Quadratic Reciprocity

via Quadratic and Cyclotomic Fields

Tushar Muralidharan

Australian National University

November 2023

Table of Contents

Table of Contents

What is Quadratic Reciprocity?

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

Definition

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

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

What is Quadratic Reciprocity?

Definition

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

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

Theorem (Quadratic Reciprocity Law)

Let p and q be distinct odd primes. Then

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

Why Should We Care?

It is 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.

Ireland and Rosen,
A Classical Introduction to Modern Number Theory

Why Should We Care?

Theorem (Quadratic Reciprocity Law)

Let p and q be distinct odd primes. Then

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

If we know whether p is a quadratic residue modulo q, then we can deduce whether q is a quadratic residue modulo p.

Why Should We Care?

Theorem (Quadratic Reciprocity Law)

Let p and q be distinct odd primes. Then

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

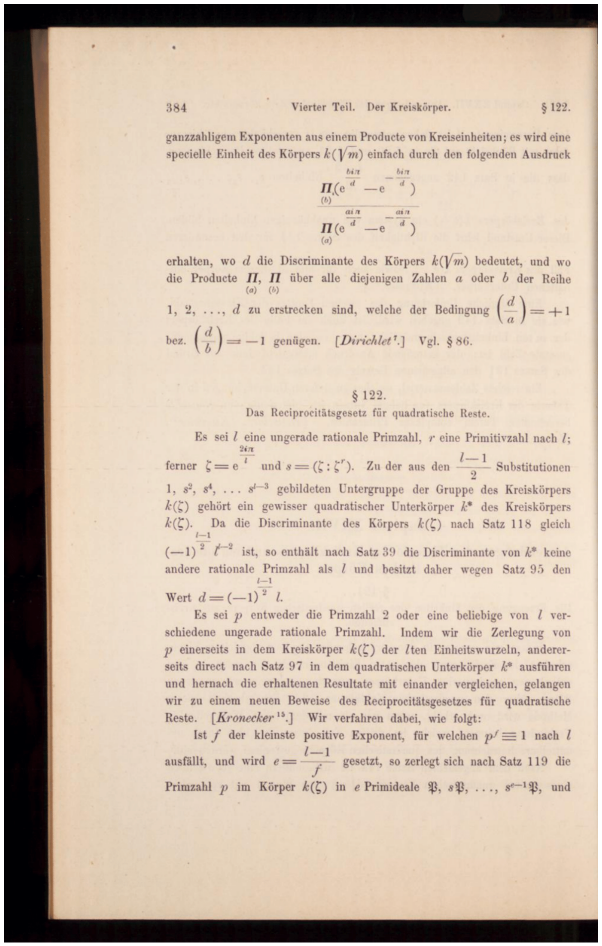
If we know whether p is a quadratic residue modulo q, then we can deduce whether q is a quadratic residue modulo p.

> *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.*

Table of Contents

A Proof

We follow the proof of David Hilbert, given in his seminal work *Theory of Algebraic Number Fields* in 1896.



384 Vierter Teil. Der Kreiskörper. § 122.

ganzzahligem Exponenten aus einem Producte von Kreiseinheiten; es wird eine specielle Einheit des Körpers $k(\sqrt{m})$ einfach durch den folgenden Ausdruck

$$\frac{\prod_{(b)}(e^{\frac{bi\pi}{d}} - e^{-\frac{bi\pi}{d}})}{\prod_{(a)}(e^{\frac{ai\pi}{d}} - e^{-\frac{ai\pi}{d}})}$$

erhalten, wo d die Discriminante des Körpers $k(\sqrt{m})$ bedeutet, und wo die Producte $\prod_{(a)}$, $\prod_{(b)}$ über alle diejenigen Zahlen a oder b der Reihe $1, 2, \ldots, d$ zu erstrecken sind, welche der Bedingung $\left(\frac{d}{a}\right) = +1$ bez. $\left(\frac{d}{b}\right) = -1$ genügen. [*Dirichlet*[7].] Vgl. § 86.

