Radboud University

Radboud University Nijmegen

Faculty of Science

The Hasse Norm Principle and Biquadratic Fields

Thesis MSc Mathematics

Author:
Merlijn Keune

Student number:
4052218

Supervisor:
dr. Wieb Bosma

Second reader:
dr. Victoria Hoskins

November 2021

Abstract

The Hasse Norm Principle is valid for an extension $L : K$ of number fields when for every $a \in K^*$, a is a norm of $L : K$ if and only if it is a local norm at every prime of K. In 1931 Hasse proved this principle to be valid for all cyclic extensions of number fields. He also disproved his own conjecture that this principle is valid for all abelian extensions of number fields by showing it is not valid for the biquadratic extension $\mathbb{Q}(\sqrt{-3}, \sqrt{13}) : \mathbb{Q}$. Later also Tate provided an example showing the principle is not valid for $\mathbb{Q}(\sqrt{13}, \sqrt{17}) : \mathbb{Q}$, using modern methods of class field theory.

In this thesis both these examples are treated in a relatively elementary way, using the classical ideal theoretic approach of class field theory. We use Hasse's original method of proof to show that also Tate's example can be proved in this setting. Afterwards we extend Tate's example to $\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}$ with prime numbers $p, q \equiv 1 \pmod 4$ such that $\left(\frac{p}{q}\right) = 1$, still aiming to use as few tools as possible.

Contents

1. History

In 1931 the German mathematician Helmut Hasse published an article [5] in which he proved what is now known as the Hasse Norm Theorem: in a cyclic extension $L : K$ of number fields, an element $a \in K^*$ is a global norm if and only if it is a local norm everywhere. To be more precise, there exists an $\alpha \in L^*$ such that $\mathrm{N}_K^L(\alpha) = a$ if and only if for every prime $\mathfrak{p}$ of K there exists an $\alpha_\mathfrak{q} \in L_\mathfrak{q}^*$ such that $\mathrm{N}_\mathfrak{p}^\mathfrak{q}(\alpha_\mathfrak{q}) = a$, where $\mathfrak{q}$ is a prime of L above $\mathfrak{p}$, $L_\mathfrak{q}$ and $K_\mathfrak{p}$ are completions of L and K at their respective primes $\mathfrak{q}$ and $\mathfrak{p}$, and $\mathrm{N}_\mathfrak{p}^\mathfrak{q}$ denotes the norm from $L_\mathfrak{q}$ to $K_\mathfrak{p}$. More generally, for an arbitrary extension of number fields we say the Hasse Norm Principle is valid when elements are global norms if and only if they are local norms everywhere. In that terminology, the Hasse Norm Theorem simply states that the Hasse Norm Principle is valid for all cyclic extensions of number fields.

Unlike many other theorems in class field theory, there is no analogue for this theorem for abelian extensions of number fields. In an article published in 1930 [4], after proving the special case of the theorem of cyclic extensions of prime degree, Hasse conjectured the norm principle to be valid for all abelian extensions of number fields. He disproved this in the 1931 article [5] by providing a counterexample: in the biquadratic extension $\mathbb{Q}(\sqrt{-3}, \sqrt{13}) : \mathbb{Q}$ the element 3 is a local norm everywhere, but not a global norm. Hence the Hasse Norm Principle is not valid for $\mathbb{Q}(\sqrt{-3}, \sqrt{13}) : \mathbb{Q}$.

Later on, in 1967, another example was given by John Tate, as an exercise in the book Algebraic Number Theory [1]. Using the more modern methods of idèles and cohomology, he provides a class of squares that are local norms at every prime of the extension $\mathbb{Q}(\sqrt{13}, \sqrt{17}) : \mathbb{Q}$, but not global norms.

Beside these widely known examples, there are numerous mathematicians who have published on this subject, aiming to find more precise criteria for whether or not the Hasse Norm Principle is valid for a given number field extension. Notably, German mathematician Arnold Scholz wrote a number of articles about it during the 1930's. In 1936 [14] he introduced the concept of a knot of an extension $L : K$ of number fields: the group of all $a \in K^*$ that are local norms everywhere, divided by the subgroup of global norms. In that terminology, the Hasse Norm Principle is valid for an extension if and only if it has a trivial knot. Despite being regarded as a mathematical genius, Scholz was notoriously bad at expressing his ideas on paper. That may have contributed to many of his results being forgotten over the years, only to be rediscovered by others much later. For example, the extension $\mathbb{Q}(\sqrt{13}, \sqrt{17}) : \mathbb{Q}$ covered by Tate, already appeared in Scholz's work in 1936. In more recent decades, his work has gained renewed appreciation.

Lastly we mention the work of Wolfram Jehne, a student of Hasse, who in 1979 published an article [9] on knots in which he treats these from the more modern idèle theoretic viewpoint of class field theory – also used by Tate in the example we mentioned above – allowing him to greatly extend the results reached by Scholz. For biquadratic extensions $L : \mathbb{Q}$, what this thesis is concerned with, his work shows that the knot is trivial if and only if there is a prime p such that the local degree at p, the degree of $L_{\mathfrak{p}} : \mathbb{Q}_p$ with $\mathfrak{p}$ a prime of L above p, equals 4. While this result is quite definitive, it does not provide explicit examples of elements in the non-trivial knots.

Both of the aforementioned examples are often referred to in books and articles, but mostly either without proof or with an incorrect proof. This thesis will provide relatively elementary proofs of both examples, set in the ideal theoretic approach to class field theory, making no use of idèles or cohomology. Subsequently we will generalize this method to apply to any biquadratic field extension $\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}$ with prime numbers $p, q \equiv 1 \pmod 4$ such that $\left(\frac{p}{q}\right) = 1$, giving a class of squares that are local norms everywhere, but not global norms.

2. The Classical Examples

We first turn our attention to the two examples given by Hasse and Tate. Before giving proofs of those, some tools that will be useful are treated.

2.1 Artin's Reciprocity Law

While in this thesis the aim is to use relatively basic tools, the most notable exception is Artin's Reciprocity Law. This is a central theorem in Class Field Theory, so any course on the subject should treat it at some point. While stated in slightly varying ways, any number of textbooks can be used to find a proof of this theorem, for example Algebraic Number Fields by Janusz [8], Chapter V, Theorem 5.8. Here we present the theorem as stated in Number Fields by Keune [10]. The differences in formulation and notation that can be found throughout different sources should not cause any trouble, since we're actually interested in a relatively simple case, where the number field extension considered is unramified. This completely removes any difficulties regarding notation, resulting in the very simple statement in Corollary 3, which is all that will be used.

For readability we will go over some notation used in the theorem, assuming knowledge of the concepts they represent.

Notation 1. Let $L : K$ be an abelian extension of number fields.

- $\mathbb{I}(K)$ denotes the group of fractional ideals of $\mathcal{O}_K$, the ring of integers of K.
- $\mathbb{I}^L(K) = \{\mathfrak{a} \in \mathbb{I}(K) \mid v_\mathfrak{p}(\mathfrak{a}) = 0 \text{ for all in } L \text{ ramifying } \mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)\}$, the subgroup of $\mathbb{I}(K)$ generated by the non-ramifying prime ideals of $\mathcal{O}_K$.
- A modulus $\mathfrak{m}$ of K, a formal product of primes of K, consists of a product of finite primes denoted by $\mathfrak{m}_0$ and a product of infinite primes denoted by $\mathfrak{m}_\infty$, so that $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$.
- $\mathbb{I}^\mathfrak{m}(K) = \{\mathfrak{a} \in \mathbb{I}(K) \mid v_\mathfrak{p}(\mathfrak{a}) = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0\}$, the subgroup of $\mathbb{I}(K)$ generated by the prime ideals of $\mathcal{O}_K$ not dividing the finite part $\mathfrak{m}_0$ of a modulus $\mathfrak{m}$ of K.
- $\mathbb{S}_\mathfrak{m}(K) = \{\alpha\mathcal{O}_K \in \mathbb{I}(K) \mid \alpha \in K, v_\mathfrak{p}(\alpha) = 0 \text{ and } v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0) \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0, \text{ and } \sigma_\mathfrak{p}(\alpha) > 0 \text{ for all real } \mathfrak{p} \mid \mathfrak{m}_\infty\}$, where $\sigma_\mathfrak{p} \colon K \to \mathbb{R}$ is the embedding of K in $\mathbb{R}$ associated with the real infinite prime $\mathfrak{p}$. $\mathbb{S}_\mathfrak{m}(K)$ is called the ray modulo $\mathfrak{m}$ of K.

