Formalizing the Ring of Adèles of a Global Field

María Inés de Frutos-Fernández ⊠☆®

Imperial College London, United Kingdom

- 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 formalized 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 \rightarrow Logic and verification; Theory of computation \rightarrow Type theory

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

Funding EPSRC Grant $\mathrm{EP/V048724/1}$: 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 could 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.

2 Formalizing the Ring of Adèles of a Global Field

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 repository¹ containing the version of the code referred to in this article and the associated documentation² in HTML format. Note that 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:

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

 $\mathbb{A}_{\mathbb{Q}}$ 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.

1.1 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].

 $^{^1 \ \, {\}tt https://github.com/mariainesdff/ideles/tree/journal-submission}$

https://mariainesdff.github.io/ideles/journal-submission/

This project is based on Lean's mathematical library mathlib, which is characterized by its decentralized nature with over 300 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 with some implementation remarks and a discussion of future work connected to this project.

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 $\mathtt{mathlib}$ [4]. We work with the one formalized in $\mathtt{is_dedekind_domain}$: 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
def maximal_spectrum := {v : prime_spectrum R // v.val ≠ 0 }
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 v value v is v and v is v and v is v and v is v and v in v and v is v and v in v and v is v and v in v and v in v and v is v and v in v and v is v and v in v in v and v in v in v and v in v

- 1. $\operatorname{val}_v(r) = \infty$ if and only if r = 0,
- 2. $\operatorname{val}_v(rs) = \operatorname{val}_v(r) + \operatorname{val}_v(s)$ for all r, s in R, and
- 3. $\operatorname{val}_v(r+s) \ge \min{\{\operatorname{val}_v(r), \operatorname{val}_v(s)\}}$ 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 $\operatorname{val}_v(r/s) := \operatorname{val}_v(r) - \operatorname{val}_v(s)$. 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 $n_v^{-\operatorname{val}_v(r)}$. 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) $|r + s|_v \le \max\{|r|_v, |s|_v\}$ 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 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 \mathbb{Z}), which is a way to represent $n_v^{\mathbb{Z}} \cup \{0\}$ in Lean. We used associates.mk instead of working directly with ideals simply because the corresponding factorization API was more convenient.

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.

```
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, 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 : \exists \ (\pi : \texttt{K}), \ v.valuation\_def \ \pi = \texttt{multiplicative.of\_add} \ (-1 : \ \mathbb{Z})
```

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 .

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 , so that we automatically have an inclusion of R_v in K_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.,

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

where v runs over the set of maximal ideals of R. Recall that $x_v \in R_v$ is equivalent to $|x_v|_v \le 1$, 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 := (\Pi (v : maximal_spectrum R), (K_v K v))
def finite_adele_ring' := { x : (K_hat R K) // \forall^f (v : maximal_spectrum R) in
    filter.cofinite, (x v \in R_v K v) }
instance : comm_ring (finite_adele_ring' R K) := ...
```

We endow $\mathbb{A}_{R,f}$ with the topology generated by the set $\{\Pi_v U_v \mid U_v \text{ is open and } U_v = R_v \text{ for almost all } v\}$ 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.

```
def finite_adele_ring'.generating_set : set (set (finite_adele_ring' R K)) :=
{U : set (finite_adele_ring' R K) |
    ∃ (V : ∏ (v : maximal_spectrum R), set (K_v K v)),
    (∀ x : finite_adele_ring' R K, x ∈ U ↔ ∀ v, x.val v ∈ V v) ∧
    (∀ v, is_open (V v)) ∧ ∀<sup>f</sup> v in filter.cofinite, V v = R_v K v}
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 $\operatorname{inj}_K : K \to \mathbb{A}_{R,f}$ sending k to $(k)_v$ is an injective ring homomorphism, which allows us to regard K as a subring of $\mathbb{A}_{R,f}$.

```
def inj_K : K \rightarrow finite_adele_ring' R K := \lambda x, \langle(\lambda v : maximal_spectrum R, (coe : K \rightarrow (K_v K v)) x), inj_K_image R K x\rangle
```

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 omit for now the formalization of the proof that the two definitions yield isomorphic topological rings. 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_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}) .

```
def finite_idele_group' := units (finite_adele_ring' R K)
instance : topological_space (finite_idele_group' R K) := units.topological_space
instance : group (finite_idele_group' R K) := units.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 $\mathtt{inj_units_K}$ from K^* to $\mathbb{I}_{R,f}$ and proving that it is an injective group homomorphism.

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 formalized this definition in fractional_ideal.factorization, where we express I as a finprod over all maximal ideals of R. We also provide some API to work with the exponents appearing in this factorization.

```
lemma fractional_ideal.factorization (I : fractional_ideal (non_zero_divisors R) K) (hI : I \neq 0) {a : R} {J : ideal R} (haJ : I = fractional_ideal.span_singleton (non_zero_divisors R) ((algebra_map R K) a)^-1 * \uparrowJ) :  \Pi^f \text{ (v : maximal_spectrum R),}  (v.val.val : fractional_ideal (non_zero_divisors R) K)^ ((associates.mk v.val.val).count (associates.mk J).factors - (associates.mk v.val.val).count (associates.mk (ideal.span{a})).factors : \mathbb{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 $\Pi_v v^{\text{val}_v(x_v)}$. Since for every $(x_v)_v \in \mathbb{I}_{R,f}$ there are finitely many maximal ideals v such that $\text{val}_v(x_v)$ is nonzero, this product is actually finite, so it indeed defines a nonzero fractional ideal of R.

