Higher Reciprocity Laws

Wojtek Wawrów

20 August 2018

Introduction

Quadratic reciprocity is, on its own, already a quite profound statement, but on the other hand it is just the first in a large family of statements, known collectively as reciprocity laws, which in various ways describe behavior of polynomials modulo primes, but also behavior of primes in various fields. In this talk we shall explore this variety of generalizations.

1 Quadratic Reciprocity

Recall the following definition:

Definition 1.1. For p an odd prime and $a \in \mathbb{Z}$ not divisible by p we define the *Legendre symbol* by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

The *law of quadratic reciprocity* is as follows:

Theorem 1.2. *For p, q distinct odd primes,*

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

One way of viewing this theorem is to fix the top number, call it a, and ask about the values of $\left(\frac{a}{p}\right)$ as p varies. It turns out that the quadratic character of a modulo different primes p is described very simply by a congruence condition on p modulo $4a$.

It's clear that $\left(\frac{a}{p}\right)$ describes how the polynomial $x^2 - a$ factors modulo p. What's perhaps less clear is that the same value describes how p factors into ideals in the ring of integers $\mathcal{O}_K$ of the field $K = \mathbb{Q}(\sqrt{a})$. Indeed, we have:

Proposition 1.3. *Let p be an odd prime and $a \in \mathbb{Z}$ be not divisible by p. Then (p) is either a prime ideal or a product of two prime ideals. The former happens iff $\left(\frac{a}{p}\right) = -1$.*

Proof (sketch). The first statement follows from some general facts about factorization of primes: if we factor $(p) = \mathfrak{p}_1 \dots \mathfrak{p}_k$ and $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field with p^{f_i} elements, then $f_1 + \dots + f_k$ is equal to the degree of K over $\mathbb{Q}$, which is 2 in our case, hence either $k = 1, f_1 = 2$ or $k = 2, f_1 = f_2 = 1$.

Take now any prime factor $\mathfrak{p}$ of (p) and consider $\mathcal{O}_K/\mathfrak{p}$. Observe that the residue class of $\sqrt{a}$ is a square root of a. If $\left(\frac{a}{p}\right) = 1$, the square roots of a modulo $\mathfrak{p}$ are congruent to integers, which

implies $\sqrt{a}$ is congruent to an integer modulo $\mathfrak{p}$. It's not hard to see this couldn't be the case if $\mathfrak{p} = (p)$, so (p) must factor.

Now, if $\left(\frac{a}{p}\right) = -1$, then $\mathcal{O}_K/\mathfrak{p}$ cannot have p elements, since a has no square root in $\mathbb{F}_p$, so we must have that $\mathfrak{p} = (p)$ is prime. □

Therefore, quadratic reciprocity can be used to describe how different primes factor in some fixed quadratic extension $\mathbb{Q}(\sqrt{a})$. Actually, we will use this point of view to *prove* quadratic reciprocity, but we will look into that later.

It is possible to extend the Legendre symbol and quadratic reciprocity so that we don't have to restrict ourselves to primes only.

Definition 1.4. For $a \in \mathbb{Z}$ and odd $b \in \mathbb{N}$ relatively prime to a we define the *Jacobi symbol* as follows: first write $b = p_1 \dots p_k$ as a product of odd primes. Then

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

From this definition it is clear $\left(\frac{a}{b}\right)$ is multiplicative in both the top and bottom variables. From quadratic reciprocity it's not hard to deduce:

Theorem 1.5. *For two relatively prime odd numbers $a, b \in \mathbb{N}$,*

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

2 Cubic and Biquadratic Reciprocity

Historically, the first analogues of quadratic reciprocity were, unsurprisingly, cubic and biquadratic (or quartic) reciprocity, which respectively concern cubes and fourth powers. We start with the former.

Firstly, $\mathbb{Z}$ is not the right ring to consider cubic reciprocity in. Rather, we look at $\mathbb{Z}[\omega]$, which contains all the cube roots of unity $1, \omega, \omega^2$. Consider now a prime $\pi \in \mathbb{Z}[\omega]$; just like how we exclude 2 in quadratic reciprocity, we exclude primes dividing 3 here (which are the associates of $1 - \omega$). Now, for any $\alpha \in \mathbb{Z}[\omega]$ not divisible by π we would like to define an analogue $\left(\frac{\alpha}{\pi}\right)_3$ of the Legendre symbol $\left(\frac{a}{p}\right)$. It should take values in $\{1, \omega, \omega^2\}$ and be equal to 1 if and only if α is a cube modulo π, but it's not clear how to assign values to non-cubes. To the rescue comes Euler's criterion:

Proposition 2.1. *For p prime in $\mathbb{Z}$, $a \in \mathbb{Z}$ indivisible by p, we have*

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

It has the following analogue in the considered case:

Proposition 2.2. *For π, α as above, there is precisely one $\rho \in \{1, \omega, \omega^2\}$ such that*

$$\alpha^{\frac{N\pi-1}{3}} \equiv \rho \pmod{\pi}.$$

Moreover, $\rho = 1$ if and only if α is a cube modulo π.

