Formalizing the Ring of Adèles of a Global Field

María Inés de Frutos-Fernández
Imperial College London, UK

Abstract

The ring of adèles of a global field and its group of units, the group of idèles, are fundamental objects in modern number theory. We discuss a formalization of their definitions in the Lean 3 theorem prover. As a prerequisite, we formalize adic valuations on Dedekind domains. We present some applications, including the statement of the main theorem of global class field theory and a proof that the ideal class group of a number field is isomorphic to an explicit quotient of its idèle class group.

2012 ACM Subject Classification Theory of computation → Logic and verification; Theory of computation → Type theory

Keywords and phrases formal math, algebraic number theory, class field theory, Lean, mathlib

Digital Object Identifier 10.4230/LIPIcs.ITP.2022.14

Supplementary Material
Software (Source Code): `https://github.com/mariainesdff/ideles-journal`
InteractiveResource (Website): `https://mariainesdff.github.io/ideles-journal/`

Funding EPSRC Grant EP/V048724/1: Digitising the Langlands Program (UK).

Acknowledgements I would like to thank Kevin Buzzard for his constant support and for many helpful conversations during the completion of this project, and Ashvni Narayanan for pointing out that the finite adèle ring can be defined for any Dedekind domain. I am also grateful to Patrick Massot for making some of the topological prerequisites available in `mathlib`, and to Sebastian Monnet for formalizing the topology on the infinite Galois group. Finally, I thank the `mathlib` community for their helpful advice, and the `mathlib` maintainers for the insightful reviews of the parts of this project already submitted to the library.

1 Introduction

Number theory is the branch of mathematics that studies the ring of integer numbers $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$, the rational numbers. While this description may seem deceptively simple, it is a very rich area, involving myriads of abstractions and techniques.

Consider for example the problem of finding all integer solutions to a polynomial equation in several variables (a "Diophantine equation"). Perhaps the most famous of these equations is $x^n + y^n = z^n$, where n is an integer greater than 2. Fermat's Last Theorem tells us that this equation has no integer solutions for which the product xyz is nonzero. While Fermat was able to state this conjecture around 1637, its proof was not concluded until 1995, although some particular cases were established sooner.

The general proof, due to Wiles and Taylor, is built upon the combined work of hundreds of mathematicians who over the last couple of centuries developed a rich arithmetic theory of elliptic curves, modular forms and Galois representations. The key result is a special case of the Taniyama–Shimura–Weil conjecture. If we want to be able to formalize a complete proof of Fermat's Last Theorem in a theorem prover, we first need to formalize all the necessary ingredients.

In this paper we formalize the ring of adèles and the group of idèles of a *global field* (a generalization of the field $\mathbb{Q}$). As a consequence of our work we are able to state the main theorem of global class field theory. Class field theory is needed for the proof of the

Taniyama–Shimura–Weil conjecture, which implies Fermat's Last Theorem. Adèles and idèles are used in many areas of current research, including the theory of automorphic forms and the Langlands program, an ambitious group of conjectures that seek to establish deep connections between geometry and number theory.

Our formalization was carried out using the Lean 3 theorem prover [9]. At the time of writing this paper, the source code is in the process of being integrated in Lean's mathematics library `mathlib`. We provide a public repository[1] containing the version of the code referred to in this article and the associated documentation[2] in HTML format. This is the first time that adèles and idèles have been formalized in any theorem prover.

Before describing our formalization, we give a quick overview of the ring of adèles of $\mathbb{Q}$. When studying the rational numbers, both algebraic and analytic methods can be employed. A natural way to do analysis over $\mathbb{Q}$ is by regarding it as a subspace of the real numbers $\mathbb{R}$, which are by definition the completion of $\mathbb{Q}$ with respect to the usual absolute value. However, this is not the only absolute value that can be defined on $\mathbb{Q}$: in fact, for every prime number p, there is a p-adic absolute value $|\cdot|_p$ and we can consider the corresponding completion $\mathbb{Q}_p$ of $\mathbb{Q}$. Ostrowki's theorem tells us that, up to equivalence, there are no more nontrivial absolute values on the rational numbers.

We remark that while the field $\mathbb{Q}_p$ of p-adic numbers is a basic object in number theory, it was not formalized in any proof assistant until 2015, when Pelayo, Voevodsky, and Warren formalized it in the Coq UniMath library [15]. The p-adic numbers were added to Lean's mathematical library `mathlib` in 2018, by R. Y. Lewis [12].

Since the various absolute values on $\mathbb{Q}$ provide us with different insights about the rationals, a natural question is whether it is possible to study all of them simultaneously. A first approximation would be to consider the product of the completions with respect to each absolute value. However, for technical reasons it is better to work with the following subset of the product:

$$\mathbb{A}_{\mathbb{Q}} := \prod_p{}' \mathbb{Q}_p \times \mathbb{R} := \left\{ (x_p)_p \in \prod_p \mathbb{Q}_p \;\middle|\; |x_p|_p \leq 1 \text{ for all but finitely many } p \right\} \times \mathbb{R}.$$

$\mathbb{A}_{\mathbb{Q}}$ is a ring under component-wise addition and multiplication, it contains $\mathbb{Q}$ as a subring via the diagonal map $r \mapsto ((r)_p, r)$, and it can be endowed with a topology that makes it into a locally compact topological ring. We call $\mathbb{A}_{\mathbb{Q}}$ the ring of adèles or adèle ring of $\mathbb{Q}$ and $\mathbb{A}_{\mathbb{Q},f} := \prod_p{}' \mathbb{Q}_p$ its finite adèle ring. The groups of units of these rings are respectively called the idèle group $\mathbb{I}_{\mathbb{Q}}$ and finite idèle group $\mathbb{I}_{\mathbb{Q},f}$ of $\mathbb{Q}$.

The definitions of adèle ring and idèle group can be generalized to any global field K [2]; see sections 3 and 4 for the details. Global fields are one of the main subjects of study in algebraic number theory and they can be of two kinds: number fields, which are finite extensions of the field $\mathbb{Q}$, and function fields, which are finite extensions of the field $\mathbb{F}_q(t)$ of rational functions over a finite field $\mathbb{F}_q$.

Every global field is the field of fractions of a Dedekind domain, but the converse is not true. However, the definition of finite adèle ring makes sense for any Dedekind domain, so we have formalized it in that degree of generality.

[1] `https://github.com/mariainesdff/ideles-journal`
[2] `https://mariainesdff.github.io/ideles-journal/`

1.1 Lean and mathlib

Lean 3 is a functional programming language and interactive theorem prover [9] based on dependent type theory, with proof irrelevance and non-cumulative universes [7]. For an introduction to Lean, see for instance [3].

This project is based on Lean's mathematical library `mathlib`, which is characterized by its decentralized nature with over 200 contributors. Due to the distributed organization of `mathlib`, it is impossible to cite every author who contributed a piece of code that we used. However, we remark that our formalization makes extensive use of the theory of Dedekind domains [4] and of the theory of uniform spaces and completions, originally developed in the perfectoid space formalization project [6].