- $\mathcal{C}\ell(K) = \mathbb{I}(K)/\mathbb{P}(K)$, the ideal class group of K, consisting of the fractional ideals of K modulo the principal fractional ideals $\mathbb{P}(K)$.
- $\varphi_K^{(L)} \colon \mathbb{I}^L(K) \to \mathrm{Gal}(L:K)$ is the Artin map, defined by sending a non-ramifying prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ to its Frobenius automorphism $\varphi_{\mathfrak{p}}^{(L)}$.

Theorem 2 (Artin's Reciprocity Law)**.** *Let $L:K$ be an abelian extension of number fields. Then there is a modulus $\mathfrak{m}$ of K having the ramifying primes as its prime divisors, such that the Artin map $\varphi_K^{(L)} \colon \mathbb{I}^L(K) \to \mathrm{Gal}(L:K)$ induces an isomorphism*

$$\mathbb{I}^{\mathfrak{m}}(K)/\,\mathrm{N}_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K) \xrightarrow{\sim} \mathrm{Gal}(L:K).$$

Corollary 3. *Let $L:K$ be an unramified abelian extension of number fields. Then the Artin map induces a surjective homomorphism*

$$\mathcal{C}\ell(K) \to \mathrm{Gal}(L:K).$$

Proof. Since there are no ramifying primes, Theorem 2 holds for the trivial modulus $\mathfrak{m} = (1)$. Then the isomorphism translates to

$$\mathbb{I}(K)/\,\mathrm{N}_K^L(\mathbb{I}(L))\mathbb{P}(K) \xrightarrow{\sim} \mathrm{Gal}(L:K).$$

The left hand side of this isomorphism is a factor group of $\mathcal{C}\ell(K) = \mathbb{I}(K)/\mathbb{P}(K)$, from which the corollary follows. □

2.2 Local Degrees

Throughout this thesis, we will be considering biquadratic field extensions of $\mathbb{Q}$. As mentioned earlier, the work of Jehne [9] shows that for the Hasse Norm Principle not to be valid for such an extension, it is necessary that no local degree of 4 occurs. While we are explicitly avoiding to make use of the methods he used to obtain this result, it does mean that our examples will naturally take place in extensions where no local degree of 4 occurs, and our proofs will rely on this fact. Here we will make precise what that means and look at the splitting behavior of primes in biquadratic number field extensions to find out when exactly such a local degree can appear, to be able to quickly show that they do not appear in the examples we will be working with. We begin with a formal definition to avoid confusion.

Definition 4. Let $L:K$ be a Galois extension of number fields, $\mathfrak{p}$ a prime of K and $\mathfrak{q}$ a prime of L above $\mathfrak{p}$. Then the local degree of $L:K$ at $\mathfrak{p}$ is the degree of the field extension $L_{\mathfrak{q}} : K_{\mathfrak{p}}$, where $L_{\mathfrak{q}}$ and $K_{\mathfrak{p}}$ are the completions of L and K at their respective primes.

Since the completion at an infinite prime is always either $\mathbb{R}$ or $\mathbb{C}$, the local degree at such a prime can only be 1 or 2. As we're only concerned with local degrees of 4 in the following, we assume all primes in this section to be finite.

Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with $m \neq n$ square-free integers $\neq 1$ and $k = \frac{mn}{\gcd(m,n)^2}$, so that also k is a square-free integer $\neq 1$ and the three quadratic subfields of L are $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{k})$.

Let p be a prime number and $\mathfrak{q}$ a prime of L above p. Completing $\mathbb{Q}$ and L at their corresponding primes, we obtain the local fields $\mathbb{Q}_p$ of p-adic numbers and $L_\mathfrak{q} = \mathbb{Q}_p(\sqrt{m}, \sqrt{n})$. Using the notation $e_p^{(L)}$ for the ramification index of p in L and similarly $f_p^{(L)}$ and $r_p^{(L)}$ for the residue class degree and the number of distinct primes $\mathfrak{q}$ of L above p respectively, we know that $r_p^{(L)} e_p^{(L)} f_p^{(L)} = [L : \mathbb{Q}] = 4$ and $[L_\mathfrak{q} : \mathbb{Q}_p] = e_p^{(L)} f_p^{(L)}$. So the extension $L_\mathfrak{q} : \mathbb{Q}_p$ has degree ≤ 4, being equal to 4 only when $r_p^{(L)} = 1$.

For a non-ramifying prime $r_p^{(L)} = 1$ would mean that $f_p^{(L)} = 4$, meaning that p remains prime in L. This however is impossible: if p were to remain prime in L, it would remain prime in all quadratic subfields, implying for $p = 2$ that $m \equiv n \equiv k \equiv 5 \pmod 8$ and for p odd that $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) = \left(\frac{k}{p}\right) = -1$, which both are obviously not possible.

So a local degree of 4 is only possible at ramifying primes that do not split. For a prime p to ramify completely in L it would need to ramify in all quadratic subfields. Since the primes ramifying in a quadratic number field $\mathbb{Q}(\sqrt{m})$ are exactly those that divide the discriminant of the quadratic field, which is either m or $4m$, ramifying in all three of them is only possible for $p = 2$.

The only case remaining is for $p\mathcal{O}_L$ to decompose as $\mathfrak{p}^2$. For odd p, ramifying in L means it has to ramify in exactly two of the quadratic subfields, since it necessarily divides two of the discriminants of the quadratic subfields of L. In the third quadratic subfield it has to remain prime for this splitting behavior to occur. For $p = 2$ it is also possible to ramify in one subfield, and remain prime in the other two. Summarizing, we have:

Lemma 5. *Let $L : \mathbb{Q}$ be a biquadratic number field extension and p a prime with local degree 4. Then p ramifies in L and either $p = 2$ and p doesn't split in any of the quadratic subfields, or p is odd and ramifies in exactly two of the quadratic subfields and remains prime in the third.* □

2.3 Hasse's Example: $\mathbb{Q}(\sqrt{-3}, \sqrt{13})$

For this section, unless specified otherwise, let $L = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$, $K = \mathbb{Q}(\sqrt{-39})$ and $\mathrm{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau \rangle$ such that $L^\sigma = \mathbb{Q}(\sqrt{-3})$ and $L^\tau = \mathbb{Q}(\sqrt{13})$. We also use the notation σ to indicate the restriction of $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ to K.

The original example by Hasse [5] shows that 3 is a local norm everywhere for the extension $L : \mathbb{Q}$, but not a global norm. The proof given here is directly based on the method used by Hasse, without making use of norm residue symbols. To start with, we determine some useful facts about the extension $L : \mathbb{Q}$ and its sub-extensions.

Firstly, the easy part of the example is demonstrated: 3 is a local norm at every prime of $\mathbb{Q}$. We use Lemma 5 of the previous section to quickly establish this.

Lemma 6. *For every prime p of $\mathbb{Q}$ and $\mathfrak{q}$ a prime of L above p, the local extension $L_\mathfrak{q} : \mathbb{Q}_p$ is of degree 1 or 2.*

Proof. A local extension at an infinite prime has degree 1 or 2 by definition. The only finite primes ramifying in L are 3 and 13, which both split in one of the quadratic subfields:

3 splits in $\mathbb{Q}(\sqrt{13})$ and 13 splits in $\mathbb{Q}(\sqrt{-3})$. Using Lemma 5 we see that a local degree of 4 does not exist. □

Lemma 7. *The number* 3 *is a local norm of* $L : \mathbb{Q}$ *at every prime* p *of* $\mathbb{Q}$.

