Reciprocity laws

Caleb Ji

September 23, 2024

1 What is quadratic reciprocity good for?

You may have heard of Gauss' law of quadratic reciprocity:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

for distinct odd primes p, q. With deep mathematical prescience, Gauss called this the "Theorem Aurum", though even he could not have foreseen the full wealth of mathematics this theorem would lead to. Indeed, while this result may initially seem little more than an isolated curiosity, its generalizations and reinterpretations was a driving force in the early days of algebraic number theory, culminating in the class field theory of the early 20th century. The goal of this article is to sketch some of these ideas, focusing on reciprocity laws as a unifying theme in class field theory.

Outline and Prerequisites

In Section 2 we define Legendre symbols and Jacobi symbols and give a proof of quadratic reciprocity using algebraic number theory. In section 3 we generalize these definitions to power residue symbols. While versions of the power reciprocity law can be stated without much extra machinery, to fully understand it we will need to introduce Hilbert symbols. The statement of Hilbert reciprocity involves local fields, but specializes to the classical reciprocity laws considered earlier. This leads to Section 4, where we explain Hilbert symbols from the perspective of local class field theory and Kummer theory. Then in Section 5 we put these ideas together to state global Artin reciprocity, which includes Hilbert reciprocity as a special case.

Sections 2 and 3 should be readable by anyone with a strong grasp of elementary number theory and abstract algebra. However, some standard notions from algebraic number theory will appear, such as the splitting of primes and the Frobenius element. If the reader is unfamiliar with these concepts, they can either take them on faith or take this opportunity to learn them. Sections 4 and 5 rely on algebraic number theory more heavily, and in particular a knowledge of local fields. This material, as well as the background for it, can be found in many places, such as [Mil20a], [Mil20b], and [Neu99].

2 Quadratic reciprocity revisited

In this section we review the definition of Legendre and Jacobi symbols and give a proof of quadratic reciprocity. Our proof is not the easiest, it has the advantage of giving a new interpretation of the meaning of a Legendre symbol through algebraic number theory. Although this method of proof isn't directly generalizable to the higher cases, it previews some of the concepts that will be used.

2.1 Legendre and Jacobi symbols

Definition 2.1 (Legendre symbol)**.** *For an odd prime p, we define the Legendre symbol for $a \in \mathbb{Z}$ as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \textit{ is a nonzero quadratic residue} \pmod p \\ -1 & a \textit{ is not a quadratic residue} \pmod p \\ 0 & p|a. \end{cases}$$

Because $\mathbb{F}_p^*$ is multiplicative, we have $\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \pmod p$, from which the multiplicativity of the Legendre symbol is clear.

One can easily extend the definition of Legendre symbols to Jacobi symbols in which the denominator is allowed to be any odd integer greater than 1.

Definition 2.2 (Jacobi symbol)**.** *Let n be an odd integer greater than 1 with prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$. We define the Jacobi symbol for $a \in \mathbb{Z}$ as*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{a_k}.$$

Note that the sign of the Jacobi symbol does not always indicate whether a is a quadratic residue $\pmod n$, but the Jacobi symbol does behave like the Legendre symbol formally; e.g. it satisfies multiplicativity. Furthermore, it also satisfies quadratic reciprocity.

Theorem 2.3 (Quadratic reciprocity)**.** *If p and q are two distinct odd primes, then we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}}.$$

Furthermore, using Jacobi symbols, if m and n are odd and relatively prime, we have

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{2}}.$$

There are many, many proofs of quadratic reciprocity. We will present one which is not the easiest or most elementary, but it has the key advantage of interpreting the Legendre symbol in terms of algebraic number theory, which will be useful to keep in mind for generalizations.

2.2 Splitting of prime ideals

Before class field theory really took off, mathematicians were able to understand important parts of it through quadratic, cubic, and quartic reciprocity laws. We begin by describing what the law of quadratic reciprocity implies for quadratic number fields.

