m0}$ has rank one. The definition of rank one valuation was first formalized in [13] ↗.

The conditions in Definitions 2.2 and 2.8 are analogous — apart from the codomain of the function — and the terms "multiplicative valuation" and "nonarchimedean multiplicative norm" are often used interchangeably in the mathematical literature. While `mathlib` does not yet provide a way to relate these two notions, a dictionary between them has been formalized in [13]. Namely, if K is a field with a nonarchimedean norm, the definition `valuation_from_norm` ↗ yields the corresponding valuation $v: K \longrightarrow \mathbb{R}_{\geq 0}$. Conversely, if L is a field with a rank one valuation, then `norm_def` ↗ is the corresponding norm function on L. To make use of this dictionary in our project, we need to provide an injective morphism $\mathbb{Z}_{m0} \longrightarrow \mathbb{R}_{\geq 0}$ of linearly ordered groups with zero. We can define this morphism by picking any real $n > 1$ and identifying $\mathbb{Z}_{m0}$ with the subset $n^{\mathbb{Z}} \cup \{0\}$ of $\mathbb{R}_{\geq 0}$, via the map sending 0 to 0 and `of_add(x)` to n^x, for $x \in \mathbb{Z}$.

We construct this morphism as ↗

```
def with_zero_mult_int_to_nnreal {n : ℝ≥0}
  (he : n ≠ 0)  : ℤₘ₀ →*₀ ℝ≥0 :=
{ to_fun := λ x, if hx : n = 0 then 0 else
    n^(to_add (with_zero.unzero hx)),
  ... }
```

and then we prove ↗ that this map is order-preserving whenever $n > 1$. Each choice of n gives rise to a different morphism, and hence to a different norm attached to a valuation $v: K \longrightarrow \mathbb{Z}_{m0}$, although any two such norms define the same uniformity on K. When the quotient $K^\circ/\mathfrak{m}_{K^\circ}$ is finite of order p^k for some prime p, the standard choice is $n = p^k$. Otherwise there is not a preferred n, so in our formalization we pick $n = 6$. We refer to this n associated to v as `v.base` ↗.

Let now K be a complete discretely valued field and let L be a finite field extension, so that L/K is automatically algebraic. The above discussion allows us to apply the following theorem to conclude that there is a unique norm $|\cdot|_L$ on L extending the norm $|\cdot|_K$ associated with the valuation on K.

Theorem 2.9. *Let K be a field that is complete with respect to a nonarchimedean multiplicative norm $|\cdot|_K$ and let L/K be an algebraic extension. Then there is a unique multiplicative nonarchimedean norm on L, called the* spectral norm, *extending the norm $|\cdot|_K$.*

Proof. See [4, 3.2.4/2] for the informal proof and [13, §3.2] for a discussion of the Lean formalization. □

In the setting that we are considering, the norm whose existence is guaranteed by Theorem 2.9 is formalized in the declaration `discrete_norm_extension` ↗.

Since the extension L/K is algebraic, there is an explicit formula for the norm $|x|_L$ of an element $x \in L$: if x has minimal polynomial $f_x(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$, then $|x|_L = |a_0|_K^{1/m}$. We prove this in ↗:

```
theorem spectral_norm_eq_root_zero_coeff :
  spectral_norm K L x = ‖(minpoly K x).coeff 0‖
    ^ (1/(minpoly K x).nat_degree : ℝ)
```

Since for every $x \in L$, the degree of the minimal polynomial f_x of x over K divides the degree $[L : K]$ of the extension L/K ↗, we see that the norm $|\cdot|_L$ takes values in the subset $n^{\frac{\mathbb{Z}}{[L:K]}} \cup \{0\}$ of $\mathbb{R}_{\geq 0}$. The norm needs not surject onto that subset but, since $\mathbb{Z}$ is cyclic, its image is of the form $n^{\frac{b\mathbb{Z}}{[L:K]}} \cup \{0\}$ for some $b \in \mathbb{Z}_{>0}$. Informally speaking, to obtain the corresponding normalized valuation we just need to rescale the norm by raising it to the $([L : K]/b)$-th power, and use the identification between $n^{\mathbb{Z}} \cup \{0\}$ and $\mathbb{Z}_{m0}$.

In order to formalize this idea, we have to be careful to proceed in such a way that we do not leave the type $\mathbb{Z}_{m0}$, since taking the b^{th}-root of an element of $\mathbb{Z}_{m0}$ is not a well-defined operation. We start by constructing a map ↗

```
pow_extension_on_units : Lˣ → multiplicative ℤ
```

that sends $x \in L^\times$ to $v(a_0)^{\frac{[L:K]}{\deg f_x}}$, which is well-defined by lemma `unit_pow_ne_zero` ↗. Then we find the positive number `exp_extension_on_units` ↗, denoted b above, such that the image of `pow_extension_on_units` is generated by `of_add (exp_extension_on_units : ℤ)`. Hence, using the lemma `exists_mul_exp_extension_on_units` ↗, we can obtain the natural number c such that

```
pow_extension_on_units K L x =
  (of_add (exp_extension_on_units))^c;
```

which leads to our definition of the extended valuation ↗:

```
def extension_def : L → ℤₘ₀ := λ x,
  if hx : x = 0 then 0 else (of_add (-1 : ℤ)) ^
    (exists_mul_exp_extension_on_units K
      (is_unit_iff_ne_zero.mpr hx).unit).some
```

