QUADRATIC RECIPROCITY VIA QUADRATIC AND CYCLOTOMIC FIELDS

TUSHAR MURALIDHARAN

October 27, 2023

Abstract. We find the Frobenius maps for quadratic and cyclotomic fields, and obtain a surprisingly simple proof of the quadratic reciprocity law. We introduce the Frobenius automorphism and its role in the context of Galois extensions, enabling us to prove the equivalence between the Legendre symbol, the behavior of prime splitting in a quadratic field, and the Frobenius automorphism.

1. Introduction

We say that a is a *quadratic residue modulo* n if a is congruent to a perfect square modulo n; that is, if $x^2 \equiv a \bmod n$ for some integer x.

Definition 1. Let p be an odd prime. For any integer a, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

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

The quadratic reciprocity law is the following statement.

Theorem 1 (Quadratic Reciprocity Law)**.** *Let p and q be distinct odd primes. Then*

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

Ireland and Rosen, in their renowned text *A Classical Introduction to Modern Number Theory*, view the quadratic reciprocity law as "among the deepest and most beautiful results of elementary number theory and the beginning of a line of reciprocity theorems that culminate in the very general Artin reciprocity law, perhaps the most impressive theorem in all number theory."

The quadratic reciprocity law exhibits a surprising relationship between the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$; if we know whether p is a quadratic residue modulo q, then we can deduce whether q is a quadratic residue modulo p. The law can be stated in words in a seemingly different form:

> If p and q are distinct odd primes, at least one of which is congruent to 1 modulo 4, then p is a quadratic residue modulo q if and only if q is a quadratic residue modulo p; otherwise exactly one of p and q is a quadratic residue modulo the other.

To see that this is the same statement, note that $\frac{p-1}{2}\cdot\frac{q-1}{2}$ is odd if both $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd, and even otherwise. In the former case, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ and hence, exactly one of p and q is a quadratic residue modulo the other. Since an integer of the form $\frac{n-1}{2}$ is odd if and only if n is congruent to 3 modulo 4, this case occurs precisely when both p and q are congruent to 3 modulo 4. In the latter case, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ and hence, both or neither of p and q is a quadratic residue modulo the other. Since an integer

of the form $\frac{n-1}{2}$ is even if and only if n is congruent to 1 modulo 4, this case occurs when at least one of p and q are congruent to 1 modulo 4.

To prove the quadratic reciprocity law, we follow the proof of David Hilbert, given in his seminal work titled *Theory of Algebraic Number Fields* in 1896. We use yet another an equivalent formulation of the statement. For an odd prime p, define

$$p^* = (-1)^{\frac{p-1}{2}} p.$$

We claim that the quadratic reciprocity law is equivalent to the equation

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right). \tag{1}$$

The Legendre symbol can be shown to be multiplicative, so we have $\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$. Since $q-1$ is even, we have that -1 is a square modulo q if and only if 4 divides $q-1$. That is, we have $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$. Therefore, we have shown $\left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)$. Multiplying both sides by $\left(\frac{p}{q}\right)$ then yields the equivalence. We will prove the quadratic reciprocity law in this equivalent form.

2. Cyclotomic Fields

We come to the setting for our upcoming proof.

Definition 2. Let ζ_n be a primitive n-th root of unity. Then the *n-th cyclotomic field* is $\mathbb{Q}(\zeta_n)$.

Let $L = \mathbb{Q}(\zeta_p)$, where p is an odd prime. Later, we will choose an arbitrary distinct odd prime and denote it as q as in the quadratic reciprocity law. We have the following characterization of the Galois group of $L/\mathbb{Q}$.

Theorem 2. *There is an isomorphism*

$$\mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$$

which sends the automorphism σ_a satisfying $\sigma_a(\zeta_p) = \zeta_p^a$ to the residue a mod p.

Proof. First, we verify that the map is indeed a homomorphism. Every automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ is of the form σ_a for some $a \in \{1, \ldots, p\}$. For automorphisms σ_a and σ_b in $\mathrm{Gal}(L/\mathbb{Q})$, we have

$$(\sigma_a\sigma_b)(\zeta_p) = \sigma_a(\sigma_b(\zeta_p)) = \sigma_a(\zeta_p^b) = \sigma_a(\zeta_p)^b = (\zeta_p^a)^b = \zeta_p^{ab}.$$

Thus, the automorphism $\sigma_a\sigma_b$ is sent to ab mod p. Since σ_a and σ_b are sent to a mod p and b mod p, this shows that the map is a homomorphism.

For injectivity, suppose that σ_a is sent to some $a \equiv 1 \bmod p$. Then $\zeta_p^a = \zeta_p$, so σ_a must be the identity automorphism.

Lastly, every residue a mod p is the image of the automorphism σ_a in $\mathrm{Gal}(L/\mathbb{Q})$. Thus, the map is surjective.