Given two distinct odd primes p, p, set $p^* = (-1)^{(p-1)/2}p$ so that the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}[\sqrt{p^*}]$ is given by $\mathbb{Z}[\sqrt{p^*}]$. We can ask when (q) splits in $\mathcal{O}_K$. If p^* is a quadratic residue $\pmod q$, say $p^* \equiv k^2 \pmod q$, then $(q)|(k+\sqrt{p^*})(k-\sqrt{p^*})$, but (q) doesn't divide either, so it must split. Similarly, we can show that if p^* is not a quadratic residue $\pmod q$, then (q) remains inert. In other words, $\left(\frac{p^*}{q}\right)$ indicates whether (q) splits in $\mathcal{O}_K$.

However, this answer is not completely satisfactory. For example, it doesn't give the density of primes which split. Instead, it would be much nicer to have a condition $\pmod p$. But quadratic reciprocity gives us precisely that! Indeed, by quadratic reciprocity, we have $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. This means that (q) splits precisely when q is a quadratic residues $\pmod q$. Thus the set of primes which split is determined by half the possible residues $\pmod q$, and furthermore by Dirichlet's theorem comprise a density of half the primes.

2.3 A proof using algebraic number theory

Reflecting on the previous interpretation, we see that by quadratic reciprocity, both $\left(\frac{p^*}{q}\right)$ and $\left(\frac{q}{p}\right)$ indicate whether (q) splits in $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{p^*}}{2}]$. If one could prove this statement on its own, it would give a very satisfying proof of quadratic reciprocity as it would show that these two Legendre symbols both have a natural meaning which was not at all obvious from their definition. We have already seen how $\left(\frac{p^*}{q}\right)$ indicates the splitting of (q) in a fairly elementary way. Thus it remains to show

$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow (q) \text{ splits completely in } \mathbb{Z}\left[\frac{1+\sqrt{p^*}}{2}\right], \tag{1}$$

and this will take a bit of algebraic number theory.

Note that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/(p-1)$, so there is a unique intermediate quadratic extension corresponding to the subgroup $\mathbb{Z}/\frac{p-1}{2}$. We can explicitly construct this quadratic extension by considering the Gauss sum $\sum_{i=1}^{p-1}\left(\frac{-1}{p}\right)\zeta_p^i = \sqrt{p^*}$. This shows that this quadratic extension is indeed given by $K = \mathbb{Q}(\sqrt{p^*})$.

Let α be a prime of $\mathbb{Z}[\frac{1+\sqrt{p^*}}{2}]$ lying over (q) and let β be a prime of $\mathbb{Z}[\zeta_p]$ lying over (q). Because (q) is unramified in both these extensions, we have isomorphisms

The key to the proof of 1 will be to consider the Frobenius element $\phi \in \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ associated to β. We recall that this is the element which acts by $\phi(x) = x^q$ on $\mathbb{Z}[\zeta_p]/\beta$, which can be concretely realized as the element of the Galois group sending ζ_p to ζ_p^q. If q is a quadratic residue, then the subgroup generated by ϕ has index 2 and fixes K. Otherwise, it cannot contain this subgroup and thus cannot fix K. Thus, to prove 1 it suffices to show

$$\phi \text{ fixes } K \Leftrightarrow (q) \text{ splits completely in } \mathbb{Z}\left[\frac{1+\sqrt{p^*}}{2}\right]. \tag{2}$$

To do this, consider the restriction of ϕ to K. As an element of $\mathrm{Gal}(K/\mathbb{Q})$, this is a Frobenius element associated to α. Now since ϕ_K generates $\mathrm{Gal}(\mathcal{O}_K/\alpha/\mathbb{Z}/q)$, it fixing K is equivalent to the triviality of that group, which is equivalent to q splitting in $\mathcal{O}_K$, as desired.

Exercises

1. Determine which primes split in the ring of integers of $\mathbb{Q}[\sqrt{-q^*}]$.
2. Determine the splitting behavior of all primes in the ring of integers of $\mathbb{Q}[\sqrt{n}]$ for all n.

3 Power residue symbols

We can naïvely try to generalize quadratic reciprocity by simply replacing squares with nth powers. In fact, this approach does work and was what mathematicians historically considered. By the time of class field theory this perspective had already been thoroughly engulfed in deeper theories, but it is still useful to start here.

