Local-global principle in class field theory

Antoine Labelle

March 2022

1 Introduction

In these notes, based on the book *Class field theory* by J. S. Milne., we give an overview of the main theorems of class field theory, which an emphasis on the interplay between the local and global cases. We start by defining places of global fields and how local fields arise from those in section 2. In section 3, we define the norm map of a Galois extension, the key definition needed in order to state the main theorems of local class field theory in section 4. We then go back to global fields and define the idèle class group in section 5. Finally, in section 6, we state the main theorems in the global case using this idèle class group.

2 Global and local fields

Definition 2.1. *An* absolute value *on a field K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying :*

1. $|x| = 0$ *if and only if* $x = 0$.
2. $|xy| = |x||y|$. *(multiplicativity)*
3. $|x + y| \leq |x| + |y|$. *(triangle inequality)*

We say that two absolute values $|\cdot|_1, |\cdot|_2$ are equivalent if $|x|_1 = |x|_2^c$ for some constant $c > 0$. The trivial absolute value is the absolute value $|x| = 1$ for every $x \in K^\times$.

Let K be a number field, i.e. a finite field extension of $\mathbb{Q}$. A *place* of K is an equivalence class of nontrivial absolute values. For example, the places of $\mathbb{Q}$ are classified by the following theorem of Ostrowski:

Theorem 2.2. *All places of $\mathbb{Q}$ are of one of the following forms:*

- *For each prime number p, there is a place of $\mathbb{Q}$ corresponding to the absolute value $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is the exponent of p in the prime factorization of x.*
- *The infinite place, corresponding to the absolute value $|\cdot|_\infty$ defined by the usual absolute value on $\mathbb{R}$.*

More generally, if K is a number field, there is one place for each prime ideal of the ring of algebraic integers $\mathcal{O}_K$ of K and one place for each of the $n = [K : \mathbb{Q}]$ embeddings of K inside $\mathbb{C}$ (and all places of K fall in one of these two cases). We call places of the former kind finite *places, while those of the latter kind are called* infinite.

Given a place v of K, we can form the completion K_v of K with respect to the corresponding absolute value by quotienting the ring of Cauchy sequences by null sequences. For example, in the case $K = \mathbb{Q}$

and $v = v_\infty$, this is the usual construction of $\mathbb{R}$ with Cauchy sequences. In the case of the finite place corresponding to a prime p, we obtain the p-adic numbers $\mathbb{Q}_p$.

A common theme in number theory is to study a number field K by studying "locally" what happens in each completion K_v. For this reason, number fields are often call *global fields*, while their completions K_v are called *local fields*. A concrete example of this *local-global* principle is the Hasse-Minkowski theorem, which says that the quadratic equation

$$a_1X_1^2 + a_2X_2^2 + \ldots + a_nX_n^2 = 0$$

has a solution over $\mathbb{Q}$ if and only if it has a solution over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every p.

3 Norm groups

3.1 Motivating example

Consider the quadratic equation

$$X^2 - aY^2 - bZ^2 = 0$$

for $a, b \in K^\times$. We'd like to understand when this equation has a nontrivial solution $(X, YZ) \neq (0,0,0)$. Assume that a is not a perfect square in K, so that there is no nontrivial solution with $Z = 0$. By making the substitution $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, we see that this can be rewritten as

$$x^2 - ay^2 = b.$$

Note that the left hand side of this expression can be factored as a difference of squares if we pass to the extension

$$L = K[\sqrt{a}] = \{x + y\sqrt{a} : x, y \in K\}.$$

More precisely, if we define a norm map $\mathrm{Nm} : L^\times \to K^\times$ by

$$\mathrm{Nm}(x + y\sqrt{a}) = (x + y\sqrt{a})(x - y\sqrt{a}) = x^2 - ay^2$$

then the equation just becomes

$$\mathrm{Nm}(x + y\sqrt{a}) = b$$

so understanding when the equation has a solution is equivalent to understanding what is the image of the norm homomorphism from $L^\times$ to $K^\times$.

One consequence of class field theory is that, when K is a local field (for example $\mathbb{Q}_p$), the image $\mathrm{Nm}(L^\times)$ is an index 2 subgroup of $K^\times$. In particular, if we define

$$(a, b) = \begin{cases} 1 & \text{if } X^2 - aY^2 - bZ^2 = 0 \text{ has a nontrivial solution in K} \\ -1 & \text{otherwise} \end{cases}$$

this implies that $(\cdot,\cdot) : K^\times \times K^\times \to \{\pm 1\}$ is bimultiplicative (i.e. $(a, bb') = (a, b)(a, b')$ and $(aa', b) = (a, b)(a', b)$), since the product of two non-norms from $L^\times$ is a norm. The map $(\cdot,\cdot)$ is called the Hilbert symbol and is a very important tool in the theory of quadratic forms.

3.2 The norm map for general extensions

More generally whenever we have a finite Galois extension L/K, we can define a norm map $\mathrm{Nm} : L^\times \to K^\times$ by

$$\mathrm{Nm}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha$$

for every $\alpha \in L^\times$. It is clear that the product on the right hand side is fixed by every element of $\mathrm{Gal}(L/K)$, so $\mathrm{Nm}(\alpha)$ is really an element of K. It is also clear from this definition that Nm is an homomorphism from the multiplicative group of L to the multiplicative group of K. Its image $\mathrm{Nm}(L^\times)$

Note that our definition of Nm from the previous section is a special case of this construction, since $\mathrm{Gal}(K[\sqrt{a}]/K)$ is a group with two elements : the identity and the field automorphism sending $x + y\sqrt{a}$ to $x - y\sqrt{a}$.

4 Local class field theory

One of the big problems in algebraic number theory is to classify all finite extensions of a given global or local field. In general, this is an extremely difficult problem. Class field theory, however, gives a very satisfying answer to this problem, for the special case of abelian extensions (that is, Galois extensions L of K for which the group $\mathrm{Gal}(L/K)$ is abelian). In the local case this answer is particularly simple. It turns out that, when K is a local field, the map

$$\begin{aligned} \{\text{finite abelian extensions of } K\} &\longrightarrow \left\{\text{finite index open subgroups of } K^\times\right\} \\ L &\longmapsto \mathrm{Nm}(L^\times) \end{aligned} \tag{$*$}$$

sending an abelian extension to its norm group gives a bijection from the set of abelian extensions of K to the set of finite index open subgroups of $K^\times$. Moreover, given a finite index open subgroup $H \subset K^\times$, the Galois group of the corresponding extension L can be recovered as $\mathrm{Gal}(L/K) \cong K^\times/H$.

All these isomorphisms between abelian Galois groups over K and finite quotients of $K^\times$ can be bundled together in a single map, called the Artin map. We define K^{ab} to be the union of all abelian extensions of K (in a fixed algebraic closure). This is an infinite extension of K (except in the case $K = \mathbb{R}$ or $\mathbb{C}$), but there still exists a version of Galois theory for infinite extensions, provided that we put the right topology on the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Theorem 4.1 (Artin reciprocity)**.** *Let K be a local field. There exists an homomorphism*

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

satisfying the following property:

For any finite abelian extension L of K, the kernel of the composite

$$K^\times \xrightarrow{\phi_K} Gal(K^{ab}/K) \xrightarrow{restriction} Gal(L/K)$$

is exactly the norm group $Nm(L^\times)$, and ϕ_K induces an ismorphism

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

One consequence of Theorem 4.1 is that two different abelian extensions of K have different norm groups, i.e. $(*)$ is injective. On the other, it does not imply that $(*)$ is surjective (in fact, Theorem 4.1 could hold even if there was no abelian extension of K at all). For this, we need the second main theorem of local class field theory, which tells us that there are "enough" abelian extensions of K.

Theorem 4.2 (Existence theorem). *For every open subgroup of finite index $H \subset K^\times$, there exists an abelian extension L of K such that $H = Nm(L^\times)$.*

The proofs of these two theorems are very involved and make heavy use of the theory of group cohomology.

5 Idèles

In order to do class field theory for global fields, we need to introduce an important object that is gonna play the role played by the multiplicative group $K^\times$ in the local case : the idèle class group. In particular, global class field theory will tell us that there is a correspondence between abelian extensions of a global field K and finite index open subgroups of its idèle class group.

Definition 5.1. *Let K be a global field. The* group of idèles $\mathbb{I}_K$ *of K is defined as*

$$\mathbb{I}_K = \left\{ (a_v) \in \prod_v K_v^\times \;\middle|\; |a_v|_v = 1 \textit{ for all but finitely many } v \right\}$$

where the product is over all places of K. It is a topological group under the topology induced by the product topology on $\prod_v K_v^\times$.

The group of idèles is a convenient way to package the information about the local fields at all the places of K in a single group. We add the condition that $|a_v|_v = 1$ for almost all v instead of working directly with the product $\prod K_v^\times$ because this direct product is "too big" in some sense while $\mathbb{I}_K$ is much more well-behaved. A concrete example of that is that $\prod K_v^\times$ is not locally compact, but $\mathbb{I}_K$ is, which is crucial in particular to develop harmonic analysis on the idèles.

There is a diagonal embedding $K^\times \hookrightarrow \mathbb{I}_K$ given by $x \mapsto (\ldots, x, x, x, \ldots)$ (where each x is seen as an element of a different completion K_v). This makes $K^\times$ a discrete subgroup of $\mathbb{I}_K$.

Definition 5.2. *The idèle class group of K, denoted $\mathbf{C}_K$, is defined as the quotient $\mathbb{I}_K/K^\times$.*

This turns out to be the crucial object for global class field theory, as we will see in the next section.

Example 5.3. *Consider the case $K = \mathbb{Q}$. Then the idèles correspond to the elements*

$$(a_\infty, a_2, a_3, a_5, \ldots) \in \mathbb{R}^\times \times \prod_{p \textit{ prime}} \mathbb{Q}_p^\times$$

such that $a_p \in \mathbb{Z}_p^\times$ for all but finitely many p. For all p such that a_p is not a unit of $\mathbb{Z}_p$, we can factor out $p^{v_p(a_p)}$ to make it a unit and, if $a_\infty < 0$, we can factor out -1 to make it positive. Using unique factorization of rationals into products of prime powers and ± 1, we see that each idèle can be written uniquely as

$$a \cdot (b_\infty, b_2, b_3, b_5, \ldots)$$

with $a \in \mathbb{Q}^\times$, $b_\infty \in \mathbb{R}_{>0}$ and $b_p \in \mathbb{Z}_p^\times$. Hence

$$\mathbb{I}_\mathbb{Q} = \mathbb{Q}^\times \times \mathbb{R}_{>0} \times \prod_{p \textit{ prime}} \mathbb{Z}_p^\times$$

and

$$\mathbf{C}_\mathbb{Q} = \mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times = \mathbb{R}_{>0} \times \prod_{p \textit{ prime}} \mathbb{Z}_p^\times.$$

If we let $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ be the ring of profinite integers, then we can rewrite this even more compactly as

$$\mathbf{C}_\mathbb{Q} = \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times.$$

6 Global class field theory

Following the local-global philosophy, we expect that it should be possible to use the classification of abelian extensions of local fields to obtain analogous results for global fields. Indeed, this is done by global class field theory.

In order to formulate it we need to extend the norm map to the idèle class group. Let L/K be an extension of global fields. For every place v of K and place w of L extending v, we have an extension L_w/K_v, with it's usual norm map $\mathrm{Nm} : L_w^\times \to K_v^\times$. Since there are finitely many places w of L extending any place v of K and $|x|_w = 1 \Rightarrow |\mathrm{Nm}(x)|_v = 1$ for every $x \in L_w$, we can combine the norm maps at each place together to get a norm map $\mathbb{I}_L \to \mathbb{I}_K$ defined by $(a_w)_w \mapsto (b_v)_v$ where

$$b_v = \prod_{w \text{ extending } v} \mathrm{Nm}(a_w).$$

Moreover, one can show that the restriction of this map to $L^\times \subset \mathbb{I}_L$ (using the diagonal embedding defined in the previous section) agree with the usual norm map $L^\times \to K^\times$. In particular, we get an induced map

$$\mathrm{Nm} : \mathbf{C}_L \to \mathbf{C}_K.$$

With this norm map defined, we can state the main theorems of global class field theory. Notice how they perfectly mirror the local versions.