To connect the extended norm and the extended valuation we prove in pow_eq_pow_root_zero_coeff that for every multiple d of $\deg f_x$, the following equality holds:

$$\texttt{of\_add}\left(\log_n\left(|x|_L^d\right)\right) = v(a_0)^{\frac{d}{\deg f_x}} \qquad (2)$$

Using (2) we deduce that extension_def K L satisfies the properties in Definition 2.2 since spectral_norm K L is a multiplicative nonarchimedean norm on L (as proven in [13, §3.2]). We then prove that this valuation is discrete and that L is complete with respect to the induced uniform structure.

The next theorem we prove says that the integral closure O_L of the unit ball K° inside L is again a discrete valuation ring (we refer to [6, Chapitre 5, §2, n°1] for generalities about integral closures). This follows from the fact that O_L is actually equal to the unit ball with respect to the extended discrete valuation on L, formalized as

```
lemma integral_closure_eq_integer :
  integral_closure hv.v.valuation_subring L =
  (extended_valuation K L).valuation_subring
```

3 Local Fields

In this section we describe our formalization of the basic theory of local fields, a special kind of discretely valued fields which are fundamental objects of study in number theory. For instance, given a number field L with ring of integers O_L, one can subsequently apply the constructions of Example 2.3 to the different maximal ideals $\mathfrak{m} \subseteq O_L$ — thus obtaining a collection of DVR's — followed by the completion procedure described in §2.4. The resulting collection of fields $\widehat{L}_\mathfrak{m}$ are precisely the local fields occurring in the "local-to-global" approach to class field theory briefly mentioned in the Introduction.

Before giving the definition, we make a preliminary observation. Theorem 2.5 shows that every DVR is a local ring, so it has a unique maximal ideal. On the other hand, given a field K endowed with a discrete valuation, the code excerpt 2 shows that its unit ball K° is a DVR, whose maximal ideal we denote $\mathfrak{m}_{K^\circ}$. It is then possible to unambiguously (although slightly inappropriately) speak of the *residue field* of K to mean the field $K^\circ/\mathfrak{m}_{K^\circ}$.

Definition 3.1. A *local field* is a field complete with respect to a discrete valuation and with finite residue field.

The definition is implemented as follows:

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

Remark 3.2. What we call "local fields" are normally referred to as "nonarchimedean local fields", to distinguish them from the archimedean local fields $\mathbb{R}$ and $\mathbb{C}$. Since we only consider the nonarchimedean case in this work, we have opted for this simplification. Observe that the requirement that the residue field is finite is sometimes omitted. Accordingly, the completion $\widehat{\mathbb{C}(X)}$ is a valued field with residue field $\mathbb{C}$ that we do not qualify to be local, although this is sometimes the case in the literature.

A local field K can be of two kinds: of *equal characteristic*, if both K and its residue field have characteristic p for some prime number p, or of *mixed characteristic*, if K has characteristic 0 and its residue field has characteristic p. Moreover, in the first case K is a finite extension of $\mathbb{F}_p((X))$ while in the second it is a finite extension of $\mathbb{Q}_p$ (see [6, Chapitre VI, §9, n°3]); this motivates our definitions in §§3.1–3.2.

3.1 Equal characteristic

Recall that we denote by $\widehat{\mathbb{F}_p(X)}$ the completion of $\mathbb{F}_p(X)$ with respect to the maximal ideal $\mathfrak{m} = (X)$.

Definition 3.3. An *equal characteristic local field* is a finite dimensional field extension of $\widehat{\mathbb{F}_p(X)}$, for some prime number p.

This definition is formalized as :

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

The first example of equal characteristic local field is $\widehat{\mathbb{F}_p(X)}$ itself, and we record our proof of this in the instance FpX_completion .eq_char_local_field. Being a finite extension of the complete discretely valued field $\widehat{\mathbb{F}_p(X)}$, any equal characteristic local field K is endowed with a unique nontrivial valuation, which is again discrete, and K is complete with respect to it.

```
instance : valued K ℤₘ₀ :=
extension.valued (FpX_completion p) K
instance : complete_space K :=
extension.complete_space (FpX_completion p) K
instance : is_discrete
  (eq_char_local_field.valued p K).v :=
extension.is_discrete_of_finite
  (FpX_completion p) K
```

Remark 3.4. Given any field K, the X-adic completion $\widehat{K(X)}$ of the field of rational functions is isomorphic to the field of Laurent series indexed by $\mathbb{Z}$ with only finitely many negative nonzero coefficients:

$$K(\!(X)\!) = \Big\{ f = \sum_{n \in \mathbb{Z}} a_n X^n \mid a_n \in K \text{ and } a_n = 0 \text{ if } n \ll 0 \Big\}.$$

Accordingly, the unit ball $\big(\widehat{K(X)}\big)^{\circ}$ is isomorphic to the ring of power series

$$K[[X]] = \Big\{ \sum a_n X^n \in K(\!(X)\!) \mid a_n = 0 \, \forall \, n \leq 0, \Big\}.$$