In Lean's core library and `mathlib`, type classes are used to handle mathematical structures on types. For example, the type class `ring` packages two operations, addition and multiplication, as well as a list of properties they must satisfy. Then, given a type `R`, we can declare an instance `[ring R]`, and Lean's instance resolution procedure will infer that `R` has a ring structure. Besides `instance`, whose behaviour we have just described, we use in this paper the keywords `variables`, `def`, `lemma` and `theorem`, which have the evident meaning.

1.2 Structure of the paper

We start Section 2 with some background on Dedekind domains and their nonarchimedean absolute values, which we then use to define the finite adèle ring and the finite idèle group and explore how the latter is related to the group of invertible fractional ideals. In Section 3, we build on this work to define the adèle ring, the idèle group and the idèle class group of a number field, while in Section 4 we treat the function field case. In Section 5 we discuss two applications of the idèle group to class field theory. Finally, we conclude Section 6.1 with some implementation remarks and a discussion of future work connected to this project.

2 The finite adèle ring of a Dedekind domain

2.1 Dedekind domains and adic valuations

There are several equivalent definitions of Dedekind domain, three of which have been formalized in `mathlib` [4]. We work with the one formalized in `is_dedekind_domain` : a Dedekind domain R is an integrally closed Noetherian integral domain with Krull dimension 0 or 1 [14].

A Dedekind domain of Krull dimension 0 is a field. In this project we will only consider Dedekind domains of Krull dimension 1, for which the maximal ideals are exactly the nonzero prime ideals. Some examples are the integers $\mathbb{Z}$, the Gaussian integers $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$, or the ring of univariate polynomials $k[X]$ over a field k. All of these examples are unique factorization domains; however, not every Dedekind domain is. For instance, $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is a Dedekind domain but not a unique factorization domain, since elements like $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ admit two genuinely distinct factorizations.

The maximal spectrum of R is the set of its maximal ideals (implemented as a type in Lean). The fraction field K of R is the smallest field containing R; its elements can be represented by fractions r/s, where r and s are in R and s is nonzero. For example, the fraction fields of $\mathbb{Z}$, $\mathbb{Z}[i]$, and $k[X]$ are respectively $\mathbb{Q}$, $\mathbb{Q}(i) := \{a + bi \mid a, b \in \mathbb{Q}\}$, and the field $k(X)$ of rational functions over k.

```
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]
-- Note : not the maximal spectrum if R is a field
structure maximal_spectrum :=
(as_ideal : ideal R)
(is_prime : as_ideal.is_prime)
(ne_bot   : as_ideal ≠ ⊥)
variable (v : maximal_spectrum R)
```

Let R be a Dedekind domain (of Krull dimension 1). Then every nonzero ideal of R can be written as a product of maximal ideals, and this factorization is unique up to reordering. In particular, given an element $r \in R$ and a maximal ideal v of R, we can count how many times v appears in the factorization of the principal ideal (r), and this defines a nonarchimedean additive valuation on R [10, Chapter II], that is, a function $\mathrm{val}_v : R \to \mathbb{Z} \cup \{\infty\}$ such that

1. $\mathrm{val}_v(r) = \infty$ if and only if $r = 0$,
2. $\mathrm{val}_v(rs) = \mathrm{val}_v(r) + \mathrm{val}_v(s)$ for all r, s in R, and
3. $\mathrm{val}_v(r + s) \geq \min\{\mathrm{val}_v(r), \mathrm{val}_v(s)\}$ for all r, s in R.

The function val_v is called the v-adic valuation on R. It can be extended to a valuation on the fraction field K of R by defining $\mathrm{val}_v(r/s) := \mathrm{val}_v(r) - \mathrm{val}_v(s)$. For example, when $R = \mathbb{Z}$ and $v = (p)$ is the ideal generated by a prime number, val_v is the p-adic valuation on $\mathbb{Z}$ and $\mathbb{Q}$.

For both theoretical and implementation reasons, it is more convenient to work with the multiplicative version of the valuation: given any real number $n_v > 1$, we define a function $|\cdot|_v : R \to n_v^{\mathbb{Z}\cup\{-\infty\}} = n_v^{\mathbb{Z}} \cup \{0\}$ sending r to $n_v^{-\mathrm{val}_v(r)}$. From the definition of val_v, we immediately deduce that $|\cdot|_v$ has the following properties:

(i) $|r|_v = 0$ if and only if $r = 0$,
(ii) $|rs|_v = |r|_v|s|_v$ for all r, s in R, and
(iii) $|r + s|_v \leq \max\{|r|_v, |s|_v\}$ for all r, s in R.

A function $|\cdot|_v$ satisfying conditions (i) – (iii) is called a nonarchimedean absolute value (note that the third condition is stronger than $|r + s|_v \leq |r|_v + |s|_v$). The choice of n_v used in the definition is not relevant, in the sense that any two choices of n_v will yield equivalent absolute values. If, instead of property (iii), the function $|\cdot|_v$ satisfies only the weaker condition $|r + s|_v \leq |r|_v + |s|_v$, we say that it is an archimedean absolute value.

We formalized the v-adic absolute value on R in `mathlib` using the structure `valuation`, which consists on a function $|\cdot|$ from a ring R to a `linear_ordered_comm_monoid_with_zero` Γ_0 satisfying conditions (ii) and (iii), plus $|0| = 0$ and $|1| = 1$. We chose Γ_0 equal to `with_zero (multiplicative ℤ)`, which is a way to represent $n_v^{\mathbb{Z}} \cup \{0\}$ in Lean : if `T` is a type that carries some additive structure, then `multiplicative T` carries the corresponding multiplicative structure. The definition `with_zero` is used to add a new element 0 to a given type.

In the code below, if r is a nonzero element of R, we use `(associates.mk (ideal.span r : ideal R)).factors` to obtain the multiset of factors of the ideal (r) and we count how many times the maximal ideal v appears in this factorization with `(associates.mk v.as_ideal).count`. This count is returned as a natural number; after coercing to $\mathbb{Z}$ and taking its negative, we use `multiplicative.of_add` to get the corresponding element of `multiplicative ℤ`.

Let us briefly explain why we use `associates.mk` in this definition. Two elements of a monoid are associated if they differ by multiplication by a unit, and this defines an equivalence relation. In `mathlib`, given a monoid `M`, `associates M` is the quotient of `M` by this equivalence relation, and `associates.mk` is the canonical map sending an element to its equivalence class.