Proof. Let p be a prime of $\mathbb{Q}$ and $\mathfrak{q}$ a prime of L above p. By Lemma 6 we know that the local degree $[L_\mathfrak{q} : \mathbb{Q}_p]$ is either 1 or 2. Since the case where it is 1 is trivial, assume $[L_\mathfrak{q} : \mathbb{Q}_p] = 2$. Then the non-trivial element of $\mathrm{Gal}(L_\mathfrak{q} : \mathbb{Q}_p)$ is a prolongation of either σ, τ or $\sigma\tau$. Since $(4 - \sqrt{13}) \cdot \sigma(4 - \sqrt{13}) = (4 - \sqrt{13})(4 + \sqrt{13}) = 3$ and $\sqrt{-3} \cdot \tau(\sqrt{-3}) = \sqrt{-3} \cdot \sigma\tau(\sqrt{-3}) = \sqrt{-3} \cdot -\sqrt{-3} = 3$, in any case 3 is a local norm. □

> More generally, we could have used norm residue symbols here like Hasse did in his original proof. For an abelian extension of number fields $L : K$, letting the symbol $\left(\frac{a, L:K}{\mathfrak{p}}\right)$ denote the image of $a \in K^*$ under the local Artin map $\vartheta_\mathfrak{p}^{(L)}$, this symbol equals 1 if and only if a is a local norm at $\mathfrak{p}$. One can use the identity
>
> $$\left(\frac{a, K_1K_2 : K}{\mathfrak{p}}\right) = \left(\frac{a, K_1 : K}{\mathfrak{p}}\right)\left(\frac{a, K_2 : K}{\mathfrak{p}}\right)$$
>
> to conclude that in our example 3 is a local norm at every prime: since 3 is a norm of $\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}$ and of $\mathbb{Q}(\sqrt{13}) : \mathbb{Q}$, the Hasse Norm Theorem implies $\left(\frac{3, \mathbb{Q}(\sqrt{-3}):\mathbb{Q}}{p}\right) = \left(\frac{3, \mathbb{Q}(\sqrt{13}):\mathbb{Q}}{p}\right) = 1$ for every prime p of $\mathbb{Q}$, and so
>
> $$\left(\frac{3, L : \mathbb{Q}}{p}\right) = \left(\frac{3, \mathbb{Q}(\sqrt{-3}) : \mathbb{Q}}{p}\right)\left(\frac{3, \mathbb{Q}(\sqrt{13}) : \mathbb{Q}}{p}\right) = 1$$
>
> for every p. See for example Hasse [4], §6, (9.) for a proof of this identity.

To make explicit calculations, we will be using the ideal class group $\mathcal{C}\ell(K)$ of K. Determining the ideal class group of a quadratic extension of $\mathbb{Q}$ is an easy exercise, so we limit ourselves to stating some easy results.

Lemma 8. *The ideal class group* $\mathcal{C}\ell(K)$ *of* K *is cyclic of order* 4 *and is generated by the class* $[\mathfrak{p}_2]$, *where* $\mathfrak{p}_2 = \left(2, \frac{1+\sqrt{-39}}{2}\right)$ *is a prime above* 2. *The class of the unique prime* $\mathfrak{p}_3 = (3, \sqrt{-39})$ *above* 3 *has order* 2. □

Also easy, but essential to this example, is the following observation.

Lemma 9. *The extension* $L : K$ *is unramified.*

Proof. Any prime ramifying in $L : \mathbb{Q}$ must ramify in at least one of the quadratic subextensions of $\mathbb{Q}$. The only finite primes ramifying in these quadratic extensions are 3 and 13, which both ramify in $K : \mathbb{Q}$. Since they can't ramify completely in $L : \mathbb{Q}$, as we've seen in section 2.2, they do not ramify in $L : K$. There are also no ramifying infinite primes, since the infinite prime of K is complex. So indeed $L : K$ is unramified. □

Finally we prove two lemmas in the more general setting of an arbitrary quadratic field K, so that we will be able to use them in the other examples as well.

Lemma 10. *Let $K = \mathbb{Q}(\sqrt{m})$ with $m \neq 1$ a square-free integer and let $\alpha \in K^*$ be an element of norm $\mathrm{N}_{\mathbb{Q}}^K(\alpha) = 1$. Let $\sigma \in \mathrm{Gal}(K : \mathbb{Q})$ be the non-trivial automorphism of K. Then there is a $\beta \in K^*$ such that $\alpha = \frac{\beta}{\sigma(\beta)}$.*

Proof. If $\alpha = -1$, we can take $\beta = \sqrt{m}$. Otherwise, take $\beta = \alpha + 1$: then $\sigma(\beta) = \sigma(\alpha) + 1$, so

$$\alpha\sigma(\beta) = \alpha\sigma(\alpha) + \alpha = 1 + \alpha = \beta$$

and indeed $\alpha = \frac{\beta}{\sigma(\beta)}$. □

> This lemma is actually a simple case of the more general theorem known as Hilbert's Theorem 90, which states that for a Galois extension $L : K$ with cyclic Galois group $\mathrm{Gal}(L : K) = \langle\sigma\rangle$ generated by σ, every $\alpha \in L^*$ of norm $\mathrm{N}_K^L(\alpha) = 1$ can be written as $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in L^*$. The name of this theorem comes from the fact that it is the 90th theorem in Hilbert's Zahlbericht [7], though the theorem was already published by Kummer in 1855 [11].

Lemma 11. *Let K be any quadratic number field. Then for every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we have $[\sigma(\mathfrak{a})]^{-1} = [\mathfrak{a}]$ in $\mathcal{C}\ell(K)$.*

Proof. For every fractional ideal $\mathfrak{a}$ we have $\mathfrak{a} \cdot \sigma(\mathfrak{a}) = \mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a})\mathcal{O}_K$, so $[\mathfrak{a}][\sigma(\mathfrak{a})] = 1$ and indeed $[\sigma(\mathfrak{a})]^{-1} = [\mathfrak{a}]$. □

For the field $K = \mathbb{Q}(\sqrt{-39})$ under consideration in this section, this leads to the following corollary:

Corollary 12. *For every ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the order of $\left[\frac{\mathfrak{a}}{\sigma(\mathfrak{a})}\right]$ in $\mathcal{C}\ell(K)$ is at most 2, and equals 2 if and only if the order of $[\mathfrak{a}]$ is 4.*

Proof. From Lemma 11 we know that $\left[\frac{\mathfrak{a}}{\sigma(\mathfrak{a})}\right] = [\mathfrak{a}]^2$. Since $\mathcal{C}\ell(K)$ is of order 4, the corollary immediately follows from this. □

We're now ready to prove the main part of the example, in which we show that 3 is not a norm of $L : \mathbb{Q}$.

Proposition 13. *In the extension $L : \mathbb{Q}$ the element 3 is a local norm at every prime of $\mathbb{Q}$, but not a global norm.*

Proof. We already saw in Lemma 7 that 3 is a local norm at every prime. It remains to be shown that 3 is not a norm of $L : \mathbb{Q}$. We will derive a contradiction by assuming it is.

Suppose there is a $\gamma \in L^*$ such that $\mathrm{N}_{\mathbb{Q}}^L(\gamma) = 3$. Consider the element $\alpha = \frac{3-\sqrt{-39}}{4} \in K^*$. It has norm $\mathrm{N}_{\mathbb{Q}}^K(\alpha) = \frac{3-\sqrt{-39}}{4} \cdot \frac{3+\sqrt{-39}}{4} = 3$. So $\mathrm{N}_{\mathbb{Q}}^L(\gamma) = \mathrm{N}_{\mathbb{Q}}^K(\mathrm{N}_K^L(\gamma)) = \mathrm{N}_{\mathbb{Q}}^K(\alpha)$ and

$$\mathrm{N}_{\mathbb{Q}}^K\left(\frac{\mathrm{N}_K^L(\gamma)}{\alpha}\right) = 1.$$

So by Lemma 10 there exists a $\beta \in K^*$ such that

$$\frac{\mathrm{N}_K^L(\gamma)}{\alpha} = \frac{\beta}{\sigma(\beta)},$$

so

$$\mathrm{N}_K^L(\gamma) = \frac{\alpha\beta}{\sigma(\beta)}. \tag{2.1}$$

Now consider the element $2\alpha = \frac{3-\sqrt{-39}}{2} \in \mathcal{O}_K$. It has norm $\mathrm{N}_{\mathbb{Q}}^K(2\alpha) = 12$ and is an element of the prime $\mathfrak{p}_2 = \left(2, \frac{1+\sqrt{-39}}{2}\right)$ above 2: $2\alpha = -\left(\frac{1+\sqrt{-39}}{2} - 2\right)$. Since the class of the unique prime $\mathfrak{p}_3$ above 3 has order 2 in $\mathcal{C}\ell(K)$, the two distinct primes above 2 can't both be factors of the principal ideal $2\alpha\mathcal{O}_K$: $[\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3] = [\mathfrak{p}_3] \neq 1$. Hence the prime factorization of $2\alpha\mathcal{O}_K$ is $\mathfrak{p}_2^2\mathfrak{p}_3$. So

$$\alpha\mathcal{O}_K = \frac{\mathfrak{p}_2^2\mathfrak{p}_3}{2\mathcal{O}_K} = \frac{\mathfrak{p}_2^2\mathfrak{p}_3}{\mathfrak{p}_2\mathfrak{p}_2'} = \frac{\mathfrak{p}_2\mathfrak{p}_3}{\sigma(\mathfrak{p}_2)}.$$