It is customary to define an equal characteristic local field as a finite extension of $\mathbb{F}_p(\!(X)\!)$ rather than of $\widehat{\mathbb{F}_p(X)}$, because elements in $\mathbb{F}_p(\!(X)\!)$ are explicit and it might be handier to work with them than with elements in $\widehat{\mathbb{F}_p(X)}$. While in pen-and-paper mathematics one can safely treat finite extensions of the two fields as leading to the same definition, we have to pick a choice in our formalization project. Since our development of extensions of complete DVR is very general and does not rely on any explicit description of the base field, and in analogy with our approach to the mixed characteristic case (see §3.2), we decide to use the type $\widehat{\mathbb{F}_p(X)}$ as the base field in our Definition 3.5. Moreover, the isomorphism $K(\!(X)\!) \cong \widehat{K(X)}$ is still not available in mathlib and we describe our formalization of this isomorphism in §3.1.1.

Our next task is to show that an equal characteristic local field K is a local field, in the sense of Definition 3.1. We have formalized this proof under the hypothesis that the extension $K/\widehat{\mathbb{F}_p(X)}$ is separable, as this is required to apply the mathlib lemma `is_integral_closure.is_noetherian` which we are using in our proof of the finiteness of the residue field. However, we point out that the separability assumption can be removed at the expense of a more involved proof, which we plan to formalize at a later date.

Since $\widehat{\mathbb{F}_p(X)}$ is a field complete with respect to a discrete valuation and K is a finite extension of $\widehat{\mathbb{F}_p(X)}$, by the discussion following (2), the X-adic valuation on $\widehat{\mathbb{F}_p(X)}$ induces a complete discretely valued structure on K, registered in the instance `eq_char_local_field.valued p K`. Hence it only remains to prove that the residue field of K is finite. To prove the finiteness statement, we first show that if E is a field complete with respect to a discrete valuation and L/E is a finite separable field extension, then the residue field of L is finite dimensional over the residue field of E:

```
finite_dimensional (residue_field E₀)
  (residue_field (integral_closure E₀ L))
```

This implies that if the residue field of E is finite, then so is the residue field of L. Now, it follows from the isomorphism $\mathbb{F}_p(\!(X)\!) \cong \widehat{\mathbb{F}_p(X)}$ discussed in §3.1.1 that $E = \widehat{\mathbb{F}_p(X)}$ has residue field $\mathbb{F}_p$, so every equal characteristic local field has finite residue field, and is therefore a local field.

The *ring of integers* of an equal characteristic local field K, denoted $\mathcal{O}_K$, is the integral closure of $\big(\widehat{\mathbb{F}_p(X)}\big)^{\circ}$ in K:

```
def ring_of_integers :=
integral_closure (FpX_int_completion p) K
```

The lemma `integral_closure_eq_integer` implies that $\mathcal{O}_K = K^{\circ}$, that is, an element of K is integral over $\big(\widehat{\mathbb{F}_p(X)}\big)^{\circ}$ if and only if its valuation is less than or equal to 1. A pivotal consequence of this equality is that $\mathcal{O}_K$ is a discrete valuation ring:

```
instance : discrete_valuation_ring (𝒪 p K) :=
integral_closure.dvr_of_finite_extension
  (FpX_completion p) K
```

3.1.1 Formalizing the isomorphism $K(\!(X)\!) \cong \widehat{K(X)}$.

Due to the relatively recent appearance of the theory of adic valuations in mathlib, the isomorphism $K(\!(X)\!) \cong \widehat{K(X)}$ was not formalized at the time of our work. Nevertheless the API for working with completions of uniform spaces and uniform fields is quite rich, as described in §2.4. The key ingredient for the formalization is the notion of *abstract completion* of uniform spaces. Given a uniform space T, a term `pkg : abstract_completion T` contains seven fields, the three most relevant for us being

i) `pkg.space`, the underlying uniform space endowed with a map `coe : pkg ⟶ T`;
ii) `pkg.complete`, which is a proof that `pkg.space` is complete;
iii) `pkg.dense_coe`, which is a proof that `coe` is injective with dense image.

In particular, there is a term `ratfunc_adic_compl_pkg` whose `space` field represents the completion $\widehat{\mathbb{F}_p(X)}$. Now, given two terms `(pkg, pkg': abstract_completion T)`, the declaration `compare pkg pkg'` provides an equivalence of uniform spaces between them, which expresses the mathematical statement that “the completion of a uniform space is unique up to a unique isomorphism”. The uniqueness of the extension (1) makes it easy to upgrade the equivalence to an equivalence of fields whenever both `pkg.space` and `pkg'.space` are fields. It follows that once we prove that $K(\!(X)\!)$ is also an abstract completion of $K(X)$, it will correspond to a term `laurent_series_pkg` and the previous discussion produces the required isomorphism, in the form

```
def laurent_series_ring_equiv :
   (laurent_series K) ≃+* (ratfunc_adic_compl K)
```

Code excerpt 5. The isomorphim between the Laurent series and the completion of rational functions.