Two ideals of a commutative ring are associated if and only if they are equal, so from a mathematical point of view, the associated relation is trivial in this case. However, from an implementation point of view, it is more convenient to work with associates than to work directly with ideals, since the corresponding factorization API (that is, the collection of available definitions and lemmas) is more extensive.

```
def int_valuation_def (r : R) : with_zero (multiplicative ℤ) :=
if r = 0 then 0 else multiplicative.of_add (-(associates.mk v.as_ideal).count
  (associates.mk (ideal.span {r} : ideal R)).factors : ℤ)
def int_valuation : valuation R (with_zero (multiplicative ℤ)) :=
{ to_fun           := v.int_valuation_def,
  map_zero'        := int_valuation.map_zero' v,
  map_one'         := int_valuation.map_one' v,
  map_mul'         := int_valuation.map_mul' v,
  map_add_le_max'  := int_valuation.map_add_le_max' v }
```

We extended `int_valuation` to a `valuation` on the fraction field K, by setting the valuation of a fraction to be the valuation of the numerator divided by the valuation of the denominator. We checked in `lemma valuation_well_defined` that this definition does not depend on the choice of fraction used to represent an element of K.

```
def valuation_def (x : K) : (with_zero (multiplicative ℤ)) :=
let s := classical.some (classical.some_spec (is_localization.mk'_surjective
  (non_zero_divisors R) x)) in
  (v.int_valuation_def (classical.some (is_localization.mk'_surjective
  (non_zero_divisors R) x)))/(v.int_valuation_def s)
```

```
lemma valuation_well_defined {r r' : R} {s s' : non_zero_divisors R}
  (h_mk : is_localization.mk' K r s = is_localization.mk' K r' s') :
  (v.int_valuation_def r)/(v.int_valuation_def s) =
  (v.int_valuation_def r')/(v.int_valuation_def s')
```

We proved several properties of the valuation[3], of which we remark the fact that for every maximal ideal v of R, there exists a uniformizer $\pi_v \in K$ for the v-adic valuation, that is, an element having absolute value $|\pi_v|_v = n_v^{-1}$, or equivalently additive v-adic valuation 1.

```
lemma valuation_exists_uniformizer :
  ∃ (π : K), v.valuation_def π = multiplicative.of_add (-1 : ℤ)
```

We also provide some examples[4] of explicit computations of 2-adic valuations of elements of $\mathbb{Z}$ and $\mathbb{Q}$.

Since $|\cdot|_v$ is an absolute value on the Dedekind domain R and its field of fractions K, we can complete R and K with respect to $|\cdot|_v$. We denote the respective completions by R_v and K_v, and recall that R_v is an integral domain with field of fractions K_v.

We first formalize the definition of K_v using the theory of completions of valued fields available in `mathlib`, which was originally developed as part of the formalization of perfectoid spaces [6]. Among the possible ways to define K_v, this one was chosen because of its powerful API : we can use the `field_completion` instance to recover the fact that K_v is a field, and `valued.extension_valuation` to extend the v-adic valuation on K to a valuation on the completion K_v. We denoted by `adic_completion K v` the completion of K with respect to the v-adic valuation.

[3] https://github.com/mariainesdff/ideles-journal/blob/master/src/valuation.lean
[4] https://github.com/mariainesdff/ideles-journal/blob/master/src/examples.lean

```
def adic_valued : valued K (with_zero (multiplicative ℤ)) := ⟨v.valuation⟩
```

```
def adic_completion := @uniform_space.completion K (us' v)
instance : field (v.adic_completion K) :=
@field_completion K _ (us' v) (tdr' v) _ (ug' v)
instance valued_adic_completion :
  valued (v.adic_completion K) (with_zero (multiplicative ℤ)):=
⟨@valued.extension_valuation K _ _ _ v.adic_valued)⟩
```

It can be shown that R_v is equal to the ring of integers of K_v, that is, the subring of K_v consisting of elements of absolute value less than or equal to one. In our formalization, we actually use this characterization to define R_v (which we called `adic_completion_integers`), so that we automatically have an inclusion of R_v in K_v.

```
def adic_completion_integers : subring (v.adic_completion K) :=
@valuation.integer (v.adic_completion K) (with_zero (multiplicative ℤ)) _ _
  v.valued_adic_completion.v
```

2.2 The finite adèle ring

Now that we have defined nonarchimedean absolute values on a Dedekind domain R and their extension to K, we can attempt to simultaneously study all of them. In order to do so, we define the finite adèle ring $\mathbb{A}_{R,f}$ of R as the restricted product of the completions K_v with respect to their ring of integers R_v, i. e.,

$$\mathbb{A}_{R,f} := \prod_v{}' K_v := \left\{ (x_v)_v \in \prod_v K_v \;\middle|\; x_v \in R_v \text{ for all but finitely many } v \right\},$$

where v runs over the set of maximal ideals of R. Recall that $x_v \in R_v$ is equivalent to $|x_v|_v \leq 1$, so $\mathbb{A}_{R,f}$ is an immediate generalization of $\mathbb{A}_{\mathbb{Q},f}$.

Since $\mathbb{A}_{R,f}$ is a subset of the product $\prod_v K_v$, it is easy to prove that it is a commutative ring with component-wise addition and multiplication (one just needs to check that it is closed under addition, negation and multiplication).

```
def K_hat := (Π (v : maximal_spectrum R), v.adic_completion K )
def finite_adele_ring' := { x : (K_hat R K) //  ∀ᶠ (v : maximal_spectrum R) in
  filter.cofinite, (x v ∈ v.adic_completion_integers K) }
instance : comm_ring (finite_adele_ring' R K) := ...
```

In Lean, the notation `{t :  T // p t}` is used to define the type of pairs `⟨t, p t⟩` where `t` is a term of type `T` that satisties some predicate `p : T → Prop`. Since we use this construction to define `finite_adele_ring'`, given a finite adèle `x :  finite_adele_ring' R K`, we can use `x.val` to get the corresponding term of the product `K_hat R K`, and `x.property` to access a proof that the component `x.val v` belongs to R_v for all but finitely many maximal ideals v. Lean's syntax to indicate that a certain property `p` holds for all but finitely many terms of a type is `∀ᶠ (t :  T) in filter.cofinite, p t`.

We endow $\mathbb{A}_{R,f}$ with the topology generated by the collection of sets $\{\Pi_v U_v \mid U_v \text{ is open and } U_v = R_v \text{ for all but finitely many } v\}$ and prove that addition and multiplication on $\mathbb{A}_{R,f}$ are continuous for this topology, which makes $\mathbb{A}_{R,f}$ into a topological ring. While these proofs are not conceptually hard, their formalization turned out to be quite long. The main reason is that, while on paper we can express that a subset U of $\mathbb{A}_{R,f}$ is equal to a product of subsets V_v of K_v by writing $U = \prod_v V_v$, this cannot be an equality in the formalization

since the two sides of the equation have different types. Instead, we are forced to say that there exists a collection of subsets V_v of K_v such that a finite idèle $x = (x_v)_v$ belongs to U if and only if x_v belongs to V_v for all v, which adds some extra bookkeeping to the proof. A second reason is that, when checking that addition (or multiplication) is continuous at the pair of adèles (x, y), the argument has to be split in several cases depending on whether the v components of x and y are integers, and whether the open sets V_v equal R_v.

```
def finite_adele_ring'.generating_set : set (set (finite_adele_ring' R K)) :=
{ U : set (finite_adele_ring' R K)
  ∃ (V : Π (v : maximal_spectrum R), set (v.adic_completion K)),
    (∀ x : finite_adele_ring' R K, x ∈ U ↔ ∀ v, x.val v ∈ V v) ∧
    (∀ v, is_open (V v)) ∧
    ∀ᶠ v in filter.cofinite, V v = v.adic_completion_integers K }
instance : topological_space (finite_adele_ring' R K) :=
topological_space.generate_from (finite_adele_ring'.generating_set R K)
```