Hence

$$\frac{\alpha\beta}{\sigma(\beta)}\mathcal{O}_K = \mathfrak{p}_3\frac{\beta\mathfrak{p}_2}{\sigma(\beta\mathfrak{p}_2)}. \tag{2.2}$$

Since $[\mathfrak{p}_3]$ is of order 2 and $\frac{\alpha\beta}{\sigma(\beta)}\mathcal{O}_K$ is a principal fractional ideal, the order of $\left[\frac{\beta\mathfrak{p}_2}{\sigma(\beta\mathfrak{p}_2)}\right]$ is also 2. By Corollary 12 this means that $[\beta\mathfrak{p}_2]$ is of order 4 and thus that there is a prime ideal $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$ such that $[\mathfrak{p}]$ is of order 4, $v_{\mathfrak{p}}(\beta\mathfrak{p}_2)$ is odd and $v_{\sigma(\mathfrak{p})}(\beta\mathfrak{p}_2)$ is even. Due to its order in the ideal class group we see $\mathfrak{p} \neq \mathfrak{p}_3$, so also

$$v_{\mathfrak{p}}\left(\mathfrak{p}_3\frac{\beta\mathfrak{p}_2}{\sigma(\beta\mathfrak{p}_2)}\right) = v_{\mathfrak{p}}(\beta\mathfrak{p}_2) - v_{\mathfrak{p}}(\sigma(\beta\mathfrak{p}_2)) = v_{\mathfrak{p}}(\beta\mathfrak{p}_2) - v_{\sigma(\mathfrak{p})}(\beta\mathfrak{p}_2)$$

is odd. By equations 2.1 and 2.2 we conclude that $v_{\mathfrak{p}}(\mathrm{N}_K^L(\gamma))$ is odd.

However, since $L : K$ is unramified, by Corollary 3 of Artin's Reciprocity Law, we have a surjective homomorphism

$$\mathcal{C}\ell(K) \to \mathrm{Gal}(L : K).$$

Since the class $[\mathfrak{p}]$ is of order 4 and therefore generates the ideal class group $\mathcal{C}\ell(K)$, its image, the Frobenius automorphism $\varphi_{\mathfrak{p}}^{(L)}$ of $\mathfrak{p}$ in L, generates $\mathrm{Gal}(L : K)$. Since $\varphi_{\mathfrak{p}}^{(L)}$ also generates the decomposition group $Z_{\mathfrak{p}}^{(L)}$ of $\mathfrak{p}$ in L, we have $Z_{\mathfrak{p}}^{(L)} = \mathrm{Gal}(L : K)$. This means that $\mathfrak{p}$ does not split in $L : K$, and since $L : K$ is unramified, that implies that $\mathfrak{p}$ remains prime in L. Let $\mathfrak{q}$ denote the prime above $\mathfrak{p}$ in L, then

$$v_{\mathfrak{p}}(\mathrm{N}_K^L(\gamma)) = v_{\mathfrak{q}}(\gamma \cdot \sigma\tau(\gamma)) = v_{\mathfrak{q}}(\gamma) + v_{\mathfrak{q}}(\sigma\tau(\gamma)) = v_{\mathfrak{q}}(\gamma) + v_{\sigma\tau(\mathfrak{q})}(\gamma) = 2v_{\mathfrak{q}}(\gamma)$$

is even. Contradiction. □

2.4 Tate's Example: $\mathbb{Q}(\sqrt{13}, \sqrt{17})$

For this second example, let $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, $K = \mathbb{Q}(\sqrt{221})$ and $\mathrm{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau \rangle$ such that $L^\sigma = \mathbb{Q}(\sqrt{13})$ and $L^\tau = \mathbb{Q}(\sqrt{17})$. Again we also use the notation σ to indicate the restriction of $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ to K.

The example given by Tate is different not only in the way it was originally approached, but also in the sense that instead of providing one example, it gives an infinitely large class of numbers that are local norms everywhere, but not global norms. It was first published in 1973 in the form of an exercise [1]. Contrary to what is done there, we show that a similar approach as the one used in Hasse's example can be used to prove the result from the classical ideal theoretic point of view.

Two of the lemmas from the previous section, Lemma 6 and Lemma 9, translate directly to this situation: again $13 \equiv 17 \equiv 1 \pmod 4$ which implies that 13 and 17 are the only primes ramifying in L, and since $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1$ we see that 13 splits in $\mathbb{Q}(\sqrt{17})$ and 17 splits in $\mathbb{Q}(\sqrt{13})$. There are no ramifying infinite primes, so we have:

Lemma 14. *For every prime p of $\mathbb{Q}$ and $\mathfrak{q}$ a prime of L above p, the local extension $L_\mathfrak{q} : \mathbb{Q}_p$ is of degree 1 or 2. Furthermore, the extension $L : K$ is unramified.* □

The class of numbers this example is about, consists of squares of natural numbers. These are trivially local norms everywhere.

Lemma 15. *For every rational number $x \in \mathbb{Q}^*$, its square x^2 is a local norm of $L : \mathbb{Q}$ at every prime p of $\mathbb{Q}$.*

Proof. If $[L_\mathfrak{q} : \mathbb{Q}_p] = 1$, the norm of x^2 is x^2. If $[L_\mathfrak{q} : \mathbb{Q}_p] = 2$, it is the norm of x. □

In Hasse's example we made use of the ideal class group of $\mathbb{Q}(\sqrt{-39})$ being of order 4. In the current case however, $\mathcal{Cl}(K)$ is of order 2. Therefore we switch to using the narrow ideal class group $\mathcal{Cl}^+(K)$ instead. The narrow ideal class group is defined as $\mathcal{Cl}^+(K) = \mathbb{I}(K)/\mathbb{P}^+(K)$, where $\mathbb{P}^+(K)$ denotes the group of principal fractional ideals generated by an element of positive norm. In an imaginary quadratic number field all norms are positive, so the ideal class group and the narrow ideal class group coincide. For a real quadratic number field it depends on the norm of the fundamental unit. If that norm is -1, the principal fractional ideals that can be generated by an element of negative norm can also be generated by an element of positive norm, so also then the two groups coincide. If on the other hand the norm of the fundamental unit is 1, like in K, where the fundamental unit is $7 + \frac{1+\sqrt{221}}{2}$, the principal fractional ideals generated by an element of negative norm form a separate class, say C, and $\mathcal{Cl}(K) \cong \mathcal{Cl}^+(K)/C$. Then the order of $\mathcal{Cl}^+(K)$ is twice the order of $\mathcal{Cl}(K)$. In our case we have:

Lemma 16. *The narrow ideal class group $\mathcal{Cl}^+(K)$ is cyclic of order 4.*

Proof. $\mathcal{Cl}(K)$ is of order 2 and is generated by the class of $\mathfrak{p}_5 = \left(5, \frac{1+\sqrt{221}}{2}\right)$. We have $\mathfrak{p}_5^2 = \frac{11+\sqrt{221}}{2}\mathcal{O}_K$ and $\mathrm{N}_\mathbb{Q}^K\left(\frac{11+\sqrt{221}}{2}\right) = -25$, so combined with the observation that the fundamental unit has norm 1, we see that $[\mathfrak{p}_5]$ is of order 4 in $\mathcal{Cl}^+(K)$. □

The proof of Lemma 11 remains valid when substituting $\mathcal{C}\ell^+(K)$ for $\mathcal{C}\ell(K)$.