3.1 Definition of power residue symbols

Power residue symbols directly generalize Legendre symbols. Recall that we may define Legendre symbols in the following way:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}.$$

where $a \in \mathbb{Z}$ and p is an odd prime.

In particular, the target is a 2nd root of 1 in $\mathbb{Z}/p$ as long as $p \nmid a$. If we want to generalize this definition to nth powers, we first need to work over a number field K containing $\mathbb{Q}(\zeta_n)$. Then $\mathbb{Z}$ is replaced with $\mathcal{O}_K$, p is replaced with a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ not dividing (n), and the target is $\mathcal{O}_K/\mathfrak{p}$.

Definition 3.1. *With the above setup, for any $a \in \mathcal{O}_K$, the nth power residue symbol is defined as*

$$\left(\frac{a}{\mathfrak{p}}\right)_n := a^{(N(\mathfrak{p})-1)/n}$$

where the result, if nonzero (i.e. $a \notin \mathfrak{p}$), is taken as an nth root of unity in $\mathcal{O}_K/\mathfrak{p}$.

For this definition to make sense, we need to know the following facts.

1. $(N(\mathfrak{p}) - 1)/n$ is an integer.
2. $a^{(N(\mathfrak{p})-1)/n}$ is equivalent to an nth root of unity $\pmod{\mathfrak{p}}$.

Proof. The first is a corollary of the following fact: the nth roots of unity $1, \zeta_n, \dots, \zeta_n^{n-1}$ lie in distinct residue classes in $\mathcal{O}_K/\mathfrak{p}$. Indeed, because $\prod_{i=1}^{n-1}(1-\zeta_n^i) = n$, if $\mathfrak{p}$ divides the ideal generated by any of the $1-\zeta_n^i$, then it divides (n), contradiction.
Thus μ_n, which of size n, is a subgroup of the multiplicative group of the finite field $\mathcal{O}_K/\mathfrak{p}$, which has size $N(\mathfrak{p}) - 1$. The result follows from Lagrange's theorem.

For 2, since $|(\mathcal{O}_K/\mathfrak{p})^*| = N(\mathfrak{p}) - 1$, we have $x^n \equiv 1 \pmod{\mathfrak{p}}$ where $x := a^{(N(\mathfrak{p})-1)/n}$. Then $\mathfrak{p} | \prod_{i=1}^{n}(x - \zeta_n^i)$, and since $\mathfrak{p}$ is a prime ideal it divides the ideal generated by one of the terms, so we are done. □

As with the Jacobi symbols, we can extend this definition so that the denominator can be any ideal in $\mathcal{O}_K$. Namely, if $I = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_k^{c_k}$ is an ideal of $\mathcal{O}_K$, then

$$\left(\frac{a}{I}\right)_n := \prod_{i=1}^{k}\left(\frac{a}{\mathfrak{p}_i}\right)_n^{c_i}.$$

A classical result extending quadratic reciprocity to some higher powers is given by the Eisenstein reciprocity law.

Theorem 3.2 (Eisenstein reciprocity). *Let l be an odd prime, let a be an integer relatively prime to l, and let α be a primary element of $\mathbb{Z}[\zeta_l]$ relatively prime to a. Then*

$$\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l.$$

Rather than discussing this result further here, we refer the reader to [IR82] for a discussion and proof. Instead, we will discuss a more general result, known as the reciprocity law for power residues. To formulate it, we need to use Hilbert symbols $(a, b)_{\mathfrak{p}}$, which we will soon define. The law states:

Theorem 3.3 (Power reciprocity law). *Let K be a number field containing the nth roots of unity. If $a, b \in K^*$ are relatively prime to each other and to n, then*

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = \prod_{\mathfrak{p}|n\infty} (a,b)_{\mathfrak{p}}.$$

This is a vast – though far from the most general – generalization of quadratic reciprocity, which can be recovered by setting $K = \mathbb{Q}$ and $n = 2$. It in turn can be deduced from a more natural formulation, known as the Hilbert reciprocity law.