We now *define* the cubic residue symbol using the above.

Definition 2.3. The *cubic residue symbol* $\left(\frac{\alpha}{\pi}\right)_3$ is the unique element of $\{1, \omega, \omega^2\}$ satisfying

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N\pi-1}{3}} \pmod{\pi}.$$

For β relatively prime to 3α, say $\beta = \pi_1 \dots \pi_k$, we define

$$\left(\frac{\alpha}{\beta}\right)_3 = \prod_{i=1}^{k} \left(\frac{\alpha}{\pi_k}\right)_3.$$

Before we state the reciprocity law for this symbol, we make one more definition.

Definition 2.4. We call $\alpha \in \mathbb{Z}[\omega]$ *primary* if it is congruent to an integer modulo $(1-\omega)^2$.

One can show that for any $\alpha \in \mathbb{Z}[\omega]$, $\rho\alpha$ is primary for precisely one cube root of unity ρ.

Theorem 2.5. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be primary, relatively prime and not divisible by $1-\omega$. Then*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3.$$

This theorem can be again viewed as describing how primes factor in a cubic extension $Q(\omega)(\sqrt[3]{\alpha})$ – a prime π either splits into three factors or remains prime, depending on whether $\left(\frac{\alpha}{\pi}\right)_3$ is 1 or not.

Even though cubic reciprocity deals with $\mathbb{Z}[\omega]$, we can translate some results it gives directly to $\mathbb{Z}$. For example, let's tackle the cubic character of 2. Let p be a prime congruent to 1 (mod 3) (otherwise everything is a cube modulo p) and let π be its prime factor; replacing π by an associate if necessary, we may without loss of generality assume π is primary. Then 2 is a cube modulo p if and only if it's a cube modulo π. Cubic reciprocity gives $\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3$ and this is equal to 1 if and only if $\pi \equiv 1 \pmod{2}$. Since $N(\pi) = p$, this can be translated back into $\mathbb{Z}$ and turns out to be equivalent to p being expressible as $a^2 + 27b^2$ for some $a, b \in \mathbb{Z}$.

For biquadratic reciprocity almost all of the above can be repeated, so we only give the definitions and the result.

Definition 2.6. For $\pi \in \mathbb{Z}[i]$ a prime not dividing 2 (i.e. not associate to $1-i$) and $\alpha \in \mathbb{Z}[i]$ not divisible by π, we define the *biquadratic residue symbol* $\left(\frac{\alpha}{\pi}\right)_4$ to be the unique element of $\{1, i, -1, -i\}$ satisfying

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{N\pi-1}{4}} \pmod{\pi}.$$

For β relatively prime to 2α, say $\beta = \pi_1 \dots \pi_k$, we define

$$\left(\frac{\alpha}{\beta}\right)_4 = \prod_{i=1}^{k} \left(\frac{\alpha}{\pi_k}\right)_4.$$

Definition 2.7. We call $\alpha \in \mathbb{Z}[i]$ *primary* if it is congruent to 1 modulo $(1-i)^3$. Every element of $\mathbb{Z}[i]$ not divisible by $1-i$ has exactly one primary associate.

Theorem 2.8. *Let $\alpha, \beta \in \mathbb{Z}[i]$ be primary, relatively prime and not divisible by $1-i$. Then*

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{\frac{N\alpha-1}{4}\cdot\frac{N\beta-1}{4}} \left(\frac{\beta}{\alpha}\right)_4.$$

Again, this describes factorization of primes in $\mathbb{Q}(i)(\sqrt[4]{\alpha})$, but this time we have three possibilities: π splits into either one, two or four primes, depending on whether $\left(\frac{\alpha}{\pi}\right)_4$ is $\pm i$, -1 or 1.

3 Eisenstein Reciprocity

We now generalize the residue symbol to arbitrary powers. Let ζ_n be a primitive n-th root of unity. Then $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, which means that in this ring we have unique factorization into ideals. However, unlike for small n, in general we do not have unique factorization of elements, which is why to express the reciprocity law, we *need* to use some analogue of the Jacobi symbol.