Lemma 17. *Let K be any quadratic number field. Then for every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we have $[\sigma(\mathfrak{a})]^{-1} = [\mathfrak{a}]$ in $\mathcal{C}\ell^+(K)$.* □

Another thing that needs to be adapted to this situation is what was shown in Lemma 10. In Proposition 13 we used an element of norm 3 to construct an element of norm 1 and apply Lemma 10 to it. In this case we won't be able to get such an element, but in Lemma 21 we will see that we're able to construct an ideal of the norm we're looking for instead.

Notation 18. The norm map $\mathrm{N}_{\mathbb{Q}}^K \colon \mathbb{I}(K) \to \mathbb{I}(\mathbb{Q})$ on fractional ideals of K takes values in $\mathbb{I}(\mathbb{Q})$. This group is isomorphic to the group $\mathbb{Q}^+$ of positive rationals. We will use this isomorphism to identify the norm of a fractional ideal of K with a positive rational. In particular for every $\alpha \in K^*$ we have $\mathrm{N}_{\mathbb{Q}}^K(\alpha\mathcal{O}_K) = \left|\mathrm{N}_{\mathbb{Q}}^K(\alpha)\right|$.

A similar result as Lemma 10 holds for ideals of norm 1.

Lemma 19. *Let K be any quadratic number field and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ of norm $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = 1$. Then there is a fractional ideal $\mathfrak{b}$ of $\mathcal{O}_K$ such that $\mathfrak{a} = \frac{\mathfrak{b}}{\sigma(\mathfrak{b})}$.*

Proof. Let $G = \mathrm{Gal}(K : \mathbb{Q})$ and consider the two G-module homomorphisms

$$\mathrm{N} \colon \mathbb{I}(K) \to \mathbb{I}(K), \quad \mathfrak{a} \mapsto \mathfrak{a}\sigma(\mathfrak{a})$$

and

$$\Delta \colon \mathbb{I}(K) \to \mathbb{I}(K), \quad \mathfrak{a} \mapsto \frac{\mathfrak{a}}{\sigma(\mathfrak{a})},$$

where $\mathbb{I}(K)$ denotes the G-module of fractional ideals of $\mathcal{O}_K$. It's easily seen that

$$\begin{aligned}
\ker(\mathrm{N}) &= \{\mathfrak{a} \in \mathbb{I}(K) \mid v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\sigma(\mathfrak{a})) = 0 \text{ for all } \mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)\} \\
&= \{\mathfrak{a} \in \mathbb{I}(K) \mid v_{\mathfrak{p}}(\mathfrak{a}) + v_{\sigma(\mathfrak{p})}(\mathfrak{a}) = 0 \text{ for all } \mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)\} \\
&= \{\mathfrak{a} \in \mathbb{I}(K) \mid v_{\mathfrak{p}}(\mathfrak{a}) = -v_{\sigma(\mathfrak{p})}(\mathfrak{a}) \text{ for all } \mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)\} \\
&= \mathrm{im}(\Delta).
\end{aligned}$$

So if $\mathrm{N}(\mathfrak{a}) = \mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = 1$ for some $\mathfrak{a} \in \mathbb{I}(K)$, then $\mathfrak{a} \in \mathrm{im}(\Delta)$, from which the lemma follows. □

> As with Lemma 10, this is an easy case of a more general result. In terms of Galois cohomology this result states that for a cyclic extension of number fields, the first cohomology group $H^1(\mathbb{I}(K))$ is trivial.

The following observation is the basis for the class of numbers this example is about.

Lemma 20. *Let p be a prime number with $\left(\frac{p}{13}\right) = \left(\frac{p}{17}\right) = -1$. Then p splits in K: $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, and the order of $[\mathfrak{p}]$ in $\mathcal{C}\ell^+(K)$ is 4.*

Proof. Firstly, since $\left(\frac{2}{17}\right) = 1$, p must be odd. Then $\left(\frac{221}{p}\right) = \left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{p}{13}\right)\left(\frac{p}{17}\right) = 1$, so p splits in K.

Suppose $\mathfrak{p}$ is a principal ideal. Then there are $a, b \in \mathbb{Z}$ such that $\mathfrak{p}$ is generated by $\frac{a+b\sqrt{221}}{2} \in \mathcal{O}_K$. Since $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{p}) = p$, we have $\mathrm{N}_{\mathbb{Q}}^K(\frac{a+b\sqrt{221}}{2}) = \pm p$, so $a^2 \pm 4p = 13 \cdot 17b^2$ and thus

$$\left(\frac{13}{p}\right) = \left(\frac{13 \cdot 17b^2}{p}\right) = \left(\frac{a^2 \pm 4p}{p}\right) = 1,$$

which is a contradiction with $\left(\frac{p}{13}\right) = -1$. So $\mathfrak{p}$ is not a principal ideal.

Since in $\mathcal{C}\ell^+(K)$ the trivial class consists of all principal ideals generated by an element with a positive norm, and the class of order 2 consists of the principal ideals generated by an element with a negative norm, $\mathfrak{p}$ must be in a class of order 4. □

We're now ready to prove the result the example is about. In the following lemma we define the class of squares that are not global norms and construct the ideal we announced before Notation 18. Then in Proposition 22 we conclude the proof.

Lemma 21. *Let $a \in \mathbb{N}\setminus\{0\}$ be a number such that $\left(\frac{p}{13}\right) = -1$ for all $p \mid a$, and $\left(\frac{a}{17}\right) = -1$. Then there exists an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ of norm $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = a^2$ such that the order of $[\mathfrak{a}] \in \mathcal{C}\ell^+(K)$ is 2.*

Proof. Write $a = p_1 \cdots p_n q_1 \cdots q_m$ so that $\left(\frac{p_i}{17}\right) = -1$ and $\left(\frac{q_j}{17}\right) = 1$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Then n is odd, since $\left(\frac{a}{17}\right) = -1$.

According to Lemma 20, every p_i splits in K as $p_i\mathcal{O}_K = \mathfrak{p}_i\mathfrak{p}_i'$ with $[\mathfrak{p}_i]$ of order 4.

Since 2 remains prime in K and for every odd q_j we have

$$\left(\frac{221}{q_j}\right) = \left(\frac{13}{q_j}\right)\left(\frac{17}{q_j}\right) = \left(\frac{q_j}{13}\right)\left(\frac{q_j}{17}\right) = -1,$$

every q_j remains prime in K. So every $[q_j\mathcal{O}_K]$ is trivial in $\mathcal{C}\ell^+(K)$.

Then

$$\mathfrak{a} = \mathfrak{p}_1^2 \cdots \mathfrak{p}_n^2 q_1\mathcal{O}_K \cdots q_m\mathcal{O}_K$$

has norm $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = a^2$ and $[\mathfrak{a}] = [\mathfrak{p}_1^2 \cdots \mathfrak{p}_n^2]$ is the unique class of $\mathcal{C}\ell^+(K)$ of order 2 due to n being odd. □

Proposition 22. *Let $a \in \mathbb{N} \setminus \{0\}$ be as in Lemma 21. Then a^2 is not a global norm of $L : \mathbb{Q}$.*

Proof. Suppose there is a $\gamma \in L^*$ such that $\mathrm{N}_{\mathbb{Q}}^L(\gamma) = a^2$. Let $\mathfrak{a}$ be the ideal of $\mathcal{O}_K$ with norm $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = a^2$ such that the order of $[\mathfrak{a}]$ in $\mathcal{C}\ell^+(K)$ is 2, as constructed in Lemma 21. Then $\mathrm{N}_{\mathbb{Q}}^L(\gamma\mathcal{O}_L) = \mathrm{N}_{\mathbb{Q}}^K(\mathrm{N}_K^L(\gamma\mathcal{O}_L)) = a^2 = \mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a})$, so

$$\mathrm{N}_{\mathbb{Q}}^K\left(\frac{\mathfrak{a}}{\mathrm{N}_K^L(\gamma\mathcal{O}_L)}\right) = 1.$$

By Lemma 19 there is a fractional ideal $\mathfrak{b} \in \mathbb{I}(K)$ such that

$$\frac{\mathfrak{a}}{\mathrm{N}_K^L(\gamma\mathcal{O}_L)} = \frac{\mathfrak{b}}{\sigma(\mathfrak{b})}.$$

Since $\mathrm{N}_K^L(\gamma\mathcal{O}_L)$ represents the trivial class of $\mathcal{Cl}^+(K)$ and $[\sigma(\mathfrak{b})]^{-1} = [\mathfrak{b}]$ by Lemma 17, we have $[\mathfrak{a}] = [\mathfrak{b}]^2$. From this it follows that the order of $[\mathfrak{b}]$ is 4.