For every element $k \in K$, there are finitely many maximal ideals v of R such that the v-adic absolute value of k is greater than 1; hence $(k)_v$ is a finite adèle of R. The map $\mathrm{inj}_K : K \to \mathbb{A}_{R,f}$ sending k to $(k)_v$ is an injective ring homomorphism, which allows us to regard K as a subring of $\mathbb{A}_{R,f}$. Note that we are using the fact that R has Krull dimension 1 to conclude the injectivity of this map, since if R had Krull dimension 0, then $\mathbb{A}_{R,f}$ would be the trivial ring, and injectivity would fail.

```
def inj_K : K → finite_adele_ring' R K :=
λ x, ⟨(λ v : maximal_spectrum R, (coe : K → (v.adic_completion K)) x),
  inj_K_image R K x⟩
```

One might wonder why we defined $\mathbb{A}_{R,f}$, instead of just working with the full product $\prod_v K_v$. The main reason for this is that, while both $\mathbb{A}_{R,f}$ and $\prod_v K_v$ are topological rings containing K as a subring, only the former is locally compact and contains K as a discrete and co-compact subring. Since $\mathbb{A}_{R,f}$ is in particular a locally compact topological group, it is possible to define a (unique up to scalars) Haar measure on $\mathbb{A}_{R,f}$, which allows us to integrate functions over $\mathbb{A}_{R,f}$. Tate famously used this integration theory in his thesis to study the properties of Hecke L-functions of number fields. Note that Haar measures have recently been formalized in `mathlib` [17].

2.2.1 Alternative definition of the finite adèle ring

There is a second characterization of the ring of finite adèles of R which is also widely used in number theory. We start with the product $\hat{R} := \prod_v R_v$ over all maximal ideals of R and observe that it contains R via the diagonal inclusion $r \mapsto (r)_v$. Hence, we can consider the localization $(\prod_v R_v)[\frac{1}{R\setminus\{0\}}]$ of $\hat{R}$ at $R \setminus \{0\}$, consisting of tuples of the form $(\frac{r_v}{s})_v$ where $r_v \in R_v$ for all v and $s \in R \setminus \{0\} \subseteq R_v \setminus \{0\}$.

To define the topological ring structure on $\hat{R}[\frac{1}{R\setminus\{0\}}]$, we use the fact that for any ring S, ring topologies on S form a complete lattice. In particular, given any map $f : T \to S$ from a topological space T to a ring S, one can define the coinduced ring topology on S to be the finest topology such that S is a topological ring and f is continuous. The complete lattice structure was formalized as part of this project and is already a part of `mathlib`. We give $\hat{R}[\frac{1}{R\setminus\{0\}}]$ the ring topology coinduced by the localization map $(r_v)_v \mapsto (\frac{r_v}{1})_v$ from $\hat{R}$ with the product topology to $\hat{R}[\frac{1}{R\setminus\{0\}}]$.

It is well known that $\mathbb{A}_{R,f}$ is isomorphic to $(\prod_v R_v)[\frac{1}{R\setminus\{0\}}]$ as topological rings. Given an element $(\frac{r_v}{s})_v \in (\prod_v R_v)[\frac{1}{R\setminus\{0\}}]$, the absolute value $|\frac{r_v}{s}|_v$ will be less than or equal to one, except possibly at the finitely many v dividing the denominator s; hence $(\frac{r_v}{s})_v$ is a finite adèle and one easily sees that this map is an isomorphism of rings. Checking that it is also a homeomorphism requires more work.

We formalized this second definition of the adèle ring in `finite_adele_ring`, but we have not yet formalized the proof that the two definitions yield isomorphic topological rings. A strategy to verify that the map described above is a homeomorphism boils down to checking that the localization maps $\hat{R} \to \hat{R}[\frac{1}{R\setminus\{0\}}]$ and $\hat{R} \to \mathbb{A}_{R,f}$ sending $(r_v)_v$ to $(\frac{r_v}{1})_v$ are both continuous and open; however, formalizing this would take some time and, since we do not have immediate plans to use this second definition of the finite adèle ring, we leave it as future work.

The `finite_adele_ring` definition has the advantage that, being defined as a localization, `finite_adele_ring R` automatically inherits a commutative topological ring structure, while for `finite_adele_ring' R` this has to be proven by hand. However, we found that for proving results such as the one described in Section 5.1, our first definition was easier to work with.

```
def finite_adele_ring := localization (diag_R R K)
instance : comm_ring (finite_adele_ring R K) := localization.comm_ring
instance : algebra (R_hat R K) (finite_adele_ring R K) := localization.algebra
instance : is_localization (diag_R R K) (finite_adele_ring R K):=
localization.is_localization
instance : topological_space (finite_adele_ring R K) :=
localization.topological_space
instance : topological_ring (finite_adele_ring R K) :=
localization.topological_ring
```

2.3 The finite idèle group

The finite idèle group $\mathbb{I}_{R,f}$ of R is the unit group of the finite adèle ring $\mathbb{A}_{R,f}$. 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 to (x, x^{-1}). This topology is finer than the subspace topology induced by the inclusion of $\mathbb{I}_{R,f}$ in $\mathbb{A}_{R,f}$, which is not a group topology since inversion fails to be continuous.

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

Note that for every nonzero $k \in K$, the finite adèle $(k)_v$ is invertible, with inverse $(k^{-1})_v$. It follows that $\mathbb{I}_{R,f}$ contains $K^* = K \setminus \{0\}$ as a subgroup. We formalize this fact by defining a function `inj_units_K` from K^* to $\mathbb{I}_{R,f}$ and proving that it is an injective group homomorphism. As in Section 2.2, the injectivity of this map requires the fact that R has Krull dimension 1.

```
def inj_units_K : units K → finite_idele_group' R K :=
λ x, ⟨inj_K R K x.val, inj_K R K x.inv, right_inv R K x, left_inv R K x⟩
```

2.4 Relation to fractional ideals

The finite idèle group of R is closely related to its group of invertible fractional ideals. A fractional ideal of R is an R-submodule I of K for which there exists an $a \in R$ such that aI is an ideal J of R. We say that I is invertible if there exists another fractional ideal I' such that $II' = R$.

For a Dedekind domain R, every nonzero fractional ideal is invertible and can be factored as a product $v_1^{n_1} \cdots v_m^{n_m}$ of maximal ideals of R where the n_i are integers, uniquely up to reordering of the factors. We formalize this definition in `fractional_ideal.factorization`, where we express I as a `finprod` over all maximal ideals of R, as follows.