Theorem 3.4 (Hilbert reciprocity). *For $a, b \in K^*$ we have*

$$\prod_{\mathfrak{p}} (a,b)_{\mathfrak{p}} = 1.$$

3.2 Hilbert symbols – first definition

We will need to think a bit about local fields in order to make sense of this reciprocity law for power residues. The prototypical example of a local field is the field of p-adic numbers $\mathbb{Q}_p$, so for simplicity we will stick with $\mathbb{Q}_p$ here.

Hilbert symbols work for every n, but they are easiest to define for $n = 2$. For a fixed n, the ideas is that we can define a *local* version of the Legendre symbol, i.e. one for every prime p. Then Hilbert reciprocity tells us something about what happens when we patch them all up, and this implies quadratic reciprocity.

Definition 3.5. *The Hilbert symbol for $n = 2$ is the bilinear pairing $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \to \{\pm 1\}$ defined by*

$$(a,b)_p = \begin{cases} 1 & ax^2 + by^2 = 1 \textit{ has a solution in } \mathbb{Q}_p^2 \\ -1 & \textit{otherwise}. \end{cases}$$

The fact that it is bilinear; i.e. $(a, bc)_p = (a, b)_p (a, c)_p$ is highly nontrivial and we will only see it later when we give a completely different interpretation of the Hilbert symbol. While one must understand this alternate definition to fully appreciate where the Hilbert symbol is coming from, one can still see from the given definition that it is hinting at detecting squares. Indeed, as the definition implies, if a is a square in $\mathbb{Q}_p^*$ then $(a, b)_p = 1$ by setting $x^2 = a^{-1}$ and $y = 0$. So this is sort of asking if a is a square 'modulo b' in a certain sense, and has the advantage of being evidently symmetric in a and b (this is special to the case of $n = 2$; in general they are reciprocals of each other).

Remark. In the statement of Hilbert reciprocity, a and b come from the number field K. The notation $(a, b)_{\mathfrak{p}}$ we are implicitly taking a and b inside $K_{\mathfrak{p}}$ via the natural embedding $K \hookrightarrow K_{\mathfrak{p}}$.

Let us now check that the power reciprocity law and Hilbert reciprocity both specialize to quadratic reciprocity when $K = \mathbb{Q}$ and $n = 2$. For simplicity we will just take the case of two primes, though this method works for the general case with Jacobi symbols as well. First we compute some Hilbert symbols. If we take $a = p, b = q$ distinct odd primes, then if r is a different odd prime then $(p, q)_r = 1$. Indeed, use the Pigeonhole principle to get a solution $\pmod p$, and then apply Hensel's lemma. Next, we see that $(p, q)_p = \left(\frac{q}{p}\right)$ and $(p, q)_q = \left(\frac{p}{q}\right)$. Now we check when $px^2 + qy^2 = 1$ has solutions in $\mathbb{Q}_2^2$. Here Hensel's lemma allows us to lift solutions in $\mathbb{Z}/8\mathbb{Z}$, so checking the remaining cases gives $(p, q)_2 = (-1)^{(p-1)(q-1)/4}$. Finally, $(p, q)_\infty$ asks if there is a solution in $\mathbb{R}$, which holds since p and q are taken to be positive.

Now the power reciprocity law gives

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (p,q)_2(p,q)_\infty = (-1)^{(p-1)(q-1)/4},$$

as desired. Hilbert reciprocity gives the exact same result.

4 Local class field theory and Hilbert reciprocity

The power reciprocity law marks a certain endpoint in the development of reciprocity laws as viewed as indicators of power residues. However, its connection to Hilbert reciprocity indicates the way to a road beyond, leading to class field theory.

4.1 Local class field theory

In order to fully appreciate the next step in the development of reciprocity laws, namely Hilbert reciprocity, we will discuss some results of local class field theory. The gist of the connection is that these nth power indicators are really a special case of norm groups, which are used to describe the abelian extensions of local fields.

The main theorems of local class field theory can be summarized as follows.