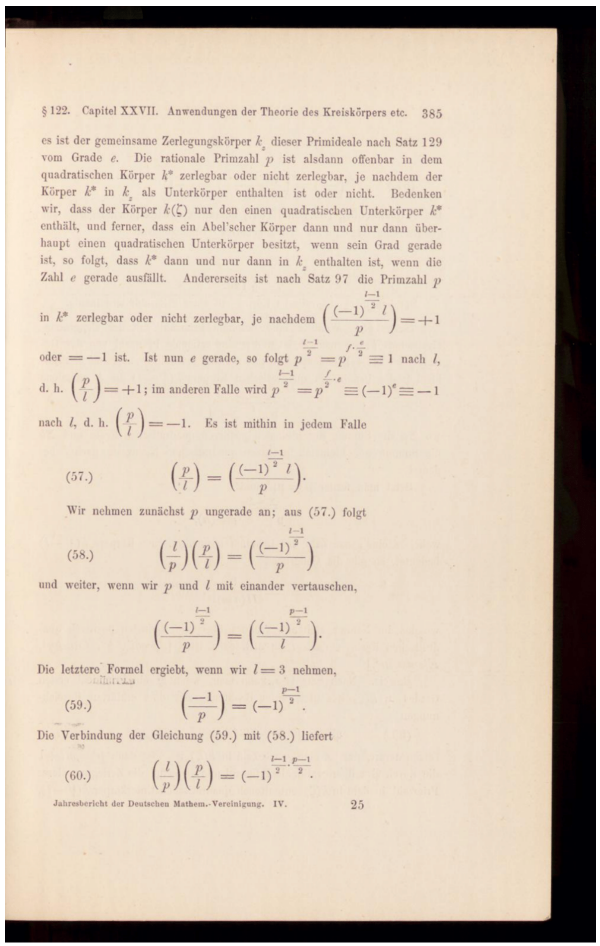
§ 122.

Das Reciprocitätsgesetz für quadratische Reste.

Es sei l eine ungerade rationale Primzahl, r eine Primitivzahl nach l; ferner $\zeta = e^{\frac{2i\pi}{l}}$ und $s = (\zeta ; \zeta^r)$. Zu der aus den $\frac{l-1}{2}$ Substitutionen $1, s^2, s^4, \ldots s^{l-3}$ gebildeten Untergruppe der Gruppe des Kreiskörpers $k(\zeta)$ gehört ein gewisser quadratischer Unterkörper k^* des Kreiskörpers $k(\zeta)$. Da die Discriminante des Körpers $k(\zeta)$ nach Satz 118 gleich $(-1)^{\frac{l-1}{2}} l^{l-2}$ ist, so enthält nach Satz 39 die Discriminante von k^* keine andere rationale Primzahl als l und besitzt daher wegen Satz 95 den Wert $d = (-1)^{\frac{l-1}{2}} l$.

Es sei p entweder die Primzahl 2 oder eine beliebige von l verschiedene ungerade rationale Primzahl. Indem wir die Zerlegung von p einerseits in dem Kreiskörper $k(\zeta)$ der $l$ten Einheitswurzeln, andererseits direct nach Satz 97 in dem quadratischen Unterkörper k^* ausführen und hernach die erhaltenen Resultate mit einander vergleichen, gelangen wir zu einem neuen Beweise des Reciprocitätsgesetzes für quadratische Reste. [*Kronecker*[13].] Wir verfahren dabei, wie folgt:

Ist f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach l ausfällt, und wird $e = \frac{l-1}{f}$ gesetzt, so zerlegt sich nach Satz 119 die Primzahl p im Körper $k(\zeta)$ in e Primideale $\mathfrak{P}, s\mathfrak{P}, \ldots, s^{e-1}\mathfrak{P}$, und



§ 122. Capitel XXVII. Anwendungen der Theorie des Kreiskörpers etc. 385

es ist der gemeinsame Zerlegungskörper k_z dieser Primideale nach Satz 129 vom Grade e. Die rationale Primzahl p ist alsdann offenbar in dem quadratischen Körper k^* zerlegbar oder nicht zerlegbar, je nachdem der Körper k^* in k_z als Unterkörper enthalten ist oder nicht. Bedenken wir, dass der Körper $k(\zeta)$ nur den einen quadratischen Unterkörper k^* enthält, und ferner, dass ein Abel'scher Körper dann und nur dann überhaupt einen quadratischen Unterkörper besitzt, wenn sein Grad gerade ist, so folgt, dass k^* dann und nur dann in k_z enthalten ist, wenn die Zahl e gerade ausfällt. Andererseits ist nach Satz 97 die Primzahl p in k^* zerlegbar oder nicht zerlegbar, je nachdem $\left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right) = +1$ oder $= -1$ ist. Ist nun e gerade, so folgt $p^{\frac{l-1}{2}} = p^{f \cdot \frac{e}{2}} \equiv 1$ nach l, d. h. $\left(\frac{p}{l}\right) = +1$; im anderen Falle wird $p^{\frac{l-1}{2}} = p^{\frac{f}{2} \cdot e} \equiv (-1)^e \equiv -1$ nach l, d. h. $\left(\frac{p}{l}\right) = -1$. Es ist mithin in jedem Falle