The `finprod` of a function `f : T → M` from a type `T` to a commutative monoid `M` is defined to be the product of all values `f t` as `t` ranges over `T`, if `f t = 1` for all but finitely many `t`; otherwise `finprod f` is defined to be one. The notation Π^f `t, f t` can be used in place of `finprod f`. Given a fractional ideal I, denote by n_v the exponent of the maximal ideal v in the factorization of I and let $f :$ maximal spectrum$(R) \to$ fractional ideals(R) be the function sending v to v^{n_v}. Since all but finitely many of the n_v are zero, I is equal to `finprod f`. Besides proving this, we provide some API to work with the exponents appearing in the factorization.

```
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) :
  Π^f (v : maximal_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
```

We can define a group homomorphism from $\mathbb{I}_{R,f}$ to the group of invertible fractional ideals by sending $(x_v)_v \in \mathbb{I}_{R,f}$ to the product $\Pi_v v^{\mathrm{val}_v(x_v)}$. Since for every $(x_v)_v \in \mathbb{I}_{R,f}$ there are finitely many maximal ideals v such that $\mathrm{val}_v(x_v)$ is nonzero, this product is actually finite, so it indeed defines a nonzero fractional ideal of R.

```
def finite_idele.to_add_valuations (x : finite_idele_group' R K) :
  Π (v : maximal_spectrum R), ℤ :=
λ v, -(with_zero.to_integer ((valuation.ne_zero_iff valued.v).mpr
  (v_comp.ne_zero R K v x)))
lemma finite_add_support (x : finite_idele_group' R K ) :
  ∀^f (v : maximal_spectrum R) in filter.cofinite,
    finite_idele.to_add_valuations R K x v = 0 := ...
def map_to_fractional_ideals.val :
  (finite_idele_group' R K) → (fractional_ideal (non_zero_divisors R) K) :=
λ x, Π^f (v : maximal_spectrum R), (v.as_ideal : fractional_ideal
  (non_zero_divisors R) K)^(finite_idele.to_add_valuations R K x v)
```

We show that this homomorphism is surjective and its kernel is the set $\mathbb{I}_{R,\infty}$ of elements $(x_v)_v$ in $\mathbb{I}_{R,f}$ having additive valuation zero at all v. Moreover, this map is continuous when the group of invertible fractional ideals is given the discrete topology.

3 Adèles and idèles of number fields

3.1 Number fields and their rings of integers

A number field K is a finite extension of the field $\mathbb{Q}$ of rational numbers [10]. Every finite extension is algebraic, so every element $k \in K$ is the root of a polynomial with coefficients in $\mathbb{Q}$. If moreover k is the root of a monic polynomial with integer coefficients, we say that k is an algebraic integer. The algebraic integers of K form a subring $\mathcal{O}_K$, called the ring of integers of K, which is a Dedekind domain of Krull dimension 1 in which every nonzero ideal is of finite index.

Remember from the introduction that one motivation for defining the adèles of K was to simultaneously study all the (equivalence classes of) nontrivial absolute values on K. These absolute values can be split into two kinds: nonarchimedean and archimedean. The nonarchimedean ones are exactly the v-adic absolute values associated to maximal ideals of the ring of integers $\mathcal{O}_K$, discussed in section 2.1.

To obtain the archimedean absolute values, we first recall that we can find a $\mathbb{Q}$-vector space basis of K of the form $\{1, \alpha, \dots, \alpha^{n-1}\}$, where n is the dimension of K over $\mathbb{Q}$ and α is an element of K. This α is a root of a degree n polynomial f_α with coefficients in $\mathbb{Q}$. For each real root r of f_α, we get an embedding of K into the real numbers $\mathbb{R}$ (the map sending α to r), and restricting the usual absolute value on $\mathbb{R}$ to the image of K, we get an archimedean absolute value on K. Similarly, for every pair of complex conjugate roots (s_1, s_2) of f_α, we get a pair of embeddings of K into the complex numbers $\mathbb{C}$, and we can restrict the complex absolute value to the image of K under one of them to get an absolute value on K. Note that the two embeddings coming from a conjugate pair yield equivalent absolute values.

3.2 The ring of adèles

Let K be a number field. We define the ring of adèles of K as the restricted product of the completions K_v of K with respect to each absolute value $|\cdot|_v$ on it: $\mathbb{A}_K := \prod'_{|\cdot|_v} K_v$. That is, $\mathbb{A}_K$ is the subring of the product $\prod_{|\cdot|_v} K_v$ consisting on tuples $(a_v)_v$ such that $|a_v|_v \leq 1$ for all but finitely many v. Since each nonarchimedean absolute value $|\cdot|_v$ corresponds to a maximal ideal v of O_K, and there are finitely many archimedean absolute values, we can rewrite this definition as

$$\mathbb{A}_K := \prod_{v \text{ max.}}' K_v \times \prod_{|\cdot|_v \text{ arch.}} K_v = \prod_{v \text{ max.}}' K_v \times (\mathbb{R} \otimes_{\mathbb{Q}} K),$$

where we have used a theorem from algebraic number theory to get the second equality. Note that $\prod'_v K_v$ is the finite adèle ring associated to the Dedekind domain $\mathcal{O}_K$; we will denote it by $\mathbb{A}_{K,f}$ and call it the finite adèle ring of K. We formalize these definitions as follows:

```
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 proved in Section 2.2 that `A_K_f` is a topological commutative ring. The product and tensor product of commutative rings are commutative rings, so `A_K` is a commutative ring. To prove that it is a topological commutative ring, it therefore suffices to show that $\mathbb{R} \otimes_{\mathbb{Q}} K$ is a topological ring. We do this by using the fact that there are isomorphisms $\mathbb{R}^n \simeq \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}^n \simeq \mathbb{R} \otimes_{\mathbb{Q}} K$, where n is the dimension of K over $\mathbb{Q}$.

Note that $\mathbb{R}^n$ is represented in Lean by the type `fin n → ℝ` of functions from $\{1,\dots,n\}$ to $\mathbb{R}$, and it is a topological commutative ring when endowed with the product topology `Pi.topological_space`:

```
variables (n : ℕ)
instance : ring (fin n → ℝ) := pi.ring
instance : topological_space (fin n → ℝ) := Pi.topological_space
instance : has_continuous_add (fin n → ℝ) := pi.has_continuous_add'
instance : has_continuous_mul (fin n → ℝ) := pi.has_continuous_mul'
instance : topological_semiring (fin n → ℝ) := topological_semiring.mk
instance : topological_ring (fin n → ℝ) := topological_ring.mk
```

We then define the topology on $\mathbb{R} \otimes_{\mathbb{Q}} K$ as the ring topology coinduced by the map $\mathbb{R}^n \to \mathbb{R} \otimes_{\mathbb{Q}} K$. Finally, `A_K` becomes a topological ring with the product topology.

```
def linear_map.Rn_to_R_tensor_K :
  (fin (finite_dimensional.finrank ℚ K) → ℝ) →ₗ[ℝ] (ℝ ⊗[ℚ] K) :=
linear_map.comp (linear_map.base_change K) (linear_map.Rn_to_R_tensor_Qn _)
def infinite_adeles.ring_topology : ring_topology (ℝ ⊗[ℚ] K) :=
ring_topology.coinduced (linear_map.Rn_to_R_tensor_K K)
instance : topological_space (ℝ ⊗[ℚ] K) :=
(infinite_adeles.ring_topology K).to_topological_space
instance : topological_ring (ℝ ⊗[ℚ] K) :=
(infinite_adeles.ring_topology K).to_topological_ring
instance : topological_space (A_K K) := prod.topological_space
instance : topological_ring (A_K K) := prod.topological_ring
```

We end this section by recalling that $\mathbb{A}_{K,f}$ contains the field K as a subring via the diagonal map sending $k \in K$ to the finite adèle $(k)_v$, which is injective due to the fact that the ring of integers of a number field is not a field[5]. Combining this with the natural inclusion $k \mapsto 1 \otimes k$ of K in $\mathbb{R} \otimes_{\mathbb{Q}} K$, we can also view K as a subring of $\mathbb{A}_K$.