Definition 3.1. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[\zeta_n]$ not dividing n and $\alpha \in \mathbb{Z}[\zeta_n]$ not in $\mathfrak{p}$. We define the *n-th power residue symbol* $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ to be the unique n-th root of unity such that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{\frac{N\mathfrak{p}-1}{n}} \pmod{\mathfrak{p}}$$

where $N\mathfrak{p}$ is the norm of $\mathfrak{p}$, defined as the number of elements in $\mathbb{Z}[\zeta_n]/\mathfrak{p}$ (which is $1 \pmod n$ since this is a field containing n-th roots of unity.)

Given any ideal $\mathfrak{b}$ relatively prime to $n\alpha$, write it as a product of prime ideals $\mathfrak{b} = \mathfrak{p}_1 \dots \mathfrak{p}_k$ and define

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_n = \prod_{i=1}^{k} \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n.$$

Finally, for $\beta \in \mathbb{Z}[\zeta_n]$ relatively prime to $n\alpha$ let

$$\left(\frac{\alpha}{\beta}\right)_n = \left(\frac{\alpha}{(\beta)}\right).$$

We can make those definition in any number field containing ζ_n.

Unfortunately, at this point we can only state the reciprocity law for n an odd prime, which we now rename to ℓ. We note the only prime dividing ℓ is $(1-\zeta_\ell)$.

Definition 3.2. We say $\alpha \in \mathbb{Z}[\zeta_\ell]$ is *primary* if it is congruent to an integer modulo $(1-\zeta_\ell)^2$.

Similarly to the cubic case, for any $\alpha \in \mathbb{Z}[\zeta_\ell]$ there is a unique ℓ-th root of unity ρ such that $\rho\alpha$ is primary. We can finally state the Eisenstein reciprocity law:

Theorem 3.3. *Let ℓ be an odd prime. Let $\alpha \in \mathbb{Z}[\zeta_\ell]$ be primary and $b \in \mathbb{Z}$ be such that α, b are relatively prime to each other and to $1-\zeta_\ell$. Then*

$$\left(\frac{\alpha}{b}\right)_\ell = \left(\frac{b}{\alpha}\right)_\ell.$$

We give one quick application of this result.

Proposition 3.4. *Suppose $a \in \mathbb{N}$ is not divisible by ℓ and is an ℓ-th power modulo p for all but finitely many primes p. Then a is an ℓ-th power in $\mathbb{N}$.*

Proof. We show the contrapositive: if a is *not* an ℓ-th power, it is not an ℓ-th power modulo p for infinitely many primes p. Factor (a) into a product of prime ideals, $(a) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$ where the $\mathfrak{p}_i$ are pairwise distinct and distinct from $(1-\zeta_\ell)$. One can show all the primes $\mathfrak{p}_i$ are *unramified* in $\mathbb{Z}[\zeta_\ell]$, which means that the exponents in the factorization of (a) are the same as the exponents in the prime factorization of a in $\mathbb{Z}$, in particular not all of them are divisible by ℓ, say $\ell \nmid e_k$.

Take any set S of prime ideals in $\mathbb{Z}[\zeta_\ell]$ which includes $(1-\zeta_\ell)$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_{k-1}$ but not $\mathfrak{p}_k$. By the Chinese remainder theorem, there is an element $\alpha \in \mathbb{Z}[\zeta_\ell]$ which is congruent to $1 \pmod{\mathfrak{p}}$

for all $\mathfrak{p} \in S$, to 1 $\pmod{(1-\ell)^2}$, and to $\delta \pmod{\mathfrak{p}_k}$, where δ is any element such that $\left(\frac{\delta}{\mathfrak{p}_k}\right)_\ell = \zeta_\ell$ (it's not hard to see such a δ exists). In particular, $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell = 1$ for $\mathfrak{p} \in S$, $\left(\frac{\alpha}{\mathfrak{p}_k}\right)_\ell = \zeta_\ell$ and α is primary. We hence have

$$\left(\frac{\alpha}{a}\right)_\ell = \left(\frac{\alpha}{(a)}\right)_\ell = \prod_{i=1}^{k} \left(\frac{\alpha}{\mathfrak{p}_i}\right)_\ell^{e_i} = \zeta_\ell^{e_k} \neq 1.$$

On the other hand, Eisenstein reciprocity gives

$$1 \neq \left(\frac{\alpha}{a}\right)_\ell = \left(\frac{a}{\alpha}\right)_\ell$$

which implies that for some prime factor $\mathfrak{q}$ of α, which must necessarily be distinct from the elements of S, a is not an ℓ-th power modulo $\mathfrak{q}$. This way we show there are infinitely many prime ideals in $\mathbb{Z}[\zeta_\ell]$ modulo which a is not an ℓ-th power, and they lie over infinitely many primes in $\mathbb{Z}$ modulo which a is not an ℓ-th power. □

The statement of Eisenstein reciprocity leaves many questions – can we generalize this to any n? To non-integer b? The answer out to be "yes" and it can be done in a way similar to the one above, but we now run into a more subtle notion of "primary". Instead of getting into that, we will present a more general approach, which lets us generalize it even to non-primary elements.