To prove that $K((X))$ is a completion of $K(X)$, we need to show that $K((X))$ is complete and that the image of the coercion $K(X) \hookrightarrow K((X))$ is dense. Ultimately, both results rely on a careful study of the interaction between the X-adic valuation on $K(X)$, the X-adic valuation on $K((X))$[5], and the coefficients of the corresponding series. For example, we show in the lemma

```
lemma valuation_le_iff_coeff_zero_of_lt {D : ℤ}
  {f : laurent_series K} : v f ≤ (of_add (-D))
  ↔ (∀ n : ℤ, n < D → f.coeff n = 0)
```

that a Laurent series has valuation bounded by `of_add (-D )` if and only if its n-th coefficient vanishes for each $n < D$. Once we can relate the valuation and the vanishing of the coefficients, the proof that $K(X)$ has dense image in $K((X))$ is very smooth. The proof of completeness heavily relies on the formalism of filters, as explained in [8, §4]. The main ingredient is the

```
lemma uniform_continuous_coeff (d : ℤ)
  (h : uniformity K = 𝓟 id_rel) :
  uniform_continuous (coeff d)
```

It shows that if K is endowed with the *discrete* uniformity ([5, Chapitre II, §1, n°1, Exemple 2]), the map $f \mapsto a_d(f)$ sending a Laurent series to its d-th coefficient is uniformly continuous, for every $d \in \mathbb{Z}$. The consequence (see [5, Chapitre II, §3, n°1, Proposition 3]) is that for every Cauchy filter $\mathscr{F}$ in $K((X))$, the push-forward $f(\mathscr{F})$ is a Cauchy filter of the discrete space K and thus converges to a point $c_d(\mathscr{F})$. It is then easy to combine the above results linking coefficients and valuation to show that, for every Cauchy filter $\mathscr{F}$, the value $c_d(\mathscr{F})$ vanishes for $d \ll 0$ and therefore

$$f(\mathscr{F}) = \sum_{d\in\mathbb{Z}} c_d X^d \in K((X)).$$

In the lemma `cauchy.eventually_mem_nhds` we then show that $\mathscr{F}$ converges to the principal filter $\mathcal{P}(f(\mathscr{F}))$, proving that $K((X))$ is complete. Finally, we can specialize to $K[[X]]$ the equivalence `laurent_series_ring_equiv` to get its integral version:

```
def power_series_ring_equiv : (power_series K)
  ≃+* ((ideal_X K).adic_completion_integers
      (ratfunc K))
```

Code excerpt 6. The isomorphism between power series and the unit ball in the completion of rational functions.

In particular, we see that the residue field of $\widehat{K(X)}$ is isomorphic to the residue field of $K((X))$, hence to K itself. The special case when $K = \mathbb{F}_p$ yields the finiteness of the residue field of $\widehat{\mathbb{F}_p(X)}$ mentioned in §3.1.

3.2 Mixed characteristic

The main formalization challenge we face when formalizing the definition of mixed characteristic local fields is analogous to the issue discussed in Remark 3.4. The basic API for the p-adic numbers $\mathbb{Q}_p$ was already available in `mathlib`, but it predated the formalization of adic valuations. Since we want to take advantage of this more general theory, our approach is to define a new type $\widehat{\mathbb{Q}}_{(p)}$

```
def Q_p : Type* :=
adic_completion ℚ (p_height_one_ideal p)
```

and to prove that it is isomorphic, as a valued field, to the field $\mathbb{Q}_p$. This isomorphism is established in the definition `padic_equiv` and its construction follows the main strategy explained in §3.1.1. Namely, we provide two abstract completions `padic_pkg` and `padic_pkg'` of $\mathbb{Q}$ and we upgrade the equivalence as uniform spaces to an isomorphism of valued fields. As a consequence, the unit ball $\left(\widehat{\mathbb{Q}}_{(p)}\right)^\circ$, called (`Z_p p`) in our code, is proved to be isomorphic to the p-adic integers $\mathbb{Z}_p$ in the declaration

```
def padic_int_ring_equiv : (Z_p p) ≃+* ℤ_[p]
```

Code excerpt 7. The isomorphism between $\left(\widehat{\mathbb{Q}}_{(p)}\right)^\circ$ and $\mathbb{Z}_p$.

We are now ready to give the following definition:

Definition 3.5. A *mixed characteristic local field* is a finite dimensional field extension of the field $\widehat{\mathbb{Q}}_{(p)}$, for some p.

This is implemented as

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

In particular, $\widehat{\mathbb{Q}}_{(p)}$ is a mixed characteristic local field.

We formalize the proof that any mixed characteristic local field K is a local field as in Definition 3.1. The proof is analogous to the one in the equal characteristic case: the only difference is that every mixed characteristic local field K is automatically separable over $\widehat{\mathbb{Q}}_{(p)}$, since this holds for every algebraic extension of a field of characteristic 0. Hence, we do not need to assume separability. Finally, the ring isomorphism in the code excerpt 7 implies that the residue field of $\left(\widehat{\mathbb{Q}}_{(p)}\right)^\circ$ is isomorphic to $\mathbb{F}_p$, since this is the case for $\mathbb{Z}_p$. As above, this ensures that every mixed characteristic local field is indeed a local field according to Definition 3.1:

```
def mixed_char_local_field.local_field :
    local_field K :=
{ complete := mixed_char_local_field.
    complete_space p K,
  is_discrete := v.valuation.is_discrete p K,
```

[5] Despite having the same name, these valuations are associated to different ideals: one is $(X) \subseteq K[X]$ and the other is $(X) \subseteq K[[X]]$.

```
  finite_residue_field := ...,
  ..(mixed_char_local_field.valued p K) }
```

The extension of the p-adic valuation to K is the unique nontrivial discrete valuation on K, and the field K is complete with respect to the induced topology.