```
def inj_K_f : K → A_K_f K := inj_K (ring_of_integers K) K
def inj_K : K → A_K K :=
λ x, ⟨inj_K_f K x, algebra.tensor_product.include_right x⟩
```

3.3 The group of idèles and the idèle class group

We define the group $\mathbb{I}_K$ of idèles of K as the unit group of the ring of adèles $\mathbb{A}_K$, and the group $\mathbb{I}_{K,f}$ of finite idèles as the unit group of $\mathbb{A}_{K,f}$.

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

For every nonzero $k \in K$, the finite adèle $(k)_v$ is a unit (with inverse $(k^{-1})_v$), and so is the adèle $((k)_v, 1 \otimes k)$. Therefore, we can regard K^* as a subgroup of the (finite) idèle group, which allows us to define the idèle class group C_K of K as the quotient of $\mathbb{I}_K$ by K^*. C_K is a topological group with the quotient topology.

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

The name idèle class group is justified by the close relation between C_K and the ideal class group of K, which we discuss in section 5.1.

[5] `https://mariainesdff.github.io/ideles-journal/adeles_number_field.html#number_field.ring_of_integers.not_field`

4 Adèles and idèles of function fields

Let k be a field, $k[t]$ be the ring of polynomials in one variable over k and $k(t)$ be the field of rational functions (quotients of polynomials) over k. A function field F is a finite field extension of $k(t)$ [16].

```
variables (k F : Type) [field k] [field F] [algebra (polynomial k) F]
  [algebra (ratfunc k) F] [function_field k F]
  [is_scalar_tower (polynomial k) (ratfunc k) F] [is_separable (ratfunc k) F]
```

All of the absolute values that can be defined over $k(t)$ are nonarchimedean: there is one v-adic absolute value for each maximal ideal v of $k[t]$, plus one extra absolute value, called the place at infinity $|\cdot|_\infty$, defined by setting $\left|\frac{f}{g}\right|_\infty = q^{\deg(f)-\deg(g)}$, where $q > 1$ is a fixed real number. The completion of $k(t)$ with respect to this absolute value is the field $k((t^{-1}))$ of formal Laurent series in t^{-1}.

Following the strategy from Section 2.1, we formalize $|\cdot|_\infty$ in Lean under the name `infty_valuation` and we let `kt_infty` denote the completion of $k(t)$ with respect to $|\cdot|_\infty$.

```
def infty_valuation_def (r : ratfunc k) : with_zero (multiplicative ℤ) :=
if (r = 0) then 0 else
  (multiplicative.of_add ((r.num.nat_degree : ℤ) - r.denom.nat_degree))
def kt_infty := @uniform_space.completion (ratfunc k) (usq' k)
```

More generally, all of the absolute values on a function field F over k are nonarchimedean. Most of them correspond to maximal ideals of the integral closure of $k[t]$ in F. The finite adèle ring of F is the restricted product

$$\mathbb{A}_{F,f} := \prod_v{}' F_v := \left\{ (x_v)_v \in \prod_v F_v \;\middle|\; |x_v|_v \leq 1 \text{ for all but finitely many } v \right\},$$

where v runs over these maximal ideals. However, F also contains a finite collection of nonarchimedean absolute values coming from the absolute value $|\cdot|_\infty$ on $k(t)$. In order to include these absolute values as well, we define the adèle ring of F as the product

$$\mathbb{A}_F := \mathbb{A}_{F,f} \times (k((t^{-1})) \otimes_{k(t)} F).$$

```
def A_F_f := finite_adele_ring' (ring_of_integers k F) F
def A_F := (A_F_f k F) × ((kt_infty k) ⊗[ratfunc k] F)
```

The (finite) adèle ring of F is a topological commutative ring. We define the (finite) idèle group of F to be its group of units, respectively denoted $\mathbb{I}_{F,f}$ and $\mathbb{I}_F$, with the topology induced by the map $x \mapsto (x, x^{-1})$ as in Section 2.3.

The idèle class group C_F of F is the quotient of $\mathbb{I}_F$ by F^*. Since, as in the number field case, the ring of integers of F is not a field[6] and hence the diagonal inclusion of F^* in $\mathbb{I}_F$ is injective, C_F is a topological group with the quotient topology.

```
def I_F_f := units (A_F_f k F)
def I_F := units (A_F k F)
def C_F := (I_F k F) / (inj_units_F.group_hom k F).range
```

[6] `https://mariainesdff.github.io/ideles-journal/adeles_function_field.html#function_field.not_is_field`

Note that in number theory one is usually interested in the adèle ring of a function field over a finite field $k = \mathbb{F}_q$. However, $\mathbb{A}_F$ can be defined for any choice of field k, so we do not require k to be finite in our formalization; instead, this finiteness assumption will have to be included in the lemmas that need it.

5 Class Field Theory

Class field theory is a branch of number theory whose goal is to describe the Galois abelian extensions of a local or global field K, as well as their corresponding Galois groups, in terms of the arithmetic of the field K [1, 8, 13]. Recall from the introduction that a global field is either a number field or a function field over a finite field $\mathbb{F}_q$. A local field is the completion of a global field with respect to an absolute value. Examples of local fields include the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the p-adic numbers $\mathbb{Q}_p$, or the field $\mathbb{F}_q((X))$ of formal Laurent series over a finite field.

In this section we discuss two class field theory results involving the definition of the idèle class group. The first one is a proof that the ideal class group of a global field is isomorphic to a quotient of its idèle class group, which we describe explicitly. The second one is a formalization of the statement of the main theorem of global class field theory.

5.1 The ideal class group is a quotient of the idèle class group

We have seen in Section 2.4 that, for any Dedekind domain R, there is a continuous surjective group homomorphism from the finite idèle group $\mathbb{I}_{R,f}$ to the group $\mathrm{Fr}(R)$ of invertible fractional ideals of R, sending $(x_v)_v$ to $\prod_v v^{\mathrm{val}_v(x_v)}$.

If K is a number field with ring of integers R, we can extend this map to a group homomorphism $\mathbb{I}_K \to \mathrm{Fr}(R)$ by pre-composing with the natural projection $\mathbb{I}_K \to \mathbb{I}_{K,f}$, obtaining again a continuous surjection. It is easy to see that an idèle $((x_v)_v, r \otimes_{\mathbb{Q}} k) \in \mathbb{I}_K$ belongs to the kernel of this map, which we denote $\mathbb{I}_{K,\infty}$, if and only if $\mathrm{val}_v(x_v)$ is equal to zero for every maximal ideal v of R. We wrote this map in Lean and formalized proofs of each of the listed properties.