4 Hilbert Reciprocity

Before we extend our reciprocity laws further, we go back and express the quadratic reciprocity using different notation. First, we need one general notion:

Definition 4.1. Let K be a finite extension of $\mathbb{Q}$. A *finite place* (or a *finite prime*) is any prime ideal in the ring of integers $\mathcal{O}_K$. A *real place* is an embedding of K into $\mathbb{R}$. A *complex place* is a pair of complex conjugate embeddings of K into $\mathbb{C}$ which don't have image in $\mathbb{R}$. Real and complex places are collectively known as *infinite places* (or *infinite primes*).

The reason why we put those two seemingly unrelated notions into one category of a "place" is that together they bijectively correspond to equivalence classes of absolute values on K (that is guaranteed by a generalization of Ostrowski's theorem). With this in mind, every place P (finite or not) on K determines an embedding of K into a locally compact field K_P – in the infinite case it's $\mathbb{R}$ or $\mathbb{C}$, in the finite case it's a analogue of the p-adic numbers; in both cases it's the completion with respect to those absolute values.

$\mathbb{Q}$ has exactly one infinite place, namely it's standard embedding into $\mathbb{R}$, which we denote by ∞. In general, with ∞ we will denote the "formal product" of all infinite primes. The finite places are just the usual primes. We now define kind of an "extension" of the Legendre symbol:

Definition 4.2. Let p be a place of $\mathbb{Q}$. For $a, b \in \mathbb{Q}_p^\times$ we define the *quadratic Hilbert symbol* as follows:

$$(a,b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a nonzero solution } (x,y,z) \in \mathbb{Q}_p^3, \\ -1 & \text{otherwise.} \end{cases}$$

For example, for $p = \infty$, $(a,b)_\infty = 1$ unless both a, b are negative – if, say, $a > 0$, then $(1, 0, \sqrt{a})$ is a real solution. The following proposition shows in what way this is a generalization of the Legendre symbol.

Proposition 4.3. *Let p, q be distinct odd primes and r a place of $\mathbb{Q}$. Then*

$$(p,q)_r = \begin{cases} \left(\frac{p}{q}\right) & \text{for } r = q, \\ \left(\frac{q}{p}\right) & \text{for } r = p, \\ (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} & \text{for } r = 2, \\ 1 & \text{for all other } r. \end{cases}$$

Proof (sketch). For $r = \infty$, it follows from the previous observation. Suppose r is finite and there is a solution, so that $(p,q)_r = 1$. Scaling the solution, we may assume x, y, z is in $\mathbb{Z}_r$ and not all of them are divisible by r. For $r = q$, modulo q we get $py^2 \equiv z^2 \pmod{q}$, which implies $\left(\frac{p}{q}\right) = 1$. Similarly, for $r = p$, $\left(\frac{q}{p}\right) = 1$. For $r = 2$, we reduce modulo 8 to find that at most one of p, q is congruent to 3 (mod 4), so $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$. All the converses follow from Hensel's lemma. □

This symbol satisfies the *Hilbert reciprocity law* (or *Hilbert product formula*):

Theorem 4.4. *For $a, b \in \mathbb{Q}^\times$,*

$$\prod_p (a,b)_p = 1,$$

the product being over all places p.

Taking $a = p, b = q$ we immediately get quadratic reciprocity by the previous proposition. Taking $b = 2$ or $b = -1$ we can similarly get the supplementary laws (which we didn't discuss). Unfortunately, there isn't a straightforward way to prove Hilbert reciprocity which would give us quadratic reciprocity; instead, we prove them the other way around.