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) \times (\mathbb{R} \otimes [\mathbb{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 $fin \ n \to \mathbb{R}$ of functions from $\{1, \ldots, n\}$ to \mathbb{R} , and we can use pi to get its topological commutative ring structure as follows:

```
variables (n : \mathbb{N}) instance : ring (\text{fin } n \to \mathbb{R}) := \text{pi.ring} instance : topological_space (\text{fin } n \to \mathbb{R}) := \text{Pi.topological_space} instance : has_continuous_add (\text{fin } n \to \mathbb{R}) := \text{pi.has_continuous_add'} instance : has_continuous_mul (\text{fin } n \to \mathbb{R}) := \text{pi.has_continuous_mul'} instance : topological_ring (\text{fin } n \to \mathbb{R}) := \text{topological_ring.mk}
```

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

```
\begin{array}{lll} \operatorname{def\ linear\_map.Rn\_to\_R\_tensor\_K} : & (\operatorname{fin\ (finite\_dimensional.finrank\ }\mathbb{Q}\ K) \to \mathbb{R}) \to_1 \\ & \mathbb{R} \ (\mathbb{R}\ \otimes \mathbb{Q} \ K) := \\ & \operatorname{linear\_map.comp\ (linear\_map.base\_change\ K)\ (linear\_map.Rn\_to\_R\_tensor\_Qn\ K)} \\ \operatorname{def\ infinite\_adeles.ring\_topology} : & \operatorname{ring\_topology} \ (\mathbb{R}\ \otimes \mathbb{Q} \ K) := \\ & \operatorname{ring\_topology.coinduced\ (linear\_map.Rn\_to\_R\_tensor\_K\ K)} \\ \operatorname{instance} : & \operatorname{topological\_space\ } (\mathbb{R}\ \otimes \mathbb{Q} \ K) := \\ \end{array}
```

```
(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 $(k)_v$. 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 \rightarrow A_K_f K := inj_K (ring_of_integers K) K def inj_K : K \rightarrow A_K K := \lambda x, \langleinj_K_f K x, algebra.tensor_product.include_right x\rangle
```

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^* :

```
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.

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 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 $|\cdot|_{\infty}$.

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

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

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.

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 number 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 $\operatorname{Fr}(R)$ of invertible fractional ideals of R, sending $(x_v)_v$ to $\prod_v v^{\operatorname{val}_v(x_v)}$.

If K is a number field with ring of integers R, we can extend this map to a group homomorphism $\mathbb{I}_K \to \operatorname{Fr}(R)$ 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 $\operatorname{val}_v(x_v)$ 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.

```
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 \leftrightarrow V 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 $\operatorname{Cl}(K)$ 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 $\prod_v v^{\operatorname{val}_v(k)}$, 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 $\operatorname{Cl}(K)$. Using the universal property of the quotient topology, we conclude that this map $C_K \to \operatorname{Cl}(K)$ is a continuous surjective homomorphism, with kernel $\mathbb{I}_{K,\infty}K^*/K^*$. Hence, by the first isomorphism theorem for topological groups, $\operatorname{Cl}(K)$ is isomorphic to the quotient of C_K by $\mathbb{I}_{K,\infty}K^*/K^*$.

By proving this theorem, 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. While we have only formalized this proof for number fields, it can be trivially adapted to the function field case.

5.2 The main theorem of global class field theory

Let K be a number field, \overline{K} an algebraic closure of K and $G_K := \operatorname{Gal}_{\overline{K}/K}$ the Galois group of the extension \overline{K}/K . The topological group G_K is isomorphic to the inverse limit $\varprojlim_L \operatorname{Gal}(L/K)$ 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.

6 Discussion

6.1 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. To define the v-adic valuations and formalize the factorization of fractional ideals, we can let R and K be of Type u for any universe u. However, to define the completions K_v and all subsequent work, we require R and K to live in Type. This is because the structure valued, which we used in our definitions of the completions, requires the field K and the linear_ordered_comm_monoid_with_zero Γ_0 to live in the same universe, and we chose Γ_0 to be with_zero(multiplicative \mathbb{Z}), which has type Type.

Secondly, we found that some definitions were unexpectedly causing timeouts or memory errors, due to the fact that Lean was not able to decide whether they were computable or not. We would like to thank Gabriel Ebner for finding the cause of these errors and providing the force_noncomputable definition to address it, as well as an associated simp lemma.

```
noncomputable def force_noncomputable \{\alpha: Sort*\} (a : \alpha) : \alpha:= function.const _ a (classical.choice \langle a \rangle) @[simp] lemma force_noncomputable_def \{\alpha\} (a : \alpha) : force_noncomputable a = a := rfl
```

As an example, the definition of the coercion map from $\mathbb{A}_{R,f}$ to $\prod_v K_v$ was causing an 'excessive memory consumption' error, which was immediately solved with the application of force_noncomputable.

```
def coe': (finite_adele_ring' R K) \to K_hat R K := force_noncomputable \$ \lambda x.val
```

6.2 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.
- Define the idèle class group and prove the results from Section 5.1 in the function field setting. The proofs will be nearly identical to the number field case.

- 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 subgroup.
- 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. URL: https://drops.dagstuhl.de/opus/volltexte/2021/13900, 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/CB09780511609572.
- 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.
- 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, page 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.
- 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.
- Henning Stichtenoth. *Algebraic Function Fields and Codes.* Universitext. Springer, 1993. URL: https://dblp.org/rec/books/daglib/0084861.bib.
- 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. URL: https://drops.dagstuhl.de/opus/volltexte/2021/13913, doi:10.4230/LIPIcs.ITP.2021.18.