www.journal.asbsociety.com

JASB
JOURNAL OF THE ASB SOCIETY

Using decomposition groups to prove theorems about quadratic residues

Perutka, Tomáš[1]*

1 *Faculty of Science, Masaryk University, 611 37 Brno, Czechia*
* *Corresponding author: tom.perutka@gmail.com*

In this text we elaborate on the modern viewpoint of the quadratic reciprocity law via methods of algebraic number theory and class field theory. We present original, short and simple proofs of so called additional quadratic reciprocity laws and of the multiplicativity of the Legendre symbol using decompositon groups of primes in quadratic and cyclotomic extensions of $\mathbb{Q}$.

Key words: Quadratic residue, decomposition group, Frobenius automorphism.

(Submitted: 11 September 2020, Accepted: 15 September 2020, Published: 28 December 2020)

Introduction

The quadratic reciprocity law is a theorem which enables us to work easily with quadratic residues. It was first proved by Gauss and since then it is (along with Fermat's Last Theorem) one of the results crucial for a further development of algebraic number theory: the work of Kummer, Kronecker, Artin and others on algebraic number theory and class field theory was partially motivated by trying to find a more general reciprocity law which would include the quadratic one as a special case. This quest was fulfilled via the Artin reciprocity law (more details, for example, are in [1]).

Gauss himself proved the quadratic reciprocity law in eight different ways; today there are more than 300 proofs (the complete list in [2]). Why is it so? Firstly, the theorem is quite popular and significant in number theory, it can be used, for example, to solve quadratic diophantine equations. The other reason is that people were looking for a proof which promises generalisation. The proof we work with is one of those proofs: it uses the full power of arithmetical results for finite Galois extensions of $\mathbb{Q}$, and the careful examination of cyclotomic and quadratic fields as well.

Let us now talk more about the structure of this text. In the first section, we mention some important prerequisites and results from algebraic number theory, mostly following [3], chapters 2-4. In Section 2, we present a proof of the quadratic reciprocity law. In Section 3, we reprove other statements about the quadratic residues by similar methods.

Conventions

The finite field with q elements will be denoted as $\mathbb{F}_q$. We will denote the element of the group $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$ containing an integer a as $[a]_n$; hence both $c \in [a]_n, [c]_n = [a]_n$ mean $c \equiv a \pmod{n}$. The ideal of a ring R generated by elements $a_1, ..., a_n$ will be denoted $(a_1, ..., a_n)$ if the ring R is evident from the context and $a_1R + \cdots + a_nR$ otherwise. All rings are commutative and prime ideals are assumed to be nonzero.

1 The prerequisites

1.1 Quadratic residues

We say that $m \in \mathbb{Z}$ is a quadratic residue modulo $n \in \mathbb{N}$ if m, n are coprime and there is $x \in \mathbb{Z}$ such that $x^2 \equiv m \pmod{n}$. We are interested only in quadratic residues modulo an odd prime p. This leads to the convention of the Legendre symbol:

Definition 1. *Let p be an odd prime, $a \in \mathbb{Z}$. Then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ 0 & \text{if } p \mid a, \\ -1 & \text{otherwise.} \end{cases}$$

The Legendre symbol gives rise to a homomorphism of groups $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \to \{\pm 1\}$. To see this, one needs to prove its multiplicativity. We will do this in Section 3.

The following theorem enables us to work with Legendre symbol quite easily:

Theorem 1. *Let p, q be a distinct odd primes. Then*

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

Furthermore, the following holds:

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{3}$$

The statement (1) is known as the quadratic reciprocity law; (2), (3) are usually called the additional or supplementary (quadratic) reciprocity laws.

To unpack the formulas a little, we will also introduce a reformulation via residue classes:

Theorem 1. *Let p, q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Furthermore, the following holds:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

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

1.2 Galois extensions

We now very briefly recall the notion of a Galois extension (more details can be found for example in [4], Chapter VI). We say that the finite field extension K/k of degree n is Galois if there are precisely n k-automorphisms (i.e. they are trivial when restricted to k) of the field K. The group of k-automorphisms is then called the Galois group and denoted as $\mathrm{Gal}\,(K/k)$.

For example, any extension of finite fields is Galois with a cyclic Galois group. The case of our interest is mostly the case of Galois extensions $K/\mathbb{Q}$.

For Galois extensions, there is a one-to-one correspondence between the intermediate fields $k \subseteq M \subseteq K$ and the subgroups of $\mathrm{Gal}\,(K/k)$ realized as follows:

- $k \subseteq M \subseteq K \mapsto \{\sigma \in \mathrm{Gal}\,(K/k)\,; \sigma|_M = \mathrm{id}_M\}$,
- $H \subseteq \mathrm{Gal}\,(K/k) \mapsto \{\alpha \in K; \forall \sigma \in H\,:\,\sigma(\alpha) = \alpha\}$.

Moreover, the extension K/M is Galois for any intermediate field M. The extension M/k is Galois if and only if the group $\mathrm{Gal}\,(K/M)$ is a normal subgroup of $\mathrm{Gal}\,(K/k)$; in that case we have the isomorphism $\mathrm{Gal}\,(M/k) \cong \mathrm{Gal}\,(K/k)\,/\,\mathrm{Gal}\,(K/M)$ given by restriction to M. More precisely, the assignement $\sigma \in \mathrm{Gal}\,(K/k) \mapsto \sigma|_M \in \mathrm{Gal}\,(M/k)$ is a group homomorphism with kernel $\mathrm{Gal}\,(K/M)$.

1.3 Decomposition of primes in number fields

We will recall some basic facts from algebraic number theory. Consider any finite field extension $K/\mathbb{Q}$; by finiteness, each element of K is algebraic over $\mathbb{Q}$. Such K will be called a number field. We say that $\alpha \in K$ is an algebraic integer if its minimal polynomial over $\mathbb{Q}$ is monic with integer coefficients. Algebraic integers of K form a ring denoted as $\mathcal{O}_K$. It is well known that $\mathcal{O}_K$ is a Dedekind ring and hence each of its ideals (apart from $\{0\}$ and $\mathcal{O}_K$) has a unique decomposition as a product of prime ideals.

Consider any prime $p \in \mathbb{Z}$. We get

$$p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g},$$

where $\mathcal{P}_1, \ldots \mathcal{P}_g$ are distinct prime ideals of $\mathcal{O}_K$; we say that they lie over p. Moreover, each field $\mathcal{O}_K\,/\,\mathcal{P}_i$ is a finite field of characteristic p with p^{f_i} elements. All these constants are neatly tied together:

$$\sum_{i=1}^{g} e_i f_i = [K\,:\,\mathbb{Q}].$$

This whole situation is much simpler if $K/\mathbb{Q}$ is Galois. In that case we get $e_1 = \cdots = e_g = e, f_1 = \cdots = f_g = f$ and hence $efg = [K\,:\,\mathbb{Q}]$.

We will end this section with an important observation about the decomposition of primes in the case that $\mathcal{O}_K = \mathbb{Z}[\omega]$ for some algebraic integer $\omega \in K$: this will occur in the setting of both quadratic and cyclotomic fields.

Theorem 2. *Let $\omega \in K$ be an algebraic integer such that $\mathcal{O}_K = \mathbb{Z}[\omega]$ and denote by $f(x) \in \mathbb{Z}[x]$ its minimal polynomial over $\mathbb{Q}$. Consider any prime $p \in \mathbb{Z}$. Let*

$$f(x) \equiv p_1(x)^{e_1} \cdots p_g(x)^{e_g} \pmod{p}$$

be the decomposition of $f(x) \mod p \in \mathbb{F}_p[x]$ as a product of monic irreducible polynomials. Then

$$p\,\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}$$

with $f_i = |\,\mathcal{O}_K\,/\,\mathcal{P}_i\,| = \deg p_i$; moreover, $\mathcal{P}_i = (p, \widetilde{p}_i(\omega))$ for any $\widetilde{p}_i \in \mathbb{Z}[x]$ such that $\widetilde{p}_i(x) \equiv p_i(x) \pmod{p}$.

Remark 2. This may appear as something very unintuitive and surprising, but that is not the case when seen through the lens of tensoring with $\mathbb{F}_p$. We already know that $p\,\mathcal{O}_K = \mathcal{Q}_1^{e'_1} \cdots \mathcal{Q}_{g'}^{e'_{g'}}$ for some

prime ideals $\mathcal{Q}_i \subseteq \mathcal{O}_K$. So on one hand, we have

$$\mathbb{F}_p \otimes \mathcal{O}_K \cong \mathcal{O}_K / p\,\mathcal{O}_K \cong \prod_{i=1}^{g'} \mathcal{O}_K / \mathcal{Q}_i^{e_i'}$$

(the latter is due to the Chinese Reminder Theorem). And on the other hand,

$$\mathbb{F}_p \otimes \mathbb{Z}[\omega] \cong \mathbb{F}_p \otimes (\mathbb{Z}[x]/(f(x))) \cong \mathbb{F}_p[x]/(f(x) \mod p) \cong \prod_{i=1}^{g} \mathbb{F}_p[x]/\left(p_i(x)^{e_i}\right).$$

Although there are still some details to fill in (cf. [5], Thm. 4.12), the theorem above should now appear as a natural thing.

Remark 3. A more general version of the theorem is also true. If there is some algebraic integer $\omega \in K$ such that $\mathbb{Z}[\omega]$ is an additive subgroup of $\mathcal{O}_K$ of finite index d, the same conclusions as in the theorem above hold for each prime $p \in \mathbb{Z}$ not dividing d. This will come in handy in Section 1.5.

1.4 Arithmetic of abelian extensions of $\mathbb{Q}$

In this section we will work with number fields K such that $K/\mathbb{Q}$ is an abelian extension – i.e. Galois extension with commutative Galois group. We already know that for each prime $p \in \mathbb{Z}$ we have $p\,\mathcal{O}_K = \left(\mathcal{P}_1 \cdots \mathcal{P}_g\right)^e$ with $efg = [K : \mathbb{Q}]$, where $f = |\,\mathcal{O}_K / \mathcal{P}_i\,|$. Now we need to introduce some terminology:

Definition 4. *We say that the prime p*

- *ramifies in K if $e > 1$,*
- *totally ramifies in K if $e = n$ (and $f = g = 1$),*
- *is unramified in K if $e = 1$,*
- *is inert/remains prime in K if $f = n$ (and $e = g = 1$),*
- *splits completely in K if $g = n$ (and $e = f = 1$).*

The fact that K is a Galois extension enables us to define the following:

Definition 5. *Let $p \in \mathbb{Z}$ be a prime, $\mathcal{P} \subseteq \mathcal{O}_K$ be a prime ideal lying over p. Then the decomposition group of $\mathcal{P}$ in $K/\mathbb{Q}$ is the group*

$$D(\mathcal{P}) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) ; \sigma(\mathcal{P}) = \mathcal{P}\}.$$

Further, the inertia group of $\mathcal{P}$ in K is the group

$$I(\mathcal{P}) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) ; \forall \alpha \in \mathcal{O}_K : \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}}\}.$$

In the case of abelian extensions, the decomposition group does not depend on the prime ideal, but only on the prime it lies over: for any two $\mathcal{P}, \mathcal{P}'$ lying over p, we have $D(\mathcal{P}) = D\left(\mathcal{P}'\right), I(\mathcal{P}) = I\left(\mathcal{P}'\right)$. We thus speak about decomposition/inertia group of p and denote it as D_p, I_p; or $D_p(K), I_p(K)$ if we need to distinguish the field K. We can also see that $I_p \leq D_p$.

These groups carry much information about the decomposition of p. We can sum it up in the following proposition:

Proposition 6. *Let $\mathcal{P}$ be a prime lying over p. Denote $\widetilde{G} = \mathrm{Gal}\left((\mathcal{O}_K / \mathcal{P}) / \mathbb{F}_p\right)$ – this is a cyclic group of order f generated by a Frobenius automorphism $\varphi : x \mapsto x^p$. Then, there is a canonical isomorphism $h : D_p/I_p \cong \widetilde{G}$. Moreover, the field $M_{D_p} \subseteq K$ fixed by D_p in Galois correspondence is the largest subfield of K in which p splits completely.*

Also, it can be shown that I_p is trivial precisely when p is unramified. In that case $D_p \cong \widetilde{G}$ is a cyclic group with a generator $\mathrm{Frob}_p = h^{-1}(\varphi)$. This generator is called the Frobenius automorphism of p.

The Frobenius automorphism of a prime is somehow a central notion of the algebraic number theory in Galois extensions. Moreover, it is a notion upon which class field theory has been built. Let us mention just two features of this automorphism:

Proposition 7. *Let K be an abelian number field, p a prime unramified in K. Then $Frob_p = \mathrm{id}$ if and only if p splits completely in K.*

Proposition 8. *Let K, k be abelian number fields with $k \subseteq K$. Then $Frob_p(K)|_k = Frob_p(k)$ for each prime $p \in \mathbb{Z}$.*

1.5 Quadratic fields

We define a quadratic field as an extension of $\mathbb{Q}$ of degree 2 – these are precisely the fields $\mathbb{Q}\left(\sqrt{d}\right)$ where $d \neq 0, 1$ is a square-free integer. Moreover, each such extension is abelian with $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{d}\right)/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z} \cong \{\mathrm{id}, \sigma_d\}$, where $\sigma_d\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$.

There are only three ways in which a prime $p \in \mathbb{Z}$ can decompose in $\mathbb{Q}\left(\sqrt{d}\right)$:

- $e = 2, f = g = 1$ (totally ramifies),
- $f = 2, e = g = 1$ (remains prime),
- $g = 2, e = f = 1$ (splits completely).

It is straightforward to compute that $\mathcal{O}_{\mathbb{Q}\left(\sqrt{d}\right)}$ is equal to $\mathbb{Z}[\sqrt{d}]$ for $d \equiv 2, 3 \pmod 4$ and to $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ for $d \equiv 1 \pmod 4$. Hence, we know from Theorem 2 that in case $d \not\equiv 1 \pmod 4$, the decomposition of a prime $p \in \mathbb{Z}$ depends on the decomposition of $x^2 - d \pmod p$, i.e. on the Legendre symbol $\left(\frac{d}{p}\right)$!. Since $|\mathbb{Z}[\frac{1+\sqrt{d}}{2}]/\mathbb{Z}[\sqrt{d}]| = 2$, we see from Remark 3 that the same is true for odd primes in case $d \equiv 1 \pmod 4$. We thus arrive at the following proposition:

Proposition 9. *Let $d \neq 0, 1$ be a squarefree integer, $p \in \mathbb{Z}$ an odd prime. Then p*

- *totally ramifies as $\left(p, \sqrt{d}\right)^2$ if $\left(\frac{d}{p}\right) = 0$,*
- *splits completely as $\left(p, c - \sqrt{d}\right)\left(p, c + \sqrt{d}\right)$ if $\left(\frac{d}{p}\right) = 1, d \equiv c^2 \pmod p$,*
- *remains prime if $\left(\frac{d}{p}\right) = -1$.*

1.6 Cyclotomic fields

We define the n-th cyclotomic field, $n \in \mathbb{N}$, as $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ is the primitive n-th root of unity. Again, these are all abelian extensions of $\mathbb{Q}$ with canonical isomorphism $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Since each automorphism of $\mathbb{Q}(\zeta_n)$ is uniquely determined by the image of ζ_n, we can define $\phi([a]_n)$ via $\zeta_n \mapsto \zeta_n^a$. This is easily seen to be well-defined and it can be proved that it really is an isomorphism.

Not only does the isomorphism ϕ work very naturally, it also behaves well with arithmetic properties:

Theorem 3. *Let $p \in \mathbb{Z}$ be a prime, $n \in \mathbb{N}$. Then p ramifies in $\mathbb{Q}(\zeta_n)$ if and only if $p \mid n$. For $p \nmid n$, consider the Frobenius automorphism $Frob_p \in D_p(\mathbb{Q}(\zeta_n))$ of p in the n-th cyclotomic field. Then $\phi([p]_n) = Frob_p$.*

This is a quite handy result, we can, for example, deduce the following:

Corollary 10. *A prime $p \in \mathbb{Z}$ splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \pmod n$.*

Proof. This follows from Prop. 7 and the theorem above. □

2 The proof of the quadratic reciprocity law

We start with the following lemma:

Lemma 11. *Let $p \in \mathbb{Z}$ be an odd prime. Then the only quadratic subfield of $\mathbb{Q}(\zeta_p)$ is of the form $\mathbb{Q}\left(\sqrt{p^*}\right)$, where $p^* = (-1)^{\frac{p-1}{2}} p$ is equal to p if $p \equiv 1 \pmod 4$ and to $-p$ if $p \equiv 3 \pmod 4$.*

Proof. It is well-known that $\left(\mathbb{F}_p^*\right)^2 = \{a^2 | a \in \mathbb{F}_p^*\}$ is the only subgroup of $\mathbb{F}_p^*$ of index 2. Since $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) \cong \mathbb{F}_p^*$, we know from Galois theory that $\mathbb{Q}(\zeta_p)$ has a subfield K with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_p^*/\left(\mathbb{F}_p^*\right)^2$, $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/K\right) \cong \left(\mathbb{F}_p^*\right)^2$, $[K : \mathbb{Q}] = 2$, i.e. a quadratic subfield. We know from Theorem 3 that the only prime which ramifies in $\mathbb{Q}(\zeta_p)$ is p, hence we can conclude from Prop. 9 that $K = \mathbb{Q}\left(\sqrt{\pm p}\right)$. Now it is somewhat delicate to figure out the sign. One way to proceed is to use Gauss sums, the other way is to explore the decomposition of the prime 2. It is possible to show that 2 ramifies in $\mathbb{Q}\left(\sqrt{d}\right)$ for $d \not\equiv 1$ (and does not ramify otherwise) and hence we get $\pm p \equiv 1 \pmod 4$ and the lemma follows. □

Lemma 12. *The quadratic reciprocity law is equivalent to*

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

The proof is very easy and left to the reader as an exercise. □

We will now prove the quadratic reciprocity law by proving $\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p^*}{q}\right) = 1$. The equality $\left(\frac{q}{p}\right) = 1$ is equivalent to the existence of an integer a such that $q \equiv a^2 \pmod p$, which is the same as $[q]_p \in \left(\mathbb{F}_p^*\right)^2$. But from the proof of Lemma 11 and from Theorem 3, we see that this is equivalent to $\mathrm{Frob}_q\left(\mathbb{Q}(\zeta_p)\right) \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\left(\sqrt{p^*}\right)\right)$. Now we use Prop. 8 to get $\mathrm{Frob}_q\left(\mathbb{Q}\left(\sqrt{p^*}\right)\right) = \mathrm{Frob}_q\left(\mathbb{Q}(\zeta_p)\right)|_{\mathbb{Q}(\sqrt{p^*})} = \mathrm{id}$ since the restriction from $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ to $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{p^*}\right)/\mathbb{Q}\right)$ corresponds to the projection $\mathbb{F}_p^* \to \mathbb{F}_p/\left(\mathbb{F}_p^*\right)^2$. This means that q splits completely in $\mathbb{Q}\left(\sqrt{p^*}\right)$, i.e. $\left(\frac{p^*}{q}\right) = 1$. Since every step is easily reversible, the quadratic reciprocity law is proved.

To put it in a concise way, the proof is actually the following chain of equivalences:

$$\begin{aligned}
\left(\frac{q}{p}\right) = 1 &\Leftrightarrow \exists a \in \mathbb{Z} : q \equiv a^2 \pmod p \\
&\Leftrightarrow [q]_p \in \left(\mathbb{F}_p^*\right)^2 \\
&\Leftrightarrow \mathrm{Frob}_q\left(\mathbb{Q}(\zeta_p)\right) \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\left(\sqrt{p^*}\right)\right) \\
&\Leftrightarrow \mathrm{Frob}_q\left(\mathbb{Q}\left(\sqrt{p^*}\right)\right) = \mathrm{Frob}_q\left(\mathbb{Q}(\zeta_p)\right)|_{\mathbb{Q}(\sqrt{p^*})} = \mathrm{id} \\
&\Leftrightarrow q \text{ splits completely in } \mathbb{Q}\left(\sqrt{p^*}\right) \\
&\Leftrightarrow \left(\frac{p^*}{q}\right) = 1.
\end{aligned}$$

Remark 13. This proof is not easy to find in the literature; the author has found it only in [6].

3 Proofs of additional laws and other statements

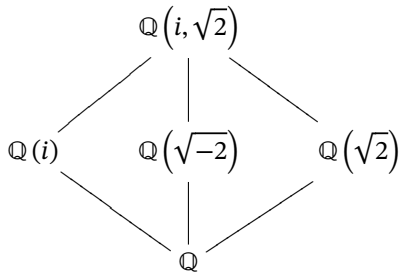
We will now apply the arithmetic of quadratic and cyclotomic fields to reprove other statements about quadratic residues. Since the situation is easier than in the case of the quadratic reciprocity law, we will be able to prove theorems in more detail.

Theorem 4. *For any odd prime p, we have* $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

Proof. We will use the fact that the field $\mathbb{Q}(i)$ is both quadratic and cyclotomic. It is the quadratic field $\mathbb{Q}\left(\sqrt{-1}\right)$, hence we know from Proposition 9 that p splits completely in it if and only if $\left(\frac{-1}{p}\right) = 1$. It is also the cyclotomic field $\mathbb{Q}(\zeta_4)$, so we see from Corollary 10 that p splits completely in it if and only if $p \equiv 1 \pmod 4$. Hence $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$ and the theorem follows. □

Theorem 5. *For any odd prime p, we have* $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$

Proof. The proof will be analogous to the previous one, but more subtle. We will now work with a field $\mathbb{Q}\left(i, \sqrt{2}\right)$, which is an abelian extension of $\mathbb{Q}$ with $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt{2}\right)/\mathbb{Q}\right) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}$, where σ is given by $\sqrt{2} \mapsto -\sqrt{2}, i \mapsto i$ and τ by $\sqrt{2} \mapsto \sqrt{2}, i \mapsto -i$. We see from Galois theory that the lattice of intermediate fields of $\mathbb{Q}\left(i, \sqrt{2}\right)/\mathbb{Q}$ looks like this:



Furthermore, $\mathbb{Q}\left(i, \sqrt{2}\right)$ is also the cyclotomic field $\mathbb{Q}(\zeta_8) = \mathbb{Q}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$, hence $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt{2}\right)/\mathbb{Q}\right)$ $\cong (\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$.

We thus have two explicit descriptions of the Galois group and now we have to find out how they match each other. For that, we need to compute how σ and τ act on ζ_8 (since they generate the Galois group):

- $\sigma\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} = \zeta_8^5 \Rightarrow \sigma$ corresponds to $[5]_8$,
- $\tau\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} = \zeta_8^7 \Rightarrow \tau$ corresponds to $[7]_8$.

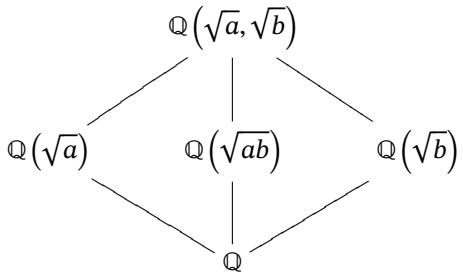
Now, we already know well that $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p$ splits completely in $\mathbb{Q}\left(\sqrt{2}\right) \Leftrightarrow \mathrm{Frob}_p\left(\mathbb{Q}\left(\sqrt{2}\right)\right)$ $= \mathrm{id}$. But we also know that $\mathrm{Frob}_p\left(\mathbb{Q}\left(\sqrt{2}\right)\right) = \mathrm{Frob}_p\left(\mathbb{Q}\left(i, \sqrt{2}\right)\right)|_{\mathbb{Q}\left(\sqrt{2}\right)}$, so $\left(\frac{2}{p}\right) = 1$ if and only if $\mathrm{Frob}_p\left(\mathbb{Q}\left(i, \sqrt{2}\right)\right) \in \mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)\right) = \{\mathrm{id}, \tau\} \cong \{[1]_8, [7]_8\}$ since τ fixes $\mathbb{Q}\left(\sqrt{2}\right)$ and corresponds to $[7]_8$. Hence $\left(\frac{2}{p}\right) = 1 \Leftrightarrow \mathrm{Frob}_p\left(\mathbb{Q}\left(i, \sqrt{2}\right)\right) \in \{\mathrm{id}, \tau\} \Leftrightarrow p \equiv 1, 7 \pmod 8$ and that is what we wanted to prove. □

Theorem 6. *The Legendre symbol is multiplicative, i.e.* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ *for each odd prime p and* $a, b \in \mathbb{Z}$.

Proof. The only non-trivial part of the proof is when we assume that a, b are distinct squarefree integers with, $a, b \neq 0, 1$, $p \nmid ab$. We will thus treat only this case and leave the rest of the proof to the reader.

With this assumption we see that $\mathbb{Q}\left(\sqrt{a}\right), \mathbb{Q}\left(\sqrt{b}\right), \mathbb{Q}\left(\sqrt{ab}\right)$ are quadratic fields embedded in the

field $\mathbb{Q}\left(\sqrt{a},\sqrt{b}\right)$ which is abelian of degree 4 over $\mathbb{Q}$:



The Galois theory tells us that these three quadratic fields are the only nontrivial subfields of $K = \mathbb{Q}\left(\sqrt{a},\sqrt{b}\right)$. Consider the group $D_p(K)$. We have seen that this group fixes the largest subfield of K in which p splits completely. This subfield cannot be $\mathbb{Q}$ because then $D_p(K) = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ would not be cyclic (p cannot ramify because of our assumption $p \nmid ab$). If this subfield is K itself, p splits completely in all subfields and in particular, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) = 1$ and the theorem holds.

It remains to examine the case when $D_p(K)$ fixes one of the quadratic subfields. But in that case, p remains prime in the other two and the two of the three Legendre symbols are equal to -1 and the third to 1. The theorem hence follows. □

Conclusion

The proofs we have seen in this text are just a few of many demonstrations of the fact that we have a very good understanding of the arithmetical theory of abelian extensions of $\mathbb{Q}$, which moreover behaves very nicely. The proofs of more general reciprocity laws over $\mathbb{Q}$ rely on class field theory, which is about much deeper examination of the phenomena we have seen here.

The natural question arises: can we prove in a similar way some kind of the quadratic reciprocity law over other number fields than $\mathbb{Q}$? It would certainly require a well-behaved arithmetical theory of abelian extensions of that field. In the current state of art, this is developed only for imaginary quadratic fields, i.e. fields $\mathbb{Q}\left(\sqrt{d}\right)$ with $d < 0$. It might be interesting to try and build a similar setting for the field $\mathbb{Q}(i)$, for example.

Acknowledgements

The author wishes to thank Radan Kučera for careful reading and commenting on the high school project which resulted in this text.

References

(1) Milne, J. S. Class Field Theory, Lecture notes, 2013, www.jmilne.org/math/.

(2) Baumgart, O., *The quadratic reciprocity law : a collection of classical proofs*; Springer: Cham, 2015, ISBN: 978-3-319-16282-9.

(3) Marcus, D., *Number fields*; Springer-Verlag: New York, 1977, ISBN: 0-387-90279-1.

(4) Lang, S., *Algebra*; Springer: New York, 2002, ISBN: 0-387-95385-X.

(5) Manin, Y. I.; Panchishkin, A. A., *Introduction to modern number theory : fundamental problems, ideas and theories*; Springer: Berlin New York, 2005, ISBN: 3-540-20364-8.

(6) Kato, K.; Kurokawa, N.; Saitō, T.; Kurihara, M., *Number theory*; Iwanami series in modern mathematics volume 186, 240, 242; American Mathematical Society: Provdence, RI, 2000, ISBN: 9780821808634 9780821813553.


JASB