We now wish to extend the Hilbert symbol to higher powers, similarly to how we have extended the Legendre and Jacobi symbols to the power residue symbol. For that we first look at some properties of the quadratic Hilbert symbol. It can be shown that for any place p the Hilbert symbol $(a,b)_p$ is symmetric and bimultiplicative as a function $\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \to \langle -1 \rangle = \{-1, 1\}$. Hensel's lemma implies the symbol is a continuous map. Moreover, it's nearly immediate from the definition that $(a,b)_p = 1$ if and only if b can be expressed as the norm of some element in the quadratic extension $\mathbb{Q}_p(\sqrt{a})$ (for this reason, this is called the *norm residue symbol* or *norm symbol*; one has to be careful defining this norm if a is a square) – note that the norm of $z + \sqrt{a}x$ is $z^2 - ax^2$, so if b is of this form we have a solution $ax^2 + by^2 = z^2$ with $y = 1$; conversely, we can divide by y to get an element of norm b from a solution.

We take those properties as kind of an axiomatic description of what the general Hilbert symbol should be. Let K be any number field which contains ζ_n. For any place P of K we wish to define a *Hilbert symbol* $(a,b)_P$ for $a, b \in K_P^\times$ taking values in $\langle \zeta_n \rangle$, the group of n-th roots of unity, which will have properties analogous to the ones above: it should be continuous, antisymmetric and bimultiplicative (why not symmetric? This can be seen from the explicit definition below, but note that in the case $n = 2$ "symmetric" and "antisymmetric" are the same thing, since both 1 and -1 are their own inverses). Next, we want the symbol to satisfy the norm condition: $(a,b)_P = 1$ if and only if b is a norm of an element in $K_P(\sqrt[n]{a})$.

The norm condition determines the symbol uniquely for infinite primes – we have seen this for $n = 2$, while for $n > 2$ there are no real primes and in $\mathbb{C}$ everything is a norm. The conditions don't determine $(a,b)_p$ for finite primes p though. However, there is a simple way to normalize this due to Hasse which involves power residue symbols:

Definition 4.5. For $P \nmid n\infty$, define the *n-th Hilbert symbol at P* by the formula

$$(a,b)_P = \pm\left(\frac{a^{-v_P(b)}b^{v_P(a)}}{P}\right)_n,$$

where the $\pm$ sign is $+$ unless n is even and $v_P(a), v_P(b)$ are both odd, and $\left(\frac{\alpha}{P}\right)_n$ is the n-th power residue symbol, defined just as in the case of $\mathbb{Q}(\zeta_n)$ (observe the numerator has P-adic order zero).

This definition satisfies all the properties we have asked for, but it tells us nothing about how to define $(a,b)_P$ for $P \mid n$. Giving an explicit definition turns out to be difficult. We shall be content with an existence statement, which gives a more general form of Hilbert reciprocity:

Theorem 4.6. *There is a unique way of choosing continuous, antisymmetric, bimultiplicative maps $(a,b)_Q : K_Q^\times \times K_Q^\times \to \langle\zeta_n\rangle$ for $Q \mid n$ which has the norm property and for which the product formula holds:*

$$\prod_P (a,b)_P = 1$$

for all $a, b \in K^\times$. Here the product ranges over all places of K.

Now suppose a, b are relatively prime to each other and to n. Then, from Hasse's definition it's not hard to compute the product over $P \nmid n\infty$:

$$\prod_{P\nmid n\infty}(a,b)_P = \pm\prod_{P\nmid n\infty}\left(\frac{a^{v_P(b)}b^{-v_P(a)}}{P}\right)_n = \pm\prod_{P\nmid n\infty}\left(\frac{a}{P}\right)_n^{-v_P(b)}\prod_{P\nmid n\infty}\left(\frac{b}{P}\right)_n^{v_P(a)} = \pm\left(\frac{a}{b}\right)_n^{-1}\left(\frac{b}{a}\right)_n,$$

and the $\pm$ sign can be further computed to be $+$. Plugging this into the product formula, we find the long-sought *power reciprocity law*:

Theorem 4.7. *For $\alpha, \beta \in \mathcal{O}_K$ relatively prime and relatively prime to n we have*

$$\left(\frac{\alpha}{\beta}\right)_n = \left(\frac{\beta}{\alpha}\right)_n \prod_{P\mid n\infty}(\alpha,\beta)_P.$$

Under appropriate assumptions on α, β, namely primarity, all the Hilbert symbols on the right take value 1, which means we have a perfectly symmetric reciprocity law similar to Eisenstein reciprocity. Just like in the quadratic case, the product formula for Hilbert symbols also encompasses all the supplementary laws we might wish for, but to express those we need to use the symbols for $P \mid n$ which are much harder to understand.

Naively, now that we have a satisfying reciprocity laws for all powers, one might think there isn't too much room to generalize. This turns out to be wrong – for once, recall that another way of viewing reciprocity is as studying how primes factor in field extensions. We can do that for a wider class of fields, *abelian extensions*, but for that we again have to take a more general approach.