Theorem 4.1 (Local reciprocity law). *Let K be a nonarchimedean local field. Then the commutative diagram below satisfies the following properties.*

$$\begin{tikzcd}
K^* \arrow[r, "\phi_K"] \arrow[d] & \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \arrow[d] \\
K^*/N(L^*) \arrow[r, "{\phi_{L/K}, \cong}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

(a) Let π be a uniformizer of K and let L be an unramified extension of K. Then $\phi_K(\pi)$ acts by the Frobenius on $\mathrm{Frob}_{L/K}$ *on L.*

(b) When restricted to any finite abelian extension L/K, we obtain an isomorphism

$$\phi_{L/K} : K^*/N(L^*) \cong \mathrm{Gal}(L/K).$$

(c) [Local existence theorem] Every open subgroup of finite index of K^* can be realized as the norm group $N(L^*)$ of some finite abelian extension L/K.

Remarks. (a) Part (a) holds for any choice of π and any finite unramified extension, not just the abelian ones.

(b) The result holds for any finite extension L if we replace $\mathrm{Gal}(L/K)$ with its abelianization $\mathrm{Gal}(L/K)^{\mathrm{ab}}$. The maps ϕ_K and $\phi_{L/K}$, or their inverses are known has local reciprocity maps. They induce an isomorphism between $\widehat{K^*}$ and $\mathrm{Gal}(K^{ab}/K)$.

(c) The converse holds and is much easier to prove.

Example 4.2. Consider the extension $L/K = \mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$, where $(n,p) = 1$. This is an unramified extension. Indeed, $\mathbb{Q}_p[\zeta_{p^m-1}]$ is the unique unramified extension of $\mathbb{Q}_p$ of order m, and if $(n,p) = 1$ then $\mathbb{Q}_p(\zeta_n)$ is contained in such a cyclotomic extension. We will illustrate what the isomorphism $\phi_{L/K}$ gives us in this instance, and in particular compute the norm group $N_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_n)^*)$.

Since L/K is unramified we have

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{F}_p[\zeta_n]/\mathbb{F}_p) \cong \mathbb{Z}/d,$$

where d is the order of $p \pmod n$. This tells us that the norm group must be a subgroup of $\mathbb{Q}_p^*$ with quotient group isomorphic to $\mathbb{Z}/d$. We have

$$\mathbb{Q}_p^* \cong \mathbb{Z}_p^* \times \langle p \rangle \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}.$$

Since L/K is unramified, we have $L^* = \mathcal{O}_L^* * \langle p \rangle$. Note that $N_{L/K}(p) = p^d$ and $N(\mathcal{O}_L^*) \subset \mathbb{Z}_p^*$. Thus the norm group $N_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_n)^*)$ contains $\mathbb{Z}_p^* * \langle p^d \rangle \subset \mathbb{Q}_p^*$ yet has index d; thus it must be precisely that. In particular, this shows that $N(\mathcal{O}_L^*) = \mathbb{Z}_p^*$.

More generally, when L/K is an unramified extension of local fields, the example above generalizes to show that $N(\mathcal{O}_L^*) = \mathcal{O}_K^*$. However, it is also possible to prove this without using class field theory. This is left as an exercise.

4.2 Kummer theory

An important example of local class field theory arises from Kummer theory. If a field K contains n distinct roots of unity (i.e. contains the roots of $x^n - 1$ and has characteristic relatively prime to n), Kummer theory explains how abelian extensions L/K of exponent n (i.e. the lcm of the orders of the elements) arise. Namely, they simply arise from extracting nth roots.

First, one sees that since K contains nth roots, the Galois group of any extension adjoining nth roots will be abelian, as the automorphisms multiply generators by elements of K. The fact that any such extension comes about this way requires some Galois cohomology or étale cohomology. For the algebraic geometer, the Kummer sequence comes from the exact sequence of sheaves

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 1$$

on the étale site $(\mathrm{Spec}\, K)_{\text{ét}}$. This leads to a long exact sequence which, after applying Hilbert Theorem 90: $H^1(\mathrm{Spec}\, K, \mathbb{G}_m) = 0$, one obtains an isomorphism

$$K^*/(K^*)^n \cong H^1(\mathrm{Spec}\, K, \mu_n).$$

Now $H^1(\mathrm{Spec}\, K, \mu_n) = H^1(G_K, \mu_n)$ classifies μ_n-torsors over $\mathrm{Spec}\, K$. The nontrivial ones are $\mathbb{Z}/n$-extensions of K, and the isomorphism sends $a \in K^*/(K^*)^n$ to the extension $K[a^{1/n}]/K$.