Hence, the map is an isomorphism. □

It is a standard fact that $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$. Theorem 2 shows that G is a cyclic group of order $p-1$. Let H be the subgroup of square elements in G. Since G is a cyclic group of even order, this is the unique subgroup of order $(p-1)/2$. By the Fundamental Theorem of Galois Theory, the subgroup H of G corresponds to a *unique quadratic extension* K of $\mathbb{Q}$ contained in L (see Figure 1). Hence, we can write $K = \mathbb{Q}(\sqrt{p^*})$ for some squarefree integer d.

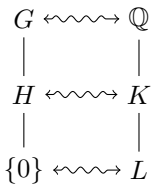

FIGURE 1. Correspondence between subgroups and subfields

To identify K, we employ the tools of algebraic number theory. The following theorem given in [1] exhibits an equivalent condition for the ramification of a prime in terms of the discriminant of a number field.

Theorem 3. *A prime p ramifies in a number field K if and only if p divides the discriminant Δ_K.*

It is a standard fact (see 4.12 in [1]) that $\Delta_L = (-1)^{(p-1)/2}p^{p-2}$, so Theorem 3 implies that p is the only prime that ramifies in L. Then p too is the only prime that can possibly ramify in $K \subset L$. Then Theorem 3 again implies that the only prime possibly dividing Δ_K is p. What is Δ_K?

3. Quadratic Fields

The following two results serve to characterize discriminants of quadratic fields.

Theorem 4. *Let $d \neq 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$ the corresponding quadratic field. Then we have*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Theorem 5. *For a squarefree integer $d \neq 1$, the corresponding quadratic field $K = \mathbb{Q}(\sqrt{d})$ has discriminant*

$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

It follows from Theorem 5 that $d \equiv 2$ or $3 \bmod 4$ is impossible, since Theorem 3 would imply that 2 ramifies in K. Therefore, we know that $d \equiv 1 \bmod 4$. Since at least one prime divides d, and p is the only prime possibly dividing d, we know that p divides d. Thus, since d is squarefree, the only possible values of d are p or $-p$. To ensure $d \equiv 1 \bmod 4$, we can only have one or the other depending on the residue of p modulo 4:

$$d = \begin{cases} p & \text{if } p \equiv 1 \pmod 4 \\ -p & \text{if } p \equiv 3 \pmod 4. \end{cases} = (-1)^{\frac{p-1}{2}}p = p^*$$

Then the unique quadratic subfield of L is $K = \mathbb{Q}(\sqrt{p^*})$.

Now let q be an odd prime distinct from p. No primes other than p are ramified in K, so q must be either split or inert. We have the following result regarding quadratic fields from [1].

Theorem 6. *Let $d \neq 1$ be squarefree and p an odd prime. Then p is split in $\mathbb{Q}(\sqrt{d})$ for $\left(\frac{d}{p}\right) = 1$, inert for $\left(\frac{d}{p}\right) = -1$, and ramified for $\left(\frac{d}{p}\right) = 0$.*

Now we come to the crux of the proof.

Theorem 7. *The following are equivalent:*

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

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

Proof. Let σ_q be the automorphism in $G = \mathrm{Gal}(L/\mathbb{Q})$ corresponding to q via Theorem 2. Let σ_q' be the restriction of σ_q on K. Then σ_q' is the automorphism in $\mathrm{Gal}(K/\mathbb{Q})$ corresponding to q. We see in Chapter 8 of [1] (involving additional definitions) that σ_q' is the identity automorphism in $\mathrm{Gal}(K/\mathbb{Q})$ if and only if q splits in K. Note that σ_q' is the identity in $\mathrm{Gal}(K/\mathbb{Q})$ if and only if σ_q' fixes K, i.e., σ_q' is in $\mathrm{Gal}(L/K)$. By Theorem 6, we have that (1) is equivalent to the statement that q is split in K. Therefore, we have that (1) is equivalent to the statement that σ_q' is in $\mathrm{Gal}(L/K)$.

Observe from Figure 1 that H corresponds to $\mathrm{Gal}(L/K)$. Recall that H was defined to be the unique subgroup of square elements of G. By the isomorphism $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$ in Theorem 2, we may identify H with the (nonzero) quadratic residues in $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore, we have that σ_q' is in $\mathrm{Gal}(L/K)$ if and only if q is a quadratic residue in $(\mathbb{Z}/p\mathbb{Z})^\times$. This is exactly (2), so the proof is complete. □

This proves the quadratic reciprocity law in the form of Equation 1.

4. Conclusion

The crucial result in the proof was Theorem 7. This theorem was able to relate the two Legendre symbols $\left(\frac{p^*}{q}\right)$ and $\left(\frac{q}{p}\right)$ because the two symbols encoded information about the order of the automorphism σ_q. This allowed for a beautiful, simplistic proof of the celebrated result of Gauss.

The quadratic reciprocity law is sometimes accompanied by the supplementary result

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 5 \bmod 8. \end{cases}.$$

Instead of looking at quadratic residues, there are also reciprocity laws for higher powers. Generalizing these methods to larger number fields is an illuminating task warranting further study.

References

[1] P. Stevenhagen (2019) *Number Rings*, Universiteit Leiden.