$$(57.) \qquad \left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right).$$

Wir nehmen zunächst p ungerade an; aus (57.) folgt

$$(58.) \qquad \left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right)$$

und weiter, wenn wir p und l mit einander vertauschen,

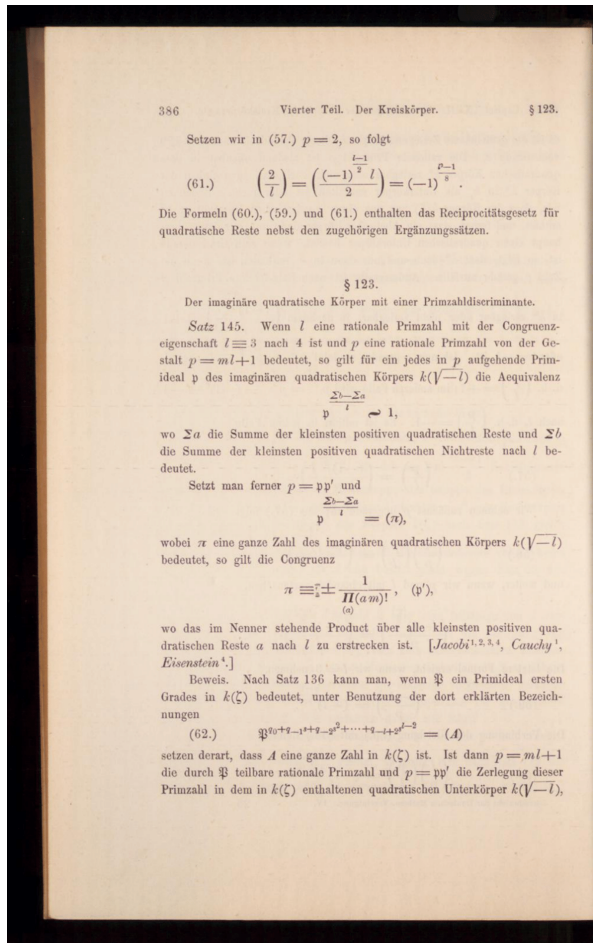
$$\left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{l}\right).$$

Die letztere Formel ergiebt, wenn wir $l = 3$ nehmen,

$$(59.) \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Die Verbindung der Gleichung (59.) mit (58.) liefert

$$(60.) \qquad \left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}}.$$



Setzen wir in (57.) $p = 2$, so folgt

$$(61.) \qquad \left(\frac{2}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{2}\right) = (-1)^{\frac{p-1}{8}}.$$

Die Formeln (60.), (59.) und (61.) enthalten das Reciprocitätsgesetz für quadratische Reste nebst den zugehörigen Ergänzungssätzen.

§ 123.

Der imaginäre quadratische Körper mit einer Primzahldiscriminante.

Satz 145. Wenn l eine rationale Primzahl mit der Congruenzeigenschaft $l \equiv 3$ nach 4 ist und p eine rationale Primzahl von der Gestalt $p = ml + 1$ bedeutet, so gilt für ein jedes in p aufgehende Primideal $\mathfrak{p}$ des imaginären quadratischen Körpers $k(\sqrt{-l})$ die Aequivalenz

$$\mathfrak{p}^{\frac{\Sigma b - \Sigma a}{l}} \sim 1,$$

wo Σa die Summe der kleinsten positiven quadratischen Reste und Σb die Summe der kleinsten positiven quadratischen Nichtreste nach l bedeutet.