5 Hasse Reciprocity

Hasse's idea begins with an observation due to Kummer that, assuming K contains all n-th roots of unity, if $b \in K$ is not a d-th power for any $d > 1$ dividing n, then $L = K(\sqrt[n]{b})$ is Galois over K

with the Galois group canonically isomorphic to $\langle\zeta_n\rangle$. Indeed, the conjugates of $\sqrt[n]{b}$ are precisely $\zeta_n^k\sqrt[n]{b}, k = 0, \ldots, n-1$, so the homomorphism $\chi_b : \sigma \mapsto \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$ is well-defined and turns out to be an isomorphism.

The Hilbert symbol has a particularly simple definition in this context for finite primes $P \nmid n$. Assume for a moment $P \nmid b$ as well. Then, by general theory we will briefly recall below, we have a unique *Frobenius automorphism* σ_P such that, for any prime P' of L lying above P, we have

$$\sigma_P(\alpha) \equiv \alpha^{NP} \pmod{P'}$$

for all $\alpha \in \mathcal{O}_K$, where NP is the norm of P. In particular, for $\alpha = \sqrt[n]{b}$ this gives

$$\chi_b(\sigma_P) = \frac{\sigma_P(\sqrt[n]{b})}{\sqrt[n]{b}} \equiv (\sqrt[n]{b})^{NP-1} = b^{\frac{NP-1}{n}} \equiv \left(\frac{b}{P}\right)_n \pmod{P},$$

by the definition of the power residue symbol. The reasoning can be also applied in K_P and we can deduce that for $a, b \in K_P^\times$ we have

$$(a, b)_P = \chi_b(\sigma_P)^{v_P(a)},$$

where σ_P denotes the Frobenius of P in $K(\sqrt[n]{b})$.

This led Hasse to define a new norm symbol, this time with values in a Galois group. Before we define it, we ought to recall some general facts.

Definition 5.1. Let L/K be a Galois extension and P a finite prime of K. Then P can be written as a product of primes $(P_1 \ldots P_g)^e$ for distinct primes P_i of L. We say $P_1, \ldots, P_g$ *lie over* P. If $e = 1$, we say P is *unramified* in L, otherwise it's *ramified*.

Proposition 5.2. *For any P' lying over P there is an automorphism $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) \equiv \alpha^{NP'} \pmod{P}$ for all $\alpha \in \mathcal{O}_K$. If P is unramified, this automorphism is unique and is denoted by $\sigma_{P'}$. If Q is another prime of L lying over P, then there is some $\sigma \in \mathrm{Gal}(L/K)$ such that $Q = \sigma P'$ and then $\sigma_Q = \sigma\sigma_{P'}\sigma^{-1}$.*

In particular, Frobenius automorphisms over an unramified P are all conjugate, and if we assume L/K is an abelian extension, they are all equal.

Definition 5.3. Suppose L/K is abelian and a finite prime P of K is unramified in L. We define the *Frobenius of P* to be $\sigma_{P'}$ for any P' lying above P and denote it by $\left(\frac{L/K}{P}\right)$. Further, for $a \in K_P^\times$, we define the *Hasse's norm symbol* to be

$$\left(\frac{a, L/K}{P}\right) = \left(\frac{L/K}{P}\right)^{v_P(a)}.$$

The above discussion implies, under the identification of $\mathrm{Gal}(K(\sqrt[n]{b})/K)$ with roots of unity, that $\left(\frac{a, K(\sqrt[n]{b})/K}{P}\right) = (a, b)_P$.

This is a good moment to pause and ask: abstractly, why do we care about the Frobenius? It turns out that it determines factorization of primes in the extension: indeed, the order of the Frobenius is equal to the degree of the residue fields extension, and the number of Frobenius automorphisms is equal to the ramification degree e. Those two numbers determine the shape of the prime factorization completely. If we have a polynomial whose root generates a Galois extension, then general facts from algebraic number theory imply that we can describe factorization of this polynomial modulo various primes.

The map $K_P^\times \to \mathrm{Gal}(L/K)$ is a continuous homomorphism and, because P is unramified in L, hence the extension $L_{P'}/K_P$ is unramified, it is not hard to show that $\left(\frac{a, L/K}{P}\right)$ is trivial if and only if $a \in K_P^\times$ is a norm of an element of $L_{P'}^\times$, generalizing a defining property of the Hilbert symbol.