The *ring of integers* O_K of a mixed characteristic local field K is the integral closure of $(\widehat{\mathbb{Q}}_{(p)})^{\circ}$ in K.

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

As in the equal characteristic case, we have that $O_K = K^{\circ}$, so in particular O_K is a discrete valuation ring.

4 Discussion

4.1 Future work

Our next project is to prove that every local field is either a mixed characteristic local field or an equal characteristic local field, and that completions of global fields at finite places are local fields. We will then relate unramified extensions of local fields with extensions of their residue fields, showing that they are all (pro-)cyclic. This paper describes one of the first steps in a larger scale project aiming at formalizing local class field theory. We plan to formulate it in cohomological terms, relying on the recent work [18] by Livingston.

4.2 Related works

We formalize our work on top of the Lean 3 library `mathlib` and the Lean 3 project [13] formalizing extensions of norms. The basic theory of DVR's was available in `mathlib` at the start of our project. The library includes a formalization of the additive valuation on a DVR but we discuss in §4.3 our choice of working with $\mathbb{Z}_{\mathrm{m}0}$-valued valuations instead.

As far as other systems are concerned, the first formalization of the p-adic numbers appeared in the Coq UniMath library in [19]. Beyond the choice of the theorem prover, the two major differences with our work come from different axiomatization settings: the authors of [19] assume the univalence axiom and work in a constructive setting, replacing the notion of being non-zero with a property of being "apart from zero". As a consequence, their construction of the p-adic integers $\mathbb{Z}_p$ follows a completely different path and involves a "carrying" operator on the ring $\mathbb{Z}[[X]]$ and an equivalence relation based on univalent "paths" rather than equality. The field $\mathbb{Q}_p$ is then defined as the Heyting field of fractions of $\mathbb{Z}_p$, a construction mimicking the usual field of fractions of an integral domain but in the setting of apartness domains. No treatment of the p-adic valuation, of the p-adic metric and more generally of topological properties is presented *ibid*. From the algebraic point of view, neither the properties of being a DVR, a Dedekind domain, or a local ring, nor algebraic extensions of $\mathbb{Q}_p$, are approached.

The p-adic numbers were later formalized in Isabelle/HOL, whose main library also contains a formalization of formal Puiseux series. The formalization of $\mathbb{Z}_p$ in [10] follows the classical path and is quite complete: both the definition as inverse limit and as completion of $\mathbb{Z}$ with respect to the p-adic valuation are formalized, together with a proof of their equivalence and of Hensel's lemma. The basic results of the topological properties of $\mathbb{Z}_p$ can also be found *ibid*., and the paper [11] contains deeper results: the field $\mathbb{Q}_p$ is defined as the fraction field of the ring $\mathbb{Z}_p$ formalized in the previous work, and it is endowed with both a valuation and a norm extending the previous ones on $\mathbb{Z}_p$. Again, the main topological properties both of $\mathbb{Q}_p$ and of $\mathbb{Q}_p^n$ are studied. Nevertheless, neither the structure of $\mathbb{Z}_p$ as a DVR, or as a Dedekind domain, are addressed; also, there is no treatment of finite extensions of $\mathbb{Q}_p$ or of localization results.

The work [15] presents the formalization of the ring $R\{\{X\}\}$ of Puiseux series (over any commutative ring R), that are a generalization of Laurent series. Both $R[[X]]$ and $R((X))$ are defined and studied *ibid*., and are endowed with a valuation and a norm, whose basic properties are formalized and extended to

$$R\{\{X\}\} = \bigcup_{d \geq 1} R((X^{1/d})).$$

The main focus of the paper is the formalization of the Newton–Puiseux' theorem stating that whenever C is an algebraically closed field of characteristic 0, the same holds for $C\{\{X\}\}$; as a consequence, few algebraic properties both of $\mathbb{F}_p((X))$ and of $\mathbb{F}_p\{\{X\}\}$ are formalized. In particular, no formalization of the DVR structure of $\mathbb{F}_p[[X]]$ or of field extensions of $\mathbb{F}_p((X))$ can be found *ibid*.

4.3 Remarks about the Implementation

Additive and multiplicative valuations. The `mathlib` library prioritizes multiplicative valuations over additive ones, providing a much wider API for the first ones. For example, the general theory of valuation rings is framed in terms of multiplicative valuations. Moreover, while `mathlib` does not yet include the definition of discrete valuation, it does provide specific examples, such as adic valuations on Dedekind domains, which take values in $\mathbb{Z}_{\mathrm{m}0}$.