Setzt man ferner $p = \mathfrak{p}\mathfrak{p}'$ und

$$\mathfrak{p}^{\frac{\Sigma b - \Sigma a}{l}} = (\pi),$$

wobei π eine ganze Zahl des imaginären quadratischen Körpers $k(\sqrt{-l})$ bedeutet, so gilt die Congruenz

$$\pi \equiv \overline{+}\frac{1}{\prod_{(a)}(am)!}, \quad (\mathfrak{p}'),$$

wo das im Nenner stehende Product über alle kleinsten positiven quadratischen Reste a nach l zu erstrecken ist. [*Jacobi*[1,2,3,4], *Cauchy*[1], *Eisenstein*[4].]

Beweis. Nach Satz 136 kann man, wenn $\mathfrak{P}$ ein Primideal ersten Grades in $k(\zeta)$ bedeutet, unter Benutzung der dort erklärten Bezeichnungen

$$(62.) \qquad \mathfrak{P}^{g_0 + g_{-1} i + g_{-2} i^2 + \cdots + g_{-l+2} i^{l-2}} = (A)$$

setzen derart, dass A eine ganze Zahl in $k(\zeta)$ ist. Ist dann $p = ml + 1$ die durch $\mathfrak{P}$ teilbare rationale Primzahl und $p = \mathfrak{p}\mathfrak{p}'$ die Zerlegung dieser Primzahl in dem in $k(\zeta)$ enthaltenen quadratischen Unterkörper $k(\sqrt{-l})$,

Cyclotomic Fields

Definition

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

Let p be an odd prime. This is where our proof starts. Later on, we'll choose an arbitrary distinct odd prime q.

Cyclotomic Fields

Definition

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

Let p be an odd prime. This is where our proof starts. Later on, we'll choose an arbitrary distinct odd prime q.

Theorem

There is an isomorphism

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

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

Cyclotomic Fields

We have $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$. This a cyclic group of even order, so there exists a unique subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (the square elements) with order $(p-1)/2$. By the Fundamental Theorem of Galois Theory, this corresponds to a unique quadratic extension K of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$.

Cyclotomic Fields

We have $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$. This a cyclic group of even order, so there exists a unique subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (the square elements) with order $(p-1)/2$. By the Fundamental Theorem of Galois Theory, this corresponds to a unique quadratic extension K of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$.

Cyclotomic Fields

We have $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$. This a cyclic group of even order, so there exists a unique subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (the square elements) with order $(p-1)/2$. By the Fundamental Theorem of Galois Theory, this corresponds to a unique quadratic extension K of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$.

$$\begin{array}{c} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \\ | \\ H \\ | \\ \{0\} \end{array} \qquad \begin{array}{c} \mathbb{Q} \\ | \\ K \\ | \\ \mathbb{Q}(\zeta_p) \end{array}$$

We've shown that $\mathbb{Q}(\zeta_p)$ **contains a unique quadratic subfield.** Write $K = \mathbb{Q}(\sqrt{p^*})$ for some squarefree integer p^*.

Cyclotomic Fields

We have the following result from Stevenhagen [1].

Theorem

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

Cyclotomic Fields

We have the following result from Stevenhagen [1].

Theorem

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

We've seen that

$$\Delta_{\mathbb{Q}(\zeta_p)} = \Delta(\Phi_p) = (-1)^{(p-1)/2} N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\Phi_p'(\zeta_p)) = (-1)^{(p-1)/2} p^{p-2},$$

where $\Phi_p(X) = \frac{X^p-1}{X-1} = \sum_{i=0}^{p-1} X^i$. In particular, p is the only prime that divides the discriminant. The theorem tells us that p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$. Then p is the only possible prime that can ramify in $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$. The theorem tells us that $\Delta_{\mathbb{Q}(\sqrt{p^*})}$ **cannot have any prime divisors other than** p. What is $\Delta_{\mathbb{Q}(\sqrt{p^*})}$?

Quadratic Fields

Theorem

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

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

Quadratic Fields

Theorem

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

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

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

Quadratic Fields

Theorem

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

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

Consider our quadratic subfield $K = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$. Recall that $\Delta_{\mathbb{Q}(\sqrt{p^*})}$ cannot have any prime divisors other than p, so we must have $p^* \equiv 1 \bmod 4$.

Quadratic Fields

Theorem

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

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

Consider our quadratic subfield $K = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$. Recall that $\Delta_{\mathbb{Q}(\sqrt{p^*})}$ cannot have any prime divisors other than p, so we must have $p^* \equiv 1 \bmod 4$. Since at least one prime divides p^*, we must have $p \mid p^*$.

Quadratic Fields

Theorem

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

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

Consider our quadratic subfield $K = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$. Recall that $\Delta_{\mathbb{Q}(\sqrt{p^*})}$ cannot have any prime divisors other than p, so we must have $p^* \equiv 1 \mod 4$. Since at least one prime divides p^*, we must have $p \mid p^*$. Then since p^* was assumed to be squarefree, we must have $p^* = \pm p$. Moreover,

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

so we have identified K.

The Next Step

Let q be an odd prime distinct from p. This is the second arbitrary prime in the theorem. No primes other than p are ramified in $\mathbb{Q}(\sqrt{p^*})$, so q must be either split or inert.

We have the following result regarding quadratic fields from Stevenhagen [1].

Theorem

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 $\left(\frac{d}{p}\right) = 0$.

Hence, q splits in $K = \mathbb{Q}(\sqrt{p^*})$ if and only if $\left(\frac{p^*}{q}\right) = 1$.

Some Useful Facts

Recall that H was defined to be the unique subgroup of square elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong C_{p-1}$. By the isomorphism

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

we may **identify H with the (nonzero) quadratic residues in** $(\mathbb{Z}/p\mathbb{Z})^\times$.

Some Useful Facts

Recall that H was defined to be the unique subgroup of square elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong C_{p-1}$. By the isomorphism

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

we may **identify H with the (nonzero) quadratic residues in** $(\mathbb{Z}/p\mathbb{Z})^\times$. Also,

$$\begin{array}{c} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \\ | \\ H \\ | \\ \{0\} \end{array} \qquad\qquad \begin{array}{c} \mathbb{Q} \\ | \\ K \\ | \\ \mathbb{Q}(\zeta_p) \end{array}$$

By the Fundamental Theorem of Galois Theory, $\boldsymbol{H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)}$.

Closing

Therefore, an automorphism $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$ if and only if q is a quadratic residue modulo p, i.e., $\left(\frac{q}{p}\right) = 1$.

Closing

Therefore, an automorphism $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$ if and only if q is a quadratic residue modulo p, i.e., $\left(\frac{q}{p}\right) = 1$.

Now, the Galois group of the quadratic extension $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ has two elements: the identity map and the conjugation map $\sqrt{p^*} \mapsto -\sqrt{p^*}$. We identify $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \{\pm 1\}$.

Closing

Therefore, an automorphism $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$ if and only if q is a quadratic residue modulo p, i.e., $\left(\frac{q}{p}\right) = 1$.

Now, the Galois group of the quadratic extension $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ has two elements: the identity map and the conjugation map $\sqrt{p^*} \mapsto -\sqrt{p^*}$. We identify $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \{\pm 1\}$.

Consider an automorphism σ_q in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let σ'_q be the restriction of σ_q on $\mathbb{Q}(\sqrt{p^*})$. Then σ'_q is the corresponding automorphism in $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$. By Stevenhagen [1] (involving additional definitions), an element σ'_q in $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ is the identity if and only if q splits in $\mathbb{Q}(\sqrt{p^*})$, i.e. $\left(\frac{p^*}{q}\right) = 1$. However, the former condition is true if and only if σ_q fixes $K = \mathbb{Q}(\sqrt{p^*})$, i.e. $\left(\frac{q}{p}\right) = 1$.

Closing

The equivalence

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

where

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

is what we need.

Closing

Since the Legendre symbol is multiplicative, we have

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

where we have used that -1 is a square modulo p only if 4 divides $p-1$, so that $\left(\frac{-1}{q}\right) = (-1)^{(p-1)/2}$. This completes the proof of quadratic reciprocity. □

Final Remarks

- The two Legendre symbols $\left(\frac{p^*}{q}\right)$ and $\left(\frac{q}{p}\right)$ secretly encoded information about the order of the Frobenius element σ_q.

Final Remarks

- The two Legendre symbols $\left(\frac{p^*}{q}\right)$ and $\left(\frac{q}{p}\right)$ secretly encoded information about the order of the Frobenius element σ_q.
- The quadratic reciprocity law is sometimes accompanied by the supplementary result

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

References

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