Finally, we have the *Hasse reciprocity law*, which is similar to Hilbert reciprocity and, unfortunately, similarly existential in nature:

Theorem 5.4. *There is a unique way of choosing continuous homomorphisms $\left(\frac{a,L/K}{Q}\right)$ from $K_Q^\times$ to $\mathrm{Gal}(L/K)$ for infinite and ramified primes Q which has the norm property as above and for which the product formula holds:*

$$\prod_P \left(\frac{a, L/K}{P}\right) = 1$$

for all $a \in K^\times$. Again the product ranges over all places of K.

6 Artin Reciprocity

In the previous sections we have arrived at a conclusion that it's possible to describe reciprocity in terms of elements of Galois groups. A rather natural question at this point is: to what extent can we describe the Galois group itself using the symbols?

Fix, throughout this section, an abelian extension L/K. For the clarity of exposition, in what follows we will ignore the infinite primes.

Definition 6.1. Let $\mathfrak{c}$ be any ideal in $\mathcal{O}_K$. By $I_K^{\mathfrak{c}}$ we denote the group of fractional ideals generated by primes not dividing $\mathfrak{c}$. Define $I_L^{\mathfrak{c}}$ similarly.

We let $K_{1,\mathfrak{c}}$ be the set of elements of K which are (quotients of elements) congruent to 1 (mod $\mathfrak{c}$).

For $\mathfrak{c}$ divisible by all primes ramifying in L we extend the symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ to the *Artin symbol* defined on $I_K^{\mathfrak{c}}$ as follows: for $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$ let

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{k} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}.$$

Hence we have a homomorphism from a group of fractional ideals to the Galois group. Naturally, we ask about kernel and image of this map. The former turns out to be easy to find:

Proposition 6.2. *For any $\mathfrak{c}$ divisible by all ramifying primes, the Artin map $I_K^{\mathfrak{c}} \to \mathrm{Gal}(L/K)$ is surjective.*

The proof is not particularly difficult, but still requires some theory. Determining the kernel is much harder and is precisely the content of *Artin reciprocity law*:

Theorem 6.3. *There is an ideal $\mathfrak{f}$ dividing the discriminant $\Delta_{L/K}$, called the* Artin conductor of L/K, *such that the kernel of the Artin map $I_K^{\mathfrak{f}} \to \mathrm{Gal}(L/K)$ is precisely $i(K_{1,\mathfrak{f}}) \cdot N(I_L^{\mathfrak{f}})$, where the first factor is the group of fractional ideals generated by elements of $K_{1,\mathfrak{f}}$, and the second factor is the group of norms of ideals in $I_L^{\mathfrak{f}}$.*

Given the properties of all the other reciprocity symbols, it is not surprising that norms from L land in the kernel and they (at least partially) generate it. The other factor is much more surprising – it tells us that the Artin symbol, at least when restricted to (principal ideals generated by the elements of) $\mathcal{O}_K$ is entirely determined by congruence conditions! We'll illustrate the power of this result by proving quadratic reciprocity from it.

Pick two distinct odd primes p, q. Let $q^* = \pm q$, with the sign chosen so that q^* is congruent to 1 (mod 4). Look at the extension L/K with $L = \mathbb{Q}(\sqrt{q^*}), K = \mathbb{Q}$. As we have noted in proposition 1.3, the quadratic character of q^* modulo p depends on whether (p) factors in L, that is, whether the Frobenius $\left(\frac{L/K}{p}\right)$ is trivial. By Artin reciprocity, Frobenius is determined by the value of p modulo $\mathfrak{f}$ for $\mathfrak{f}$ dividing the discriminant, which is equal to q^* (this uses $q^* \equiv 1 \pmod 4$). Since the Artin map maps onto a group of order two, its kernel, viewed modulo q^*, has index 2, so is necessarily the subgroup of squares modulo q. Therefore $\left(\frac{L/K}{p}\right) = 1$ if and only if p is a square modulo q, which gives $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$, a statement equivalent to quadratic reciprocity!

In almost exactly the same way we can prove cubic reciprocity – the only subtle point is computing the discriminant of a primary element. A bit more complicated is deduction of Eisenstein reciprocity from it, but it follows the same general idea. It doesn't stop there though: Artin reciprocity can be used to define the Hilbert and Hasse symbols – we define the latter: for $\mathfrak{p}$ ramifying in L and $\alpha \in K$, take $\alpha' \in K$ which is close to α in $\mathfrak{p}$-adic norm, but close to 1 in $\mathfrak{q}$-adic norm for every $\mathfrak{q} \neq \mathfrak{p}$ ramifying in L (with "close to" quantified by the exponent of $\mathfrak{p}, \mathfrak{q}$ in $\mathfrak{f}$). Writing $(\alpha') = \mathfrak{p}^e\mathfrak{a}'$, we set

$$\left(\frac{\alpha, L/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{a}'}\right).$$

It's not hard to deduce from Artin reciprocity this value doesn't depend on the choice of α'. Having defined the symbols we could also deduce full reciprocity laws, but we will omit this.