On the other hand, `mathlib` only provides the formalization of the *additive* valuation `add_val` on a discrete valuation ring, taking values in `part_enat`, a decidable version of the type `enat=`$\mathbb{N} \cup \{\infty\}$. For consistency with the rest of the library, we propose to replace `add_val` with our implementation of the multiplicative valuation.

Uniformizers. To indicate that a term `(π: R)` in a ring R is a uniformizer for a valuation v_R, we provide a predicate `is_uniformizer`:

```
def is_uniformizer (π : R) : Prop :=
vR π = (of_add (- 1 : ℤ) : ℤₘ₀)
```

We also provide a bundled version of this definition, called `uniformizer`. That is, we provide a structure `uniformizer` whose terms consists of two fields: an element π of the ring R, together with the proof that π is a uniformizer for a given valuation. Since any uniformizer is necessarily a member of the unit ball, we decided to make the field π in this definition a term of type `vR.integer` (as opposed to type `R`).

```
structure uniformizer :=
(π : vR.integer)
(valuation_eq_neg_one : is_uniformizer vR π)
```

The proposition `is_uniformizer` is useful when proving lemmas that apply to any uniformizer element, such as the lemma stating that every uniformizer is nonzero:

```
lemma uniformizer_ne_zero {π : R}
  (hπ : is_uniformizer vR π) : π ≠ 0 :=
```

By contrast, the bundled definition is more convenient to prove results that involve fixing a uniformizer. For example, we use it when proving that every nonzero $r : K^\circ$ can be factored as the product of a unit by a power of a fixed uniformizer:

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

For an in-depth discussion of bundled versus unbundled representations in Lean and in Coq, we refer the reader to [1] or [21].

Extensions and* `valued` *instances. In §2.5 we construct, for each field K complete with respect to a discrete valuation v and every finite extension L/K, a unique valuation v_L on L, recorded as (`v_L : valuation L ℤₘ₀`). However, at this level of generality we do not put a global `valued` instance on L: doing so would create infinitely many "diamonds", by which we mean the existence of two different procedures to endow an object with a certain mathematical structure (represented by two terms of the given structure that are propositionally, but not definitionally, equal). This leads to problems when exploiting the full force of the type-class inference mechanism: indeed, suppose that in a given context Γ, a term $t : T$ is well-typed assuming the existence of a term `s:S` for a certain structure `S`. Given two terms s_1,s_2:`S` that are propositionally equal, the corresponding terms t_1,t_2:`T` are different, yet carry the same mathematical information. Now, if the type-class inference mechanism can produce both terms s_1 and s_2 — say, inside a proof — the user would face the problem of having two different terms that look indistinguishable, which clearly leads to unexpected problems. In our setting, for every field K that is complete with respect to a discrete valuation v, the original valuation is propositionally but not definitionally equal to its trivial extension v_K, resulting in two terms of the structure of a `valued` field on K: to avoid any diamond, we need to exclude the second from the inference search, and therefore we need to avoid declaring a structure of `valued` field on the trivial extension K of K: this forces us to avoid declaring such a structure on *every* extension L/K. Nevertheless, we provide a lemma `trivial_extension_eq_valuation` proving the equality $v = v_K$.

We make an exception to this rule when implementing mixed and equal characteristic local fields, since we do declare `valued` instances for them. This creates a mild diamond for $\widehat{\mathbb{Q}}_{(p)}$ and $\widehat{\mathbb{F}_p(X)}$ but this does not cause trouble in our formalization, thanks to the comparison lemma `trivial_extension_` mentioned above. Indeed, in all cases where a the inference system would create problems, the lemma allows us to disambiguate the situation: for an example, the reader can inspect the proof of `FpX_int_completion.equiv_valuation_subring`, proving that the unit ball $\left(\widehat{\mathbb{F}_p(X)}\right)^\circ$ is isomorphic to the subring of $\widehat{\mathbb{F}_p(X)}$ whose elements have (X)-adic valuation less than or equal to $(1 : \mathbb{Z}_{\mathrm{m}0})$.

Fraction fields. If K is a discretely valued field, then K° is a DVR, so we put a [`valued (fraction_ring` K_0`)` $\mathbb{Z}_{\mathrm{m}0}$] instance on Frac(K°). Note that, while K and Frac(K°) are isomorphic, they are represented by different types in `mathlib`, so the above `valued` instance has a different type from the original [`valued K` $\mathbb{Z}_{\mathrm{m}0}$] instance and no diamond occurs. However, it would if we had instead decided to put this `valued` instance on any field L satisfying the condition [`is_fraction_ring` K_0 `L`], since this holds for K.

The* `normed_field` *and the* `valued` *instances. Recall from §2.5 that to each discrete valuation v on a field K we can associate a nonarchimedean multiplicative norm $|\cdot|_K$.

When there exists a preferred discrete valuation v on K, we often register it as a `valued` instance:

```
    {K : Type*} [field K] [hv : valued K ℤₘ₀]
```

In this situation, the norm $|\cdot|_K$ associated to v would be the preferred nontrivial norm on K , up to rescaling, and we would like to record a corresponding `normed_field` instance on K:

```
    {K : Type*} [normed_field K ℤₘ₀]
```

Note that the datum of a field is embedded into the definition of the `normed_field` class, while the class `valued` takes the field structure as an argument. It follows that declaring a `normed_field` instance on every field that carries a `valued` one leads to a loop in the typeclass inference system[6]. We discuss below a concrete example to illustrate this problem, for which we studied a trace of the instance search using the option `trace.class_instances` to track the typeclass inference process.