```
-- For a Dedekind domain R with fraction field K :
def map_to_fractional_ideals.val :
  (finite_idele_group' R K) → (fractional_ideal (non_zero_divisors R) K) :=
λ x, Π^f (v : maximal_spectrum R), (v.as_ideal : fractional_ideal
  (non_zero_divisors R) K)^(finite_idele.to_add_valuations R K x v)
```

```
lemma I_K.map_to_fractional_ideals.surjective :
   function.surjective (I_K.map_to_fractional_ideals K) := ...
lemma I_K.map_to_fractional_ideals.continuous :
   continuous (I_K.map_to_fractional_ideals K) := ...
lemma I_K.map_to_fractional_ideals.mem_kernel_iff (x : I_K K) :
   I_K.map_to_fractional_ideals K x = 1 ↔ ∀ v : maximal_spectrum
    (ring_of_integers K), finite_idele.to_add_valuations (ring_of_integers K) K
    (I_K.fst K x) v = 0 := ...
```

Now, we want to show that this map induces a homomorphism at the level of class groups. The ideal class group $\mathrm{Cl}(K)$ of K is defined as the quotient of the group of invertible fractional ideals of K by the subgroup of principal fractional ideals. It is an important object in algebraic number theory, since it can be interpreted as a measure of how far the ring of integers of K is from being a unique factorization domain.

Note that the idèle $((k)_v, 1 \otimes_{\mathbb{Q}} k)$ corresponding to a nonzero $k \in K$ gets mapped to $\prod_v v^{\mathrm{val}_v(k)}$, which is the principal fractional ideal generated by k. Hence, we get an induced map from the idèle class group C_K to the ideal class group $\mathrm{Cl}(K)$. Using the universal property of the quotient topology, we conclude that this map $C_K \to \mathrm{Cl}(K)$ is a continuous surjective homomorphism, with kernel $\mathbb{I}_{K,\infty}K^*/K^*$. Therefore, by the first isomorphism theorem for topological groups, $\mathrm{Cl}(K)$ is isomorphic to the quotient of C_K by $\mathbb{I}_{K,\infty}K^*/K^*$.

The complete formalization of this proof can be found in the file `ideles_number_field`[7]. The theorem also holds in the function field case, with a completely analogous proof available in the file `ideles_function_field`[8]. By providing this proof, we show that our formalization of the adèles and idèles of a global field can be effectively used in practice to prove graduate-level number theoretic results.

5.2 The main theorem of global class field theory

Let K be a number field, $\overline{K}$ an algebraic closure of K and $G_K := \mathrm{Gal}_{\overline{K}/K}$ the Galois group of the extension $\overline{K}/K$. The topological group G_K is isomorphic to the inverse limit $\varprojlim_L \mathrm{Gal}(L/K)$ over all finite extensions L/K, with the inverse limit topology. We consider the topological abelianization $G_K^{ab} := G_K/\overline{[G_K, G_K]}$ of G_K, defined as the quotient of G_K by the topological closure of the commutator subgroup of G_K. The group G_K^{ab} is a topological group with the quotient topology, because $\overline{[G_K, G_K]}$ is a normal subgroup of G_K.

An exercise in infinite Galois theory shows that G_K^{ab} is the Galois group of the maximal abelian extension K^{ab} of K. The main theorem of global class field theory allows us to describe this Galois group in terms of the idèle class group of K :

▶ **Theorem 1** (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 $\pi_0(C_K) \simeq G_K^{ab}$.*

We formalized the statement of this theorem in two parts: we first claimed the existence of a group isomorphism `main_theorem_of_global_CFT.group_isomorphism` between $\pi_0(C_K)$ and G_K^{ab} and then in `main_theorem_of_global_CFT.homeomorph` we stated that this map is also a homeomorphism. Note that a complete pen-and-paper proof of this theorem spans hundreds of pages, so we have not attempted to formalize it.

```
variables (K : Type) [field K] [number_field K]
theorem main_theorem_of_global_CFT.group_isomorphism : (number_field.C_K K) /
    (subgroup.connected_component_of_one (number_field.C_K K)) ≃* (G_K_ab K) :=
sorry
theorem main_theorem_of_global_CFT.homeomorph :
homeomorph ((number_field.C_K K) / (subgroup.connected_component_of_one
    (number_field.C_K K))) (G_K_ab K) :=
{ continuous_to_fun  := sorry,
  continuous_inv_fun := sorry,
  ..(main_theorem_of_global_CFT.group_isomorphism K) }
```

[7] https://github.com/mariainesdff/ideles-journal/blob/master/src/ideles_number_field.lean
[8] https://github.com/mariainesdff/ideles-journal/blob/master/src/ideles_function_field.lean

6 Discussion

6.1 Design choices

Now that we have described all of the number theoretical content of the paper, we can say a few words about the choices we had to make in the formalization process. When a number theorist defines the ring of adèles, they will typically let K be a *global* field and define its ring of adèles as the restricted product $\mathbb{A}_K := \prod_v' K_v$, where v runs over the set of *places* of K, that is, over the equivalence classes of nontrivial absolute values on K.

The first thing that we observe is that, in Lean, we need to treat number fields and function fields separately. Suppose first that K is a number field. The next observation is that we cannot currently construct the type of all places of K, and we need to use different tools to work with the archimedean and nonarchimedean places.

Similarly, while in the function field case all places are nonarchimedean, we do not yet have a convenient way to obtain the set of all places of a function field (this would require an algebraic geometric interpretation not yet formalized); instead, we have to distinguish between the places coming from the ring of integers of the field place, and the places at infinity (those coming from the absolute value $|\cdot|_\infty$ on $k(t)$).

However, these descriptions show that, regardless of whether K is a number field or a function field, its finite adèle ring can be described as the restricted product $\mathbb{A}_{K,f} := \prod_v' K_v$, where v runs over the maximal ideals of the ring of integers of K. In both cases, this ring of integers is a Dedekind domain. Moreover, the definition $\mathbb{A}_{R,f} := \prod_v' \mathrm{Frac}(R)_v$ makes sense for any Dedekind domain R with field of fractions $\mathrm{Frac}(R)$, regardless of whether $\mathrm{Frac}(R)$ is a global field.

We therefore chose to define `finite_adele_ring'` for any Dedekind domain R. This allowed us to unify the number and function field cases in a big part of the theory, and to show that some properties of $\mathbb{A}_{R,f}$ hold in greater generality than the one typically considered in informal mathematics.

6.2 Implementation comments

In this section we discuss some technical details of our formalization. The first one has to do with the universe in which the Dedekind domain R and its function field K are defined. Lean is based on a version of dependent type theory with a countable hierarchy of non-cumulative universes: `Type` (short for `Type 0`) is the universe of small or ordinary types, `Type 1` is a larger universe of types which contains `Type` as an element, and, in general, for any natural number $n > 0$, there is a `Type n` which contains `Type n - 1` as an element. There is an extra type, called `Prop`, which has some special properties. We can declare universe variables explicitly, or use `Type*` to avoid naming the arbitrary universe.

```
universe u
variables {T : Type u} {S : Type*}
```

Dedekind domains and their fields of fractions can be defined over any universe, as we did at the beginning of Section 2.1.