Then there must be a prime ideal $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$ such that $[\mathfrak{p}]$ is of order 4, $v_\mathfrak{p}(\mathfrak{b})$ is odd and $v_{\sigma(\mathfrak{p})}(\mathfrak{b})$ is even. Since all prime factors of $\mathfrak{a}$ either represent the trivial class of $\mathcal{Cl}^+(K)$, or appear an even number of times in the decomposition of $\mathfrak{a}$, also

$$v_\mathfrak{p}(\mathrm{N}_K^L(\gamma\mathcal{O}_L)) = v_\mathfrak{p}\left(\frac{\mathfrak{a}\mathfrak{b}}{\sigma(\mathfrak{b})}\right) = v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b}) - v_\mathfrak{p}(\sigma(\mathfrak{b})) = v_{\sigma(\mathfrak{p})}(\mathfrak{b})$$

is odd.

However, now $L : K$ is unramified and $[\mathfrak{p}]$ generates $\mathcal{Cl}^+(K)$. The surjective homomorphism $\mathcal{Cl}(K) \to \mathrm{Gal}(L : K)$ we get from Corollary 3 combined with the surjection $\mathcal{Cl}^+(K) \to \mathcal{Cl}(K), [\mathfrak{a}] \mapsto [\mathfrak{a}]$ yields a surjective homomorphism $\mathcal{Cl}^+(K) \to \mathrm{Gal}(L : K)$ generated by sending the prime ideals of $\mathcal{O}_K$ to their Frobenius automorphisms of L. So using similar reasoning as in Proposition 13, we see that the Frobenius automorphism $\varphi_\mathfrak{p}^{(L)}$ generates $\mathrm{Gal}(L : K)$ and thus that $\mathfrak{p}$ remains prime in L. So $v_\mathfrak{p}(\mathrm{N}_K^L(\gamma\mathcal{O}_L))$ is even, which is a contradiction. □

3. Extension to $\mathbb{Q}(\sqrt{p}, \sqrt{q})$

In this chapter we will generalize Tate's example to $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, where p and q are prime numbers with $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. In both previous examples we relied heavily on the structure of the (narrow) ideal class group. To be able to obtain similar results in this more general setting, we need some information about the narrow ideal class group again. Specifically, we need to know the 2-rank and the 4-rank of this group. We define this in an intuitive way.

Definition 23. Let A be a finite abelian group. Then A is isomorphic to a product of cyclic groups

$$A \cong \prod_{i=1}^{k} C_{d_i}.$$

Requiring that $d_{i+1} \mid d_i$ for $1 \leq i < k$ and $d_k \neq 1$ yields a unique decomposition of A into cyclic groups. The d_i are then called the group invariants of A. The 2^n-rank of A, for an $n \in \mathbb{N} \setminus \{0\}$, is the number of group invariants divisible by 2^n.

We will prove the classic theorem on the 2-rank of the narrow ideal class group of a quadratic number field and use that to also determine the 4-rank in our specific situation. To make computations easier, we also introduce a basic version of Hilbert symbols.

3.1 Hilbert symbols

First introduced in 1897 in Hilbert's Zahlbericht [7], the Hilbert symbol started out as a function of two rational integers and a rational prime. Over time it developed into an essential part of class field theory, growing more complex along the way. The general Hilbert symbols are defined on local fields containing sufficiently many roots of unity, and use the local Artin map in their definition. We won't be needing any of this here, so we restrict ourselves to the classical quadratic Hilbert symbol. Since we will only make very limited use of this symbol to simplify some calculations, we won't go into too many details and simply present the definition and some results on how to use and calculate them.

Though Hilbert's original definition would be sufficient for our purpose, we use a slightly evolved version that can be found in Serre's Cours d'Arithmetique [15]. This allows for some easier arguments.

In this section, let F be a completion of $\mathbb{Q}$ at a prime p. So $F = \mathbb{Q}_p$ when p is a prime number and for $p = \infty$ we have $F = \mathbb{R}$.

Definition 24. Let $a, b \in F^*$. We define the Hilbert symbol of a and b relative to F to be

$$(a,b) = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a solution } (z,x,y) \neq (0,0,0) \text{ in } F^3, \\ -1 & \text{otherwise.} \end{cases}$$

The idea behind this definition becomes clear in the following proposition.

Proposition 25. *For $a, b \in F^*$ we have*

$$(a,b) = 1 \iff a \in \mathrm{N}_F^{F(\sqrt{b})}(F(\sqrt{b})^*).$$

So $(a,b) = 1$ precisely when a is the norm of some element in $F(\sqrt{b})^*$.

Proof. First suppose b is a square in F, say $b = c^2$ for some $c \in F^*$. Then $z^2 - ax^2 - by^2 = 0$ has a solution $(c, 0, 1)$, so $(a,b) = 1$ for any a. Also $F(\sqrt{b}) = F$, so any $a \in F^*$ is simply the norm of itself.

If b is not a square in F, then $F(\sqrt{b}) : F$ is a quadratic field extension. Then every element $\alpha \in F(\sqrt{b})$ can be written as $\alpha = z + y\sqrt{b}$, with $z, y \in F$. So then $\mathrm{N}_F^{F(\sqrt{b})}(\alpha) = z^2 - by^2$. So if a is a norm there are $z, y \in F$ such that $a = z^2 - by^2$, making $(z, 1, y)$ a solution to $z^2 - ax^2 - by^2 = 0$, and thus $(a,b) = 1$.

Conversely, if $(a,b) = 1$, then $z^2 - ax^2 - by^2 = 0$ has a solution $(z,x,y) \neq (0,0,0)$. Since b is not a square, we have $x \neq 0$ and a is the norm of $\frac{z}{x} + \frac{y}{x}\sqrt{b}$:

$$\begin{aligned} 0 &= z^2 - ax^2 - by^2, \\ ax^2 &= z^2 - by^2, \\ a &= \left(\frac{z}{x}\right)^2 - b\left(\frac{y}{x}\right)^2. \end{aligned}$$

□

In this thesis we will only be using a particular kind of Hilbert symbols, where the a and b are actually rational integers. When restricted to the rationals, all Hilbert symbols relative to different F can be described by a single symbol.

Notation 26. Let $a, b \in \mathbb{Q}^*$ and p a prime of $\mathbb{Q}$. Let F be the completion of $\mathbb{Q}$ at p. We will use the notation

$$\left(\frac{a,b}{p}\right) = (a,b),$$

where (a,b) is the Hilbert symbol of a and b relative to F. We call this restriction of (a,b) the Hilbert symbol on $\mathbb{Q}$ relative to p.

The Hilbert symbol satisfies a number of identities, such as $(a,b) = (b,a)$ and $(a,-a) = 1$, that can be derived directly from the definition. These identities lead to formulas that allow actual calculation of the symbol. Since we are only interested in the case where a and b are integers, we state the theorem only for that case, simplifying the formulation.

Theorem 27. *Let p be a prime number and let $a, b \in \mathbb{Z} \setminus \{0\}$. Write $a = p^m c$, $b = p^n d$, where $m, n \in \mathbb{Z}$ and $c, d \in \mathbb{Z} \setminus \{0\}$ such that c and d are relatively prime to p. Then for odd p:*

$$\left(\frac{a,b}{p}\right) = (-1)^{mn\frac{p-1}{2}} \left(\frac{c^n d^m}{p}\right),$$

and for $p = 2$:

$$\left(\frac{a,b}{2}\right) = (-1)^{\frac{c-1}{2}\frac{d-1}{2} + n\frac{c^2-1}{8} + m\frac{d^2-1}{8}}.$$

Furthermore, for the infinite prime ∞ and $a, b \in \mathbb{Z} \setminus \{0\}$:

$$\left(\frac{a,b}{\infty}\right) = \begin{cases} -1 & \text{if } a, b < 0 \\ 1 & \text{otherwise.} \end{cases}$$

For a proof of the theorem we refer to the book by Serre [15], Theorem 1 of Chapter III. As the title of the book suggests, the proof requires a lot, though relatively basic, arithmetic and case distinctions, which does not add any additional insights in the subject of this thesis.