Theorem 6.1 (Artin reciprocity)**.** *Let K be a global field. There exists an homomorphism*

$$\phi_K : \mathbf{C}_K \to \mathit{Gal}(K^{ab}/K)$$

satisfying the following property:

For any finite abelian extension L of K, the kernel of the composite

$$\mathbf{C}_K \xrightarrow{\phi_K} \mathit{Gal}(K^{ab}/K) \xrightarrow{\textit{restriction}} \mathit{Gal}(L/K)$$

is exactly the norm group $Nm(\mathbf{C}_L)$, and ϕ_K induces an isomorphism

$$\phi_{L/K} : \mathbf{C}_K/Nm(\mathbf{C}_L) \to \mathit{Gal}(L/K).$$

Theorem 6.2 (Existence theorem)**.** *For every open subgroup of finite index $H \subset \mathbf{C}_K$, there exists an abelian extension L of K such that $H = Nm(\mathbf{C}_L)$.*

Note that, even though the mere definition of the local Artin map requires some deep theory, the global Artin map is relatively easy to describe once we have the local one. It is defined, for $\mathbf{a} = (a_v)_v \in \mathbb{I}_K$, by

$$\phi_K(\mathbf{a}) = \prod_v \phi_{K_v}(a_v),$$

where we implicitely see $\phi_{K_v}(a_v)$ as an element of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ using the embedding $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \hookrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

There are a few comments to make about this definition. First, it is crucial here that we restrict to abelian extensions since in general the inclusion $\mathrm{Gal}(L_w/K_v) \hookrightarrow \mathrm{Gal}(L/K)$ depends on the choice of w. Thus, for fixed v, it is only well-defined up to conjugation, which doesn't matter in the abelian case. The abelian restriction is also necessary for the product $\prod_v \phi_{K_v}(a_v)$ to be independent on the ordering of the terms. Let's also mention that, even though this product might have infinitely many terms, all but finitely many of them become the identity in $\mathrm{Gal}(L/K)$ for every *finite* abelian extension L/K (this is nontrivial but follows from properties of the local Artin map). Hence the product converges in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

These comments explain why we have a well defined Artin map $\mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. The main difficulty in the proof of the global Artin reciprocity theorem is to show that it factors through $\mathbf{C}_K$ and that it induces isomorphisms $\phi_{L/K}$ for every L.

Just as in the local case, we can see that Theorem 6.1 and Theorem 6.2 together give a classification of abelian extensions of K:

$$\begin{aligned}\{\text{finite abelian extensions of } K\} &\longleftrightarrow \{\text{finite index open subgroups of } \mathbf{C}_K\} \\ L &\longmapsto \mathrm{Nm}(\mathbf{C}_L)\end{aligned}$$

7 Conclusion

Through an overview of class field theory, we have shown the importance of local-global principles in number theory. Very often, in order to understand a problem about rational numbers, or other global fields, it is very helpful to start by understanding the analogous problem for local fields, which is usually easier. We can then bundle all the local information together to solve the global problem, as we did for global class field theory using the idèle class group.

Let's finish by mentioning another example of this. Using results about group cohomology of the idèle class group closely related to class field theory, one can show that, for cyclic extensions L/K of global fields, an element of K is a norm from L if and only if it is a norm locally at every place. Using the relation between quadratic forms and norm maps of quadratic extensions described in Section 3.1, we can use this this to prove the Hasse-Minkowski theorem on quadratic forms mentionned at the end of Section 2.

References

[1] Milne, J. S. *Class field theory*. Online notes, available on the author's web site at `http://www.jmilne.org/math`.

[2] Milne, J. S. *Algebraic number theory*. Online notes, available on the author's web site at `http://www.jmilne.org/math`.