```
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]
```

However, the ring $\mathbb{Z}$ has type `Type`, and hence so does `with_zero (multiplicative ℤ)`. When we started to formalize adic valuations on Dedekind domains, `mathlib`'s definition of the class `valued` required the ring `R` and the `linear_ordered_comm_group_with_zero` Γ_0 to live in the same universe:

```
universe u
class valued (R : Type u) [ring R] :=
(Γ₀ : Type u)
[grp : linear_ordered_comm_group_with_zero Γ₀]
(v : valuation R Γ₀)
```

This forced us to require our Dedekind domain R and its field of fractions K to live in `Type`. However, we observed that the definition of `valued` could be generalized to allow Γ_0 to have a different type than the ring `R`, without any negative consequences to the library. After this observation and some input from the `mathlib` community, in March 2022 the definition of `valued` was changed to the following:

```
class valued (R : Type u) [ring R] (Γ₀ : out_param (Type v))
  [linear_ordered_comm_group_with_zero Γ₀] :=
(v : valuation R Γ₀)
```

which in particular allows `R` and Γ_0 to live in different universes. With this design, we can use the variable declaration below to indicate that the ring `R` has a canonical valuation with values on Γ_0. The `out_param` in the definition of the class `valued` has the effect that, when proving lemmas about the valued structure on `R`, Lean will pick Γ_0 based on the valued instance it found.

```
universes u v
variables {R : Type u} [ring R] {Γ₀ : Type v }
  [linear_ordered_comm_group_with_zero Γ₀] [valued R Γ₀]
```

Secondly, we ran into a computability issue in Lean 3. A function is computable if there is an algorithm that can produce the output corresponding to every possible input. Every computable definition in Lean 3 is compiled to bytecode at definition time. However, functions that rely on the axiom of choice and therefore do not admit a computational interpretation are also allowed in Lean. These functions have to be declared using the `noncomputable` modifier.

When a definition is stated in Lean 3, a computability check is deployed, even if the definition has been marked as `noncomputable`. If a computable definition has been labeled as `noncomputable`, or a noncomputable definition is missing the label, an error will be raised.

We found that in some definitions, the computability check was causing unexpected timeouts. We would like to thank Gabriel Ebner for finding the cause of these errors and providing a first solution to it, the `force_noncomputable` definition, with a corresponding `simp` lemma.

```
noncomputable def force_noncomputable {α : Sort*} (a : α) : α :=
function.const _ a (classical.choice ⟨a⟩)
@[simp] lemma force_noncomputable_def {α} (a : α) : force_noncomputable a = a :=
rfl
```

The trick is that, given a value `a`, `force_noncomputable` uses the axiom of choice to return an element of the singleton `{a}`. That is, it returns the original value; however, since the axiom of choice is explicitly invoked, the definition is noncomputable. When `force_noncomputable`

is pre-composed with any definition in Lean, the new definition is noncomputable (regardless of whether the original definition was), and the computability check is able to identify this without timing out.

In March 2022, the Lean mantainers added a new `noncomputable!` modifier. Definitions with this label do not have their computability checked, get marked as noncomputable when added to the environment, and do not get compiled at definition time. Hence this modifier can be used to solve the issue we found above (in which the computability check was timing out), and it also helps in the case where a definition is correctly identified as computable but the compiler times out when producing the corresponding bytecode.

As an example, the definition of the coercion map from $\mathbb{A}_{R,f}$ to $\prod_v K_v$ was causing an "deterministic timeout" error, which was solved by using the `noncomputable!` modifier.

```
noncomputable! def coe' : (finite_adele_ring' R K) → K_hat R K := λ x, x.val
```

6.3 Future work

There are several natural directions for future formalization work stemming from this project. We list some of them, starting with the most immediate goals.

- Show that the two definitions of the finite adèle ring formalized in Section 2.2 give isomorphic topological rings. Constructing an isomorphism of rings between them will be easy, but checking that it is a homeomorphism will require some work.
- Formalize topological results about the adèle ring and the idèle group, such as the proof that $\mathbb{A}_K$ is locally compact and contains K as a discrete co-compact subring.
- Given a finite extension L/K of global fields, formalize the isomorphism $\mathbb{A}_L \simeq L \otimes \mathbb{A}_K$ and its consequences.
- Keep stating, and eventually proving, results from class field theory.
- Formalize Tate's thesis.

More generally, having the definitions of $\mathbb{A}_K$ and $\mathbb{I}_K$ opens the door to formalizing concepts and results used in state-of-the-art number theory, including the definition of automorphic forms [5] and the statement of the Langlands correspondence [11]. Note that only some cases of the Langlands correspondence have been proven, and the Langlands program is currently one of the main research areas in number theory.

References

1 Emil Artin and John Tate. *Class Field Theory*. W. A. Benjamin, New York, 1967.

2 Emil Artin and George Whaples. Axiomatic Characterization of Fields by the Product Formula for Valuations. *Bulletin of the American Mathematical Society*, 51(7):469–492, 1945. URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=MR0013145`.

3 Jeremy Avigad, Leonardo de Moura, and Soonho Kong. *Theorem Proving in Lean*. Carnegie Mellon University, 2021. Release 3.23.0. URL: `https://leanprover.github.io/theorem_proving_in_lean/`.

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

5 Daniel Bump. *Automorphic Forms and Representations*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1997. `doi:10.1017/CBO9780511609572`.

6 Kevin Buzzard, Johan Commelin, and Patrick Massot. Formalising Perfectoid Spaces. In Jasmin Blanchette and Catalin Hritcu, editors, *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, USA, January 20-21, 2020*, pages 299–312. ACM, 2020. doi:10.1145/3372885.3373830.

7 Mario Carneiro. *The Type Theory of Lean*. Springer, Berlin, Heidelberg, 2019. Master thesis. URL: https://github.com/digama0/lean-type-theory/releases.

8 J. W. S. Cassels and A. Fröhlich (eds.). *Algebraic Number Theory*. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

9 L. de Moura, S. Kong, J. Avigad, F. van Doorn, and J. von Raumer. The Lean Theorem Prover (System Description). In Felty A. and Middeldorp A., editors, *Automated Deduction - CADE-25*, volume 9195 of *Lecture Notes in Computer Science*, pages 378–388. Springer, Cham, 2015. doi:10.1007/978-3-319-21401-6_26.

10 Gerald J. Janusz. *Algebraic Number Fields*, volume 55 of *Pure and Applied Mathematics*. Academic Press, London, 2nd edition, 1996.

11 R. P. Langlands. Problems in the Theory of Automorphic Forms. In *Lectures in Modern Analysis and Applications III*, volume 170 of *Lecture Notes in Mathematics*, pages 18–61. Springer, Berlin, Heidelberg, 1970. doi:10.1007/BFb0079065.

12 Robert Y. Lewis. A Formal Proof of Hensel's Lemma over the p-Adic Integers. In *Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2019, pages 15–26, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3293880.3294089.

13 J. S. Milne. Class Field Theory (v4.03), 2020. URL: https://www.jmilne.org/math/CourseNotes/CFT.pdf.

14 Jürgen Neukirch. *Algebraic Number Theory*. Springer, Berlin, Heidelberg, 1999. doi:10.1007/978-3-662-03983-0.

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

16 Henning Stichtenoth. *Algebraic Function Fields and Codes*. Universitext. Springer, 1993. URL: https://dblp.org/rec/books/daglib/0084861.

17 Floris van Doorn. Formalized Haar Measure. In Liron Cohen and Cezary Kaliszyk, editors, *12th International Conference on Interactive Theorem Proving (ITP 2021)*, volume 193 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 18:1–18:17, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITP.2021.18.