A Proof of Quadratic Reciprocity by Galois Theory

Jack Westbrook
Instructor: Prof. Ana Caraiani

October 21, 2025

Let p, q be distinct, odd rational primes. Then

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

In addition,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \mod 8 \\ -1, & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$$

and

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

Proof. We let ζ_p denote a primitive p-th root of unity over $\mathbb{Q}$. We assume these basic results from algebraic number theory: $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, and if d is a squarefree integer then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\alpha]$ where $\alpha = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2,3 \mod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \mod 4 \end{cases}$ and $\Delta(\mathbb{Q}(\sqrt{d})) = \begin{cases} d, & \text{if } d \equiv 1 \mod 4 \\ 4d, & \text{if } d \equiv 2,3, \mod 4 \end{cases}$.

Lemma 0.1. For any group G,

$$\#\operatorname{Hom}(G, \mathbb{Z}/2\mathbb{Z}) = \#\{H \leq G \mid [G : H] = 2\} + 1.$$

Proof. If $\phi : G \to \mathbb{Z}/2\mathbb{Z}$ is a nontrivial group homomorphism, then $\ker \phi$ is an index 2 subgroup of G. Moreover, if ψ is another such homomorphism, then there is a homomorphism $\phi + \psi$ given by $(\phi + \psi)(x) = \phi(x) + \psi(x)$. Now if $\ker \phi = \ker \psi$, then $\phi + \psi = 0$. To see this, divide into cases based on whether or not an arbitrary $x \in G$ is in $\ker \phi$. As a consequence, $\phi + \phi = 0$. Then

$$\phi = (\phi + \psi) + \phi = (\phi + \phi) + \psi = \psi.$$

Therefore the set of nonzero homomorphisms injects into the set of index 2 subgroups. In addition, since every index 2 subgroup is normal, every index 2 subgroup is the kernel of a homomorphism $G \to \mathbb{Z}/2\mathbb{Z}$. Thus the set of nonzero homomorphisms is in bijection with the set of index 2 subgroups, giving the result. ∎

Lemma 0.2. The unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{\hat{p}})$ where $\hat{p} := (-1)^{\frac{p-1}{2}}p$.

Proof. We see that $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield $\mathbb{Q}(\sqrt{d})$ (for some $d \in \mathbb{Z}$ squarefree) because there is a unique subgroup of order 2 in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. More is true; because p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$ by Proposition 6.2 in [1], it follows that p is the only prime that ramifies in $\mathbb{Q}(\sqrt{d})$ as well, so the discriminant must be a power of p (positive or negative). However, the discriminant of $\mathbb{Q}(\sqrt{d})$ is d if $d \equiv 1 \mod 4$ and is $4d$ otherwise. From this it follows that $d \equiv 1 \mod 4$ and that $d = \pm p$. In particular, the quadratic subfield of $\mathbb{Q}(\zeta_p)$ is

$$\begin{cases} \mathbb{Q}(\sqrt{p}), & \text{if } p \equiv 1 \mod 4 \\ \mathbb{Q}(\sqrt{-p}), & \text{if } p \equiv 3 \mod 4 \end{cases} = \mathbb{Q}(\hat{p}).$$

■

First, we prove the easy result that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. One way to do this is by considering the field $\mathbb{F}_p$, and an algebraically closed field Ω containing $\mathbb{F}_p$. We notice that

$$\mathbb{F}_p = \{x \in \Omega \mid x^p = x\}$$

since the containment $\subset$ is clear, and both are sets of size p, so they must be equal. From this we deduce

$$\mathbb{F}_p^\times = \{x \in \Omega \mid x^{p-1} = 1\}.$$

Now let $x \in \mathbb{F}_p^\times$ be arbitrary, and $y \in \Omega$ such that $y^2 = x$. We see that $\left(\frac{x}{p}\right) = 1$ iff $y \in \mathbb{F}_p$ iff $y^{p-1} = 1$. Since $y^{p-1} = x^{\frac{p-1}{2}} \in \{\pm 1\}$, we get the exact sequence of groups

$$1 \to (\mathbb{F}_p^\times)^2 \to \mathbb{F}_p^\times \xrightarrow{x \mapsto x^{\frac{p-1}{2}}} \{\pm 1\} \to 1.$$

Thus we deduce more generally that for any $x \in \mathbb{F}_p^\times$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ (identifying $\{\pm 1\}$ with the copy embedded in $\mathbb{F}_p$).