We shall discuss one more consequence to motivate the last section. Consider any homomorphism $\rho : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ (a *character* of $\mathrm{Gal}(L/K)$). Via the Artin map, we can view it as a homomorphism $\chi : I_K^{\mathfrak{f}} \to \mathbb{C}^\times$ which by Artin reciprocity factors through $K_{1,\mathfrak{f}}$. Such characters are called *Hecke characters* modulo $\mathfrak{f}$ and they generalize Dirichlet characters to arbitrary number fields. Therefore we find that every character of the Galois group comes from a Hecke character.

Observe that this is even true for non-abelian extensions M/K, since any character of $\mathrm{Gal}(M/K)$ has abelian image, so factors to the abelianization, which is $\mathrm{Gal}(L/K)$ for L/K the maximal abelian subextension of M/K.

7 Langlands Reciprocity

In here, L/K is any finite Galois extension. We make the connection more apparent by introducing *L-functions*.

Definition 7.1. Let $\mathfrak{c}$ be an integral ideal and $\chi : I_K^{\mathfrak{c}} \to \mathbb{C}^\times$ be a Hecke character modulo $\mathfrak{c}$, i.e. it factors through $K_{1,\mathfrak{c}}$. We define the *Hecke L-function* of χ to be the function on some complex halfplane given by the following two equivalent definitions:

$$L(\chi, s) = \sum_{(I,\mathfrak{c})=1} \frac{\chi(I)}{(NI)^s} = \prod_{(\mathfrak{p},\mathfrak{c})=1} \left(1 - \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s}\right)^{-1},$$

where the sum and product are over all (respectively, all the prime) ideals relatively prime to $\mathfrak{c}$.

Now let ρ be any *n-dimensional representation* of $\mathrm{Gal}(L/K)$, i.e. a homomorphism into $\mathrm{GL}_n(\mathbb{C})$. For any prime $\mathfrak{p}$ of K unramified in L consider the Frobenius automorphisms of primes lying above $\mathfrak{p}$. By proposition 5.2 they are all conjugate in $\mathrm{Gal}(L/K)$, hence so are their images under ρ. In particular, we get the same characteristic polynomial $P_\mathfrak{p}(t) = \det(1 - t\rho(\sigma_\mathfrak{p}))$ for any Frobenius $\sigma_\mathfrak{p}$ of a prime above $\mathfrak{p}$. It is possible to similarly define $P_\mathfrak{p}$ for $\mathfrak{p}$ ramified. Now we can define the *Artin L-function* of ρ:

$$L(\rho, s) = \prod_\mathfrak{p} P_\mathfrak{p}\left((N\mathfrak{p})^{-s}\right)^{-1}.$$

What happens in the 1-dimensional case? Then ρ is just a character from $\mathrm{Gal}(L/K)$ to $\mathbb{C}^\times$. For $\mathfrak{p}$ unramified the characteristic polynomial is $1 - t\rho(\sigma_\mathfrak{p})$, while for ramified ones it works out to be 1, so the L-function is

$$L(\rho, s) = \prod_\mathfrak{p} \left(1 - \frac{\rho(\sigma_\mathfrak{p})}{(N\mathfrak{p})^s}\right)^{-1}.$$

By the discussion at the end of previous section, this L-function coincides with a Hecke L-function. Therefore the Artin reciprocity law can be concisely summarized by saying that Artin L-functions of one-dimensional representations are Hecke L-functions.

The question now is: can anything of this sort be done with higher-dimensional representations? The answer is, conjecturally, "yes". This is one of the founding blocks of the *Langlands program*. Langlands has defined so-called *automorphic cuspidial representations* which, while infinite-dimensional, are more or less well-understood, and to which we can attach *automorphic L-functions*. The *Langlands reciprocity* conjecture then states

Conjecture 7.2. *Every Artin L-function of an irreducible, finite-dimensional representation of* $\mathrm{Gal}(L/K)$ *coincides with an automorphic L-function.*

One consequence of this would be that Artin L-functions can be extended to entire functions, since this is known to hold for automorphic L-functions, which is still not known unconditionally.

The one-dimensional Langlands conjectures are, essentially, equivalent to the entirety of class field theory, so the above conjecture can be seen as a description of non-abelian class field theory.