[6] Lean 4 can detect these kinds of simple loops, so this should not be an issue once our project has been ported to Lean 4.

Suppose that we had declared `discretely_normed_field` as an instance instead of as a definition, so that every discretely valued field

```
(K : Type*) [field K] [hv : valued K ℤₘ₀]
  [is_discrete hv.v]
```

would automatically inherit a `normed_field` instance. Under this assumption, the typeclass inference system would get into an infinite loop when searching for an instance of `valuation_ring hv.v.valuation_subring.to_subring`, because one of the first results that Lean tries to apply is `valuation_ring.of_field`, that automatically infers a valuation ring structure on every field. In turn, this reduces the problem at hand to finding an instance of `field hv.v.valuation_subring.to_subring`. This leads to a dead end (since the valuation subring is not a field); however, while trying to find this instance, the inference system finds `normed_field.to_field`, and hence it starts to search for an instance of `normed_field hv.v.valuation_subring.to_subring`, for which it will try to apply the definition `discretely_normed_field`, that as input requires a `field` instance on the valuation subring which recreates the problem discussed above, resulting in the system getting stuck in an infinite loop.

However, observe that no problem arises when putting both a `valued` and a `normed_field` instance on, for instance, $\mathbb{Q}_p$, because the typeclass inference system is able to find these instances only on $\mathbb{Q}_p$.

Laurent series. As for general DVR's, an additive valuation was already available in `mathlib` for power series, with the name `hahn_series.add_val`. It is `part_enat`-valued and it is defined as the greatest n such that X^n divides the power series. Although some basic API was available, the same reasons that led us to systematically work with multiplicative valuations rather than additive ones pushed us to rely on the general theory of $\mathbb{Z}_{m0}$-valued adic valuations rather than with this *ad hoc* definition.

The main isomorphism `laurent_series_ring_equiv` exhibited in the code excerpt 5 is defined as *the inverse* of an isomorphism

$$\texttt{ratfunc\_adic\_compl\_ring\_equiv} \; : \; \widehat{K(X)} \simeq^{+*} K((X)) \, .$$

The reason is that to prove additivity and multiplicativity of the above map it suffices to observe that it coincides with the extension $\widehat{\texttt{coe}}$ (in the sense of (1)) of the coercion

$$\texttt{coe} \; : \; K(X) \to^{+*} K((X)) \, .$$

The formalism of uniform completions suffices to establish that $\widehat{\texttt{coe}}$ is a ring homomorphism simply because `coe` is, whereas there exists no explicit ring homomorphism φ such that $\widehat{\varphi}$ = `laurent_series_ring_equiv`.

The field of p-adic numbers as adic completion. Although the formalization of the isomorphism $\widehat{\mathbb{Q}}_{(p)} \cong \mathbb{Q}_p$ follows in many respects the one for Laurent series, one notable difference is that the type $\mathbb{Q}$, unlike $K(X)$, already bore an instance of `metric_space`, induced from the euclidean distance, and this induced a uniform structure on $\mathbb{Q}$. In order to define the term $\widehat{\mathbb{Q}}_{(p)}$ we needed to access the API concerning completions of adic spaces, and to do so a `valued` instance needed to be defined on $\mathbb{Q}$. The corresponding uniform space structure would conflict with the euclidean one, and therefore we needed to locally disable the `metric_space` instance on $\mathbb{Q}$ already just to *define* the type $\widehat{\mathbb{Q}}_{(p)}$.

Acknowledgments

We would like to thank Riccardo Brasca, Mario Carneiro, Antoine Chambert-Loir and Rob Lewis for interesting discussions about possible formalizations of the p-adic numbers, Heather Macbeth for helpful conversations about the formalization of Laurent series, Yaël Dillies for providing access to some results about well-founded relations and Cyril Cohen for answering some questions about p-adic numbers in Coq. We also thank the `mathlib` community as a whole for their support during the completion of this project.

The first author acknowledges support from the Grant CA1/RSUE/2021-00623 funded by the Spanish Ministry of Universities, the Recovery, Transformation and Resilience Plan, and Universidad Autónoma de Madrid. She is also grateful for the one-month invitation from Université Jean Monnet Saint-Étienne, as part of the program "Appel à Projets Recherche UJM 2023".

This work was supported by the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "France 2030" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

References

[1] Anne Baanen. 2022. Use and Abuse of Instance Parameters in the Lean Mathematical Library. In *13th International Conference on Interactive Theorem Proving (ITP 2022) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 237)*, June Andronick and Leonardo de Moura (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 4:1–4:20. https://doi.org/10.4230/LIPIcs.ITP.2022.4

[2] Anne Baanen, Sander R. Dahmen, Ashvni Narayanan, and Filippo A. E. Nuccio Mortarino Majno di Capriglio. 2021. A Formalization of Dedekind Domains and Class Groups of Global Fields. In *12th International Conference on Interactive Theorem Proving (ITP 2021) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 193)*, Liron Cohen and Cezary Kaliszyk (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 5:1–5:19. https://doi.org/10.4230/LIPIcs.ITP.2021.5

[3] Anne Baanen, Sander R. Dahmen, Ashvni Narayanan, and Filippo A. E. Nuccio Mortarino Majno di Capriglio. 2022. A formalization of Dedekind domains and class groups of global fields. *J. Automat. Reason.* 66, 4 (2022), 611–637. https://doi.org/10.1007/s10817-022-09644-0

[4] Siegfried Bosch, Ulrich Güntzer, and Reinhold Remmert. 1984. *Non-archimedean analysis : a systematic approach to rigid analytic geometry.* Springer-Verlag Berlin Heidelberg, Berlin.

[5] Nicolas Bourbaki. 1971. *Éléments de mathématique. Topologie générale. Chapitres 1 à 4.* Hermann, Paris. 357 pages.

[6] Nicolas Bourbaki. 1985. *Éléments de mathématique. Algèbre commutative. Chapitres 5 à 7.* Masson, Paris. 351 pages.

[7] Nicolas Bourbaki. 2007. *Éléments de mathématique. Algèbre. Chapitres 4 à 7.* Springer, Berlin. 422 pages.

[8] Kevin Buzzard, Johan Commelin, and Patrick Massot. 2020. Formalising Perfectoid Spaces. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs* (New Orleans, LA, USA) *(CPP 2020)*. Association for Computing Machinery, New York, NY, USA, 299–312. https://doi.org/10.1145/3372885.3373830

[9] Mario Carneiro. 2019. The Type Theory of Lean. Master thesis. https://github.com/digama0/lean-type-theory/releases/download/v1.0/main.pdf.

[10] Aaron Crighton. 2021. Hensel's Lemma for the p-adic Integers. *Archive of Formal Proofs* (March 2021). https://isa-afp.org/entries/Padic_Ints.html, Formal proof development.

[11] Aaron Crighton. 2022. p-adic Fields and p-adic Semialgebraic Sets. Formal proof development. https://isa-afp.org/entries/Padic_Field.html.

[12] María Inés de Frutos-Fernández. 2022. Formalizing the Ring of Adèles of a Global Field. In *13th International Conference on Interactive Theorem Proving (ITP 2022) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 237)*, June Andronick and Leonardo de Moura (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 14:1–14:18. https://doi.org/10.4230/LIPIcs.ITP.2022.14

[13] María Inés de Frutos-Fernández. 2023. Formalizing Norm Extensions and Applications to Number Theory. In *14th International Conference on Interactive Theorem Proving (ITP 2023) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 268)*, Adam Naumowicz and René Thiemann (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 13:1–13:18. https://doi.org/10.4230/LIPIcs.ITP.2023.13

[14] Leonardo de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer. 2015. The Lean Theorem Prover (System Description). In *Automated Deduction - CADE-25 (Lecture Notes in Computer Science, Vol. 9195)*, Amy P. Felty and Aart Middeldorp (Eds.). Springer International Publishing, Cham, 378–388. https://doi.org/10.1007/978-3-319-21401-6_26

[15] Manuel Eberl. 2021. Formal Puiseux Series. https://isa-afp.org/entries/Formal_Puiseux_Series.html, Formal proof development.

[16] Gerhard Frey. 2009. The Way to the Proof of Fermat's Last Theorem. *Annales de la Faculté des sciences de Toulouse : Mathématiques* Ser. 6, 18, S2 (2009), 5–23. https://doi.org/10.5802/afst.1227

[17] Hendrik W. Lenstra and Peter Stevenhagen. 1997. Class Field Theory and the First Case of Fermat's Last Theorem. In *Modular Forms and Fermat's Last Theorem*, Gary Cornell, Joseph H. Silverman, and Glenn Stevens (Eds.). Springer New York, New York, NY, 499–503. https://doi.org/10.1007/978-1-4612-1974-3_18

[18] Amelia Livingston. 2023. Group Cohomology in the Lean Community Library. In *14th International Conference on Interactive Theorem Proving (ITP 2023) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 268)*, Adam Naumowicz and René Thiemann (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 22:1–22:17. https://doi.org/10.4230/LIPIcs.ITP.2023.22

[19] Álvaro Pelayo, Vladimir Voevodsky, and Michael A. Warren. 2015. A univalent formalization of the p-adic numbers. *Mathematical Structures in Computer Science* 25, 5 (2015), 1147–1171. https://doi.org/10.1017/S0960129514000541

[20] Jean-Pierre Serre. 1962. *Corps locaux.* Publications de l'Institut de Mathématique de l'Université de Nancago 8. Actualités Scientifiques et Industrielles, Vol. 1296. Hermann, Paris. 243 pages.

[21] Bas Spitters and Eelis van der Weegen. 2011. Type classes for mathematics in type theory. *Mathematical Structures in Computer Science* 21, 4 (2011), 795–825. https://doi.org/10.1017/S0960129511000119

[22] John T. Tate. 1967. Global class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965).* Thompson, Washington, D.C., 162–203.

Received 2023-09-19; accepted 2023-11-25