Now to the problem of reciprocity. From Lemma 0.2, we have a nontrivial map res : $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{\hat{p}})/\mathbb{Q})$ (nontrivial since $\mathbb{Q}(\zeta_p)$ is not a quadratic extension), a map $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, and isomorphisms $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{\hat{p}})/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}$. Because each composite is nontrivial, Lemma 0.1, combined with the fact that for every cyclic group of order n and $d \mid n$ has a unique subgroup of order d, gives that the below diagram of groups commutes:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \xrightarrow{\text{res}} & \mathrm{Gal}(\mathbb{Q}(\sqrt{\hat{p}})/\mathbb{Q}) \\ \downarrow\sim & & \downarrow\sim \\ (\mathbb{Z}/p\mathbb{Z})^\times & \xrightarrow{\left(\frac{\cdot}{p}\right)} & \{\pm 1\}. \end{array}$$

There exists a unique (Frob always exists uniquely up to conjugacy, but since $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is abelian conjugacy classes are the same as elements) element $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that for a (equivalently, any, since $\mathbb{Q}(\zeta_p)$ is abelian) $\mathbb{Q}(\zeta_p)$-prime $\mathfrak{q}$ lying over q, Frob_q acts as $x \mapsto x^q$ on $\mathcal{O}_{\mathbb{Q}(\zeta_p)}/\mathfrak{q}$. In particular, since $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ by Proposition 6.2 in [1], and there exists an automorphism defined by $\zeta_p \mapsto \zeta_p^q$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ which visibly acts as $x \mapsto x^q$ on $\mathbb{Z}[\zeta_p]/\mathfrak{q}$ for any prime $\mathfrak{q} \mid q$, we see that Frob_q is the automorphism given by $\zeta_p \mapsto \zeta_p^q$. The result will follow by tracking Frob_q around both sides of the diagram.

For the top side, since q is unramified in $\mathbb{Q}(\sqrt{\hat{p}})$, it follows that either q splits or is inert. Let $\mathfrak{q}$ be a $\mathbb{Q}(\sqrt{\hat{p}})$-prime lying over q. If q splits, it follows (from $\sum_{\mathfrak{B}|\mathfrak{p}} e_{\mathfrak{B}} f_{\mathfrak{B}} = [L : K]$, i.e., Theorem 3.34 in [1]) that $\mathcal{O}_{\mathbb{Q}(\sqrt{\hat{p}})}/\mathfrak{q} \cong \mathbb{F}_q$, in which case $\mathrm{res}(\mathrm{Frob}_q)$ is indeed trivial on the residue field, hence trivial by uniqueness of Frob_q in $\mathrm{Gal}(\mathbb{Q}(\sqrt{\hat{p}})/\mathbb{Q})$. On the other hand, if q is inert, then $\mathcal{O}_{\mathbb{Q}(\sqrt{\hat{p}})}/\mathfrak{q} \cong \mathbb{F}_{q^2}$, in which case $x \mapsto x^q$ is nontrivial, so $\mathrm{res}(\mathrm{Frob}_q)$ is the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{\hat{p}})/\mathbb{Q})$.

From Theorem 3.41 in [1], q splits if and only if $x^2 - x + \frac{1-\hat{p}}{4}$ (the minimal polynomial of $\frac{1+\sqrt{\hat{p}}}{2}$, where $\mathcal{O}_{\mathbb{Q}(\sqrt{\hat{p}})} = \mathbb{Z}[\frac{1+\sqrt{\hat{p}}}{2}]$) has a root modulo q. Because this polynomial has discriminant $\hat{p}$, this is if and only if $\left(\frac{\hat{p}}{q}\right) = 1$ (any quadratic over a field of characteristic not 2 has a root if and only if its discriminant is a square). Putting these results together, we deduce that $\mathrm{res}(\mathrm{Frob}_q) \mapsto \left(\frac{\hat{p}}{q}\right)$.

For the other map to $\{\pm 1\}$, we see $\mathrm{Frob}_q \mapsto q \mapsto \left(\frac{q}{p}\right)$.

Thus commutativity gives

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

For the last claim, we will track Frob_2, which again is defined by $\zeta_p \mapsto \zeta_p^2$. Like before, 2 is either split or inert in $\mathbb{Q}(\sqrt{\hat{p}})$. From Theorem 3.41 in [1], we know that since $\mathcal{O}_{\mathbb{Q}(\sqrt{\hat{p}})} = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{\hat{p}}}{2}$ with minimal polynomial $f(x) = x^2 - x + \frac{1-\hat{p}}{4}$, then 2 splits if and only if $f(x)$ is irreducible modulo 2. If $\hat{p} \equiv 1 \mod 8$, i.e., $\frac{1-\hat{p}}{4}$ is even,

$$f(x) \equiv x(x+1) \mod 2$$

so 2 splits. If instead $\hat{p} \equiv 5 \mod 8$, i.e., $\frac{1-\hat{p}}{4}$ is odd,

$$f(x) \equiv x^2 + x + 1 \mod 2$$

which is irreducible, so 2 is inert.

We also notice that $\hat{p} \equiv 1 \mod 8$ if and only if $p \equiv \pm 1 \mod 8$, so by the same commutativity argument as before, we get that

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \mod 8$$

which is the desired result. ∎

References

[1] J. S. Milne. *Algebraic Number Theory — Course Notes*. Online: https://www.jmilne.org/math/CourseNotes/ANT.pdf. Accessed: 21 October 2025. 2020.