3.2 The 2-rank of the Narrow Ideal Class Group of a Quadratic Number Field

Even though field extensions weren't considered in those days, the theorem on the 2-rank of the narrow ideal class group of a quadratic field extension of $\mathbb{Q}$ dates all the way back to Gauss's Disquisitiones Arithmeticae [3], written in 1798 at age 21 and published in 1801, where he introduced genus theory. In the context of quadratic forms he proves the principal genus theorem. Through work of famous mathematicians like Dirichlet and Hilbert, the theory evolves from quadratic forms to quadratic field extensions of $\mathbb{Q}$. A complete account on this development of the principal genus theorem was written by Franz Lemmermeyer [12].

In this context, genus theory resulted in the theorem on the 2-rank of the narrow ideal class group through two key theorems – the principal genus theorem and the main theorem on genera. While this theory is interesting and it's history fascinating, as a part of this thesis it would require too many new tools. Instead we prove the theorem in a way based on the proof in the book Algebraic Number Theory by Fröhlich and Taylor [2]. This way

the proof fits very well within the theory we have already been using. For a detailed proof using genus theory we recommend Hasse's Number Theory [6].

For this theorem we will make use of the notion of a totally positive element:

Definition 28. Let L be a number field and $\alpha \in L^*$. We call α totally positive if it is positive under every real embedding of L into $\mathbb{R}$. We use the notation L^+ to denote the multiplicative group of totally positive elements of L.

Let K be any quadratic number field with $\mathrm{Gal}(K:\mathbb{Q}) = \langle\sigma\rangle$ and denote by P the set of prime ideals of $\mathcal{O}_K$ that are ramified in K. In other words, P contains the primes of K above the prime numbers dividing the discriminant of K. Let S be the group of fractional ideals of $\mathcal{O}_K$ of the form $\prod_{\mathfrak{p}\in P}\mathfrak{p}^{a_\mathfrak{p}}$, where the $a_\mathfrak{p}$ are integers. Let us first formulate a simple lemma concerning this group.

Lemma 29. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ such that $\mathfrak{a} = \sigma(\mathfrak{a})$. Then there exist an $r \in \mathbb{Q}^+$ and a square-free $\mathfrak{a}' \in S$ such that $\mathfrak{a} = r\mathfrak{a}'$.*

Proof. Write $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$, where the product ranges over the non-zero prime ideals of $\mathcal{O}_K$. For a given prime ideal $\mathfrak{p}$, let p be the prime number below $\mathfrak{p}$. If p remains prime in K, then obviously $\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} = (p\mathcal{O}_K)^{v_\mathfrak{p}(\mathfrak{a})}$. If p splits in K, then since $v_\mathfrak{p}(\mathfrak{a}) = v_\mathfrak{p}(\sigma(\mathfrak{a})) = v_{\sigma(\mathfrak{p})}(\mathfrak{a})$, we get $\prod_{\mathfrak{p}|p}\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} = (p\mathcal{O}_K)^{v_\mathfrak{p}(\mathfrak{a})}$. Finally for ramifying p, if $v_\mathfrak{p}(\mathfrak{a})$ is even, then $\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} = (p\mathcal{O}_K)^{\frac{v_\mathfrak{p}(\mathfrak{a})}{2}}$ and if it is odd, then $\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} = p^{\frac{v_\mathfrak{p}(\mathfrak{a})-1}{2}}\mathfrak{p}$. □

We define a group homomorphism

$$\varphi\colon S \to \mathcal{C}\ell^+(K), \quad \mathfrak{a} \mapsto [\mathfrak{a}]\,.$$

Since for every $\mathfrak{p}$ in P we have $[\mathfrak{p}]^2 = [p\mathcal{O}_K] = 1$, it is immediately clear that $\mathrm{im}(\varphi) \subseteq {}_2\mathcal{C}\ell^+(K)$, where ${}_2\mathcal{C}\ell^+(K)$ denotes the subgroup of $\mathcal{C}\ell^+(K)$ consisting of elements whose order divides 2. Furthermore we see that $S^2 \subseteq \ker(\varphi)$, which follows from the same observation. So φ induces a homomorphism

$$\varphi'\colon S/S^2 \to {}_2\mathcal{C}\ell^+(K).$$

Theorem 30. *The homomorphism $\varphi'\colon S/S^2 \to {}_2\mathcal{C}\ell^+(K)$ is surjective and its kernel is of order 2.*

Proof. For the surjectivity of φ', let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ and suppose for its class $[\mathfrak{a}]$ in $\mathcal{C}\ell^+(K)$ we have $[\mathfrak{a}]^2 = 1$. As we've seen in Lemma 17, $[\mathfrak{a}]^{-1} = [\sigma(\mathfrak{a})]$, so

$$\frac{[\mathfrak{a}]}{[\sigma(\mathfrak{a})]} = [\mathfrak{a}]^2 = 1.$$

This means that there is an $\alpha \in K$ of positive norm such that $\frac{\mathfrak{a}}{\sigma(\mathfrak{a})} = \alpha\mathcal{O}_K$. Hence

$$\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)\mathcal{O}_K = \alpha \cdot \sigma(\alpha)\mathcal{O}_K = \frac{\mathfrak{a}}{\sigma(\mathfrak{a})} \cdot \sigma\left(\frac{\mathfrak{a}}{\sigma(\mathfrak{a})}\right) = \mathcal{O}_K.$$

Because the norm of α is positive, we can conclude that $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = 1$. So by Lemma 10 there is a $\beta \in K^*$ such that $\alpha = \frac{\beta}{\sigma(\beta)}$. The signs of these β and $\sigma(\beta)$ need to be equal under every embedding in $\mathbb{R}$, so by substituting β for $-\beta$ if necessary, we may assume β to be totally positive. Now we have $\frac{\mathfrak{a}}{\sigma(\mathfrak{a})} = \alpha\mathcal{O}_K = \frac{\beta}{\sigma(\beta)}\mathcal{O}_K$ and thus

$$\mathfrak{a} \cdot \sigma(\beta) = \sigma(\mathfrak{a}) \cdot \beta = \sigma(\mathfrak{a} \cdot \sigma(\beta)).$$

By Lemma 29 there exist $r \in \mathbb{Q}^+$ and square-free $\mathfrak{a}' \in S$ such that $\mathfrak{a} \cdot \sigma(\beta) = \mathfrak{a}'r$. So by construction we get

$$\varphi(\mathfrak{a}') = [\mathfrak{a}'] = \left[\mathfrak{a} \cdot \frac{\sigma(\beta)}{r}\right] = [\mathfrak{a}],$$

showing that indeed φ' is surjective.

To prove that the kernel of $\varphi' \colon S/S^2 \to {}_2\mathcal{C}\ell^+(K)$ is of order 2, we note that $\ker(\varphi') \cong \ker(\varphi)/S^2$ and work with that instead. The plan is to show that

$$\ker(\varphi)/S^2 \cong \mathcal{O}_K^+/(\mathcal{O}_K^+)^2, \tag{3.1}$$

where $\mathcal{O}_K^+$ denotes the subgroup of totally positive units of the group $\mathcal{O}_K^*$ of multiplicative units of $\mathcal{O}_K$. It's easily seen that $[\mathcal{O}_K^+ : (\mathcal{O}_K^+)^2] = 2$ as required: for imaginary K there are no real embeddings, so $\mathcal{O}_K^+ = \mathcal{O}_K^* = \mu_K$, where μ_K is the group of roots of unity of K. Since $-1 \in \mu_K$, we see $[\mu_K : \mu_K^2] = 2$. For K real, $\mathcal{O}_K^+$ is an infinite cyclic group, so also then $[\mathcal{O}_K^+ : (\mathcal{O}_K^+)^2] = 2$.

In order to prove equation 3.1, we define a homomorphism by

$$\psi \colon \ker(\varphi) \to \mathcal{O}_K^+/(\mathcal{O}_K^+)^2, \quad \mathfrak{a} \mapsto \frac{\alpha}{\sigma(\alpha)}(\mathcal{O}_K^+)^2,$$

where $\alpha \in K^+$ is such that $\mathfrak{a} = \alpha\mathcal{O}_K$.

We first need to show that this is actually well-defined, after which we will show that ψ is surjective and has S^2 as its kernel, which will conclude the proof.