The discussion above classifies cyclic extensions of K; now what about all extensions with exponent n? This simply requires some elementary group theory, and is left as an exercise.

Exercise 4.1. Let K be a field containing the nth roots of unity with $(n, \mathrm{char}\, K) = 1$. Then if L/K is a finite abelian Galois extension with exponent dividing n, we have

$$L \cong K(a_1^{1/n}, \cdots a_k^{1/n})$$

for some $a_i \in K$.

From this we conclude that the maximal abelian extension of K of exponent n is given by $L = K[\sqrt[n]{K^*}]$. One obvious question is: is this a finite extension? And what happens when we apply class field theory to it?

Example 4.3. Let $L = K[\sqrt[n]{K^*}]$ be the extension of K obtained by obtaining all nth roots.

First, we note that Kummer theory gives an isomorphism

$$K^*/(K^*)^n \cong H^1(G_K, \mu_n) \cong H^1(\mathrm{Gal}(L/K), \mu_n)$$

as $\mathrm{Gal}(L/K)$ is the maximal abelian quotient of G_K with exponent dividing n. Note that this looks like local Artin reciprocity! Indeed, by a direct analysis we have that $K^*/(K^*)^n$ is finite, so L/K is indeed a finite extension. Since $\mathrm{Gal}(L/K)$ acts trivially on μ_n, the size of this Galois group is just $|\mathrm{Gal}(L/K)| = |K^*/N(L^*)|$ by class field theory. But it is also equal to $|K^*/(K^*)^n$. Furthermore, $K^*/N(L^*)$ has exponent n (since $\mathrm{Gal}(L/K)$ does) and thus $(K^*)^n \subset N(L^*)$. Thus $N(L^*) = (K^*)^n$.

4.3 Hilbert reciprocity revisited

We will now give a new definition of Hilbert symbols, following [Neu99], V.3. With our knowledge about $L = K[\sqrt[n]{K^*}]$, we will see how it generalizes the nth power residue symbols from earlier.

Let K be a local field containing the nth roots of unity. We have the following isomorphisms from local class field theory and Kummer theory:

$$\mathrm{Gal}(L/K) \cong K^*/K^{*n}, \qquad \mathrm{Hom}(\mathrm{Gal}(L/K, \mu_n) \cong K^*/K^{*n}.$$

We recall that the second one is defined by associating $\alpha \in K^*/K^{*n}$ with $\sigma(\alpha)/\alpha$. Taking these isomorphisms into account, we obtain a nondegenerate bilinear pairing

$$(-,-)_{\mathfrak{p}} \colon K^*/K^{*n} \times K^*/K^{*n} \to \mu_n.$$

This is the Hilbert symbol. First, let us note that local class field theory provides us with the following definition.

Definition 4.4 (local norm residue symbol). *The local norm residue symbol*

$$(-, L/K) \colon K^* \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

is defined by the local Artin map.

When we set $L = K(\sqrt[n]{b})$, we get

$$(a, K(\sqrt[n]{b})/K)\sqrt[n]{b} = (a,b)_{\mathfrak{p}}\sqrt[n]{b}.$$

The following result, which takes some work, connects the Hilbert symbols to the power residue symbols, which we recall were defined by

$$\left(\frac{a}{\mathfrak{p}}\right)_n := a^{(N(\mathfrak{p})-1)/n}.$$

Proposition 4.5 ([Neu99], p. 336). *Setting $a = \pi$, a uniformizer, we have*

$$\left(\frac{b}{\mathfrak{p}}\right) = (\pi, b)_{\mathfrak{p}}.$$

We now leave the question of reconciling this approach to Hilbert symbols with the previous one as an exercise.

Exercise 4.2. Identifying this definition of the Hilbert symbol with the previous one given in the case of $n = 2$.

The benefit to this new definition is that bilinearity is clear. From the local norm residue symbol interpretation, we see that $(a,b)_{\mathfrak{p}} = 1$ implies that a is a norm in the extension $K(\sqrt[n]{b})/K$. Furthermore, the nondegenerate condition indicates that if $(a,b)_{\mathfrak{p}} = 1$ for all $b \in K^*$, then $a \in K^{*n}$. One can also prove that $(a,b)_{\mathfrak{p}} = (b,a)_{\mathfrak{p}}^{-1}$.

We restate Hilbert reciprocity.

Theorem 4.6 (Hilbert reciprocity). *If K is a number field and $a, b \in K^*$, then*

$$\prod_{\mathfrak{p}} (a,b)_{\mathfrak{p}} = 1$$

where $\mathfrak{p}$ ranges over all places of K.

In the next section, we will deduce Hilbert reciprocity from global Artin reciprocity.

5 Artin reciprocity and the global theory

Global class field theory has a long and interesting history. Nowadays there are two main ways to state it: in terms of ideals and in terms of idèles. Using idèles, the reciprocity statement becomes simple and mirrors that of local class field theory. Another major benefit is that it lends itself well to next steps, namely Tate's thesis and its generalization to the Langlands program.

5.1 Statements of the main theorems

Let K be a global field, e.g. a number field. Then the ring of adèles $\mathbb{A}_K$ consists of the restricted product of all completions K_v (including at the infinite places), i.e., with almost all entries in $\mathcal{O}_v$. Then the idèles are defined as $\mathbb{I}_K = \mathbb{A}_K^*$. The ring of idèles takes the place of the group of units K_v^* in local class field theory.

Theorem 5.1 (Artin reciprocity). *There exists a global Artin map $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying the following properties.*

(a) The global Artin map satisfies $\phi_K(K^\times) = 1$.

(b) For every finite abelian extension L/K, ϕ_K induces an isomorphism

$$\phi_{L/K} \xrightarrow{\cong} \mathbb{I}_K/(K^\times \cdot \mathrm{Nm}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K).$$

Theorem 5.2 (existence theorem). *Let $C_K = \mathbb{I}_K/K^\times$ be the idele class group. For every open subgroup $N \subset C_K$ of finite index, there exists a unique finite abelian extension L/K such that* $\mathrm{Nm}(L/K) = N$.

The fact that the global Artin map factors through the idèle class group $C_K = \mathbb{I}_K/K^*$ is a difficult and key part of class field theory. The global Artin map extends to give an isomorphism

$$\widehat{C_K} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

The construction of the global Artin map arises directly from the construction of each individual local Artin map. Namely, we have a commutative diagram

$$\begin{tikzcd}
K_v^* \arrow[r, "\phi_v"] \arrow[d] & \mathrm{Gal}(L_w/K_v) \arrow[d] \\
\mathbb{I}_K \arrow[r, "\phi|_L"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

where the top arrow is the local Artin map and the bottom arrow is the global Artin map restricted to $\mathrm{Gal}(L/K)$. Proving this map indeed satisfies all the properties of the theorems is very involved.

5.2 Recovering Hilbert reciprocity

By choosing various field extensions of K in the statement of Artin reciprocity, we obtain various reciprocity laws. We recover Hilbert reciprocity by considering the case of $L = K[b^{1/n}]$.

Here, we do not use the isomorphism between the quotient of the idèle group and the Galois group, but rather the fact that the global Artin map is trivial when restricted to $K^{\times}$. Indeed, by the construction of the global Artin map, for any $a \in K^*$ we have

$$1 = \phi_K(a) = \prod_v \phi_{K_v}(b) = \prod_v (a, K_v[b^{1/n}]/K_v) = \prod_v (a, b),$$

as desired.

References

[IR82] Kenneth F. Ireland and Michael I. Rosen. *A classical introduction to modern number theory / Kenneth Ireland, Michael, Michael Rosen.* Graduate texts in mathematics ; 84. Springer, New York, 1982.

[Mil20a] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[Mil20b] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.