Let $\mathfrak{a} \in \ker(\varphi)$, then there is an $\alpha \in K^+$ such that $\mathfrak{a} = \alpha\mathcal{O}_K$. Since $\mathfrak{a} \in S$, we have $\mathfrak{a} = \sigma(\mathfrak{a})$, and thus $\frac{\alpha}{\sigma(\alpha)}\mathcal{O}_K = \frac{\mathfrak{a}}{\sigma(\mathfrak{a})} = \mathcal{O}_K$, so $\frac{\alpha}{\sigma(\alpha)} \in \mathcal{O}_K^* \cap K^+ = \mathcal{O}_K^+$. This α however is only unique up to a totally positive multiplicative unit. Let $\nu \in \mathcal{O}_K^+$ be such a unit, then $\nu\sigma(\nu) = \mathrm{N}_{\mathbb{Q}}^{K}(\nu) = 1$, so

$$\frac{\nu}{\sigma(\nu)} = \frac{\nu}{\sigma(\nu)}\nu\sigma(\nu) = \nu^2. \tag{3.2}$$

So as required,

$$\frac{\alpha}{\sigma(\alpha)} \equiv \frac{\alpha\nu}{\sigma(\alpha\nu)} \pmod{(\mathcal{O}_K^+)^2}$$

and we see that ψ is well-defined.

To show that $\ker(\psi) = S^2$, let $\mathfrak{a} \in S$. We have $\mathfrak{a}^2 = r\mathcal{O}_K$ for some $r \in \mathbb{Q}^+$, so since $\frac{r}{\sigma(r)} = 1$ we see that $\psi(\mathfrak{a}^2)$ is trivial and indeed $S^2 \subseteq \ker(\psi)$. Conversely, let $\mathfrak{a} \in \ker(\psi)$. In other words, $\mathfrak{a} \in S$ and $\mathfrak{a} = \alpha\mathcal{O}_K$ for an $\alpha \in K^+$ with $\frac{\alpha}{\sigma(\alpha)} \in (\mathcal{O}_K^+)^2$. So we have $\frac{\alpha}{\sigma(\alpha)} = \nu^2$ for some $\nu \in \mathcal{O}_K^+$. Just as in 3.2 we have $\nu^2 = \frac{\nu}{\sigma(\nu)}$, so

$$\frac{\alpha}{\sigma(\alpha)} = \nu^2 = \frac{\nu}{\sigma(\nu)}$$

and thus $\frac{\alpha}{\nu} = \sigma\left(\frac{\alpha}{\nu}\right)$, which implies $\frac{\alpha}{\nu} \in \mathbb{Q}^+$. Hence $\mathfrak{a} = \alpha\mathcal{O}_K = \frac{\alpha}{\nu}\mathcal{O}_K$, from which it follows that $v_\mathfrak{p}(\mathfrak{a})$ is even for all $\mathfrak{p} \in P$. So $\mathfrak{a} \in S^2$ and indeed $\ker(\psi) = S^2$.

Finally, for the surjectivity of ψ, let $\nu \in \mathcal{O}_K^+$. Then $\mathrm{N}_\mathbb{Q}^K(\nu) = 1$, so by Lemma 10 there is an $\alpha \in K^*$ such that $\nu = \frac{\alpha}{\sigma(\alpha)}$. Since ν is totally positive, α and $\sigma(\alpha)$ need to be of the same sign, so as before we may assume that α is totally positive. Then $\sigma(\alpha)\mathcal{O}_K = \nu\sigma(\alpha)\mathcal{O}_K = \alpha\mathcal{O}_K$, so we can apply Lemma 29. But because we're applying it to a principal fractional ideal here, there are $\alpha' \in K^+$ and $r \in \mathbb{Q}^+$ such that $\alpha\mathcal{O}_K = \alpha' r\mathcal{O}_K$ and $\alpha'\mathcal{O}_K \in S$. So $\alpha = \alpha' r\mu$ for some $\mu \in \mathcal{O}_K^+$, and thus by equation 3.2

$$\nu = \frac{\alpha}{\sigma(\alpha)} = \frac{\alpha' r\mu}{\sigma(\alpha' r\mu)} = \frac{\alpha'}{\sigma(\alpha')}\mu^2.$$

Hence $\psi(\alpha'\mathcal{O}_K) = \frac{\alpha}{\sigma(\alpha)}(\mathcal{O}_K^+)^2 = \nu(\mathcal{O}_K^+)^2$ as required. □

Corollary 31. *The 2-rank of $\mathcal{C}\ell^+(K)$ is $t-1$, where t denotes the number of distinct primes dividing the discriminant of K.*

Proof. The order of S/S^2 is 2^t, so by Theorem 30 we see that ${}_2\mathcal{C}\ell^+(K)$ is of order 2^{t-1}. This means it is isomorphic to C_2^{t-1} and thus that the 2-rank of $\mathcal{C}\ell^+(K)$ is $t-1$. □

Corollary 32. *For $K = \mathbb{Q}(\sqrt{pq})$ with distinct primes $p, q \equiv 1 \pmod 4$ the 2-rank is* $\mathrm{rk}_2(\mathcal{C}\ell^+(K)) = 1$. □

3.3 The 4-rank of the Narrow Ideal Class Group of $\mathbb{Q}(\sqrt{pq})$

In addition to the 2-rank, we also need the 4-rank of the narrow ideal class group. The 4-rank of the narrow ideal class group of general quadratic number fields was first established in 1934 in an article by Rédei and Reichardt [13]. We however only need a special case, and have already seen that the fields K that we're working with have $\mathrm{rk}_2(\mathcal{C}\ell^+(K)) = 1$. We'll show directly that for these fields we have $\mathrm{rk}_4(\mathcal{C}\ell^+(K)) = 1$.

Let $K = \mathbb{Q}(\sqrt{pq})$ with primes $p, q \equiv 1 \pmod 4$ such that $\left(\frac{p}{q}\right) = 1$. Then as we saw in Corollary 32, $\mathrm{rk}_2(\mathcal{C}\ell^+(K)) = 1$. This means that the 4-rank of $\mathcal{C}\ell^+(K)$ must be either 0 or 1, depending on whether or not the unique class of order 2 is a square.

We start with a lemma that will allow us to quickly prove the main result afterwards.

Lemma 33. *The primes p and q are norms of K.*

Proof. Due to symmetry, it suffices to show this for p. The Hasse Norm Theorem tells us that p is a norm of $K : \mathbb{Q}$ if and only if it is a norm locally at every prime of $\mathbb{Q}$. Using Theorem 27 on Hilbert symbols, we see that

$$\left(\frac{p, pq}{r}\right) = \left(\frac{1}{r}\right) = 1$$

for all odd prime numbers $r \neq p, q$. Also

$$\left(\frac{p, pq}{2}\right) = (-1)^{\frac{p-1}{2}\frac{pq-1}{2}} = 1 \text{ and } \left(\frac{p, pq}{\infty}\right) = 1.$$

Furthermore, using Theorem 27 again,

$$\left(\frac{p, pq}{p}\right) = \left(\frac{q}{p}\right) = 1 \text{ and } \left(\frac{p, pq}{q}\right) = \left(\frac{p}{q}\right) = 1.$$

So with Proposition 25, p is a norm locally at every prime and thus a norm of $K : \mathbb{Q}$. □

Lemma 34. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be the primes of K above p and q respectively. Then $[\mathfrak{p}]$ and $[\mathfrak{q}]$ are squares in $\mathcal{C}\ell^+(K)$.*

Proof. We again only need to consider $[\mathfrak{p}]$. By Lemma 33, p is a norm, say $\mathrm{N}_{\mathbb{Q}}^K(\alpha) = p$ for some $\alpha \in K^*$. Then since α has a positive norm, $[\mathfrak{p}] = \left[\frac{\mathfrak{p}}{\alpha}\right]$ in $\mathcal{C}\ell^+(K)$. Because $\mathrm{N}_{\mathbb{Q}}^K(\frac{\mathfrak{p}}{\alpha}) = 1$, Lemma 19 then implies $\frac{\mathfrak{p}}{\alpha} = \frac{\mathfrak{b}}{\sigma(\mathfrak{b})}$ for some fractional ideal $\mathfrak{b}$ of $\mathcal{O}_K$. So by Lemma 17

$$[\mathfrak{p}] = \left[\frac{\mathfrak{p}}{\alpha}\right] = \left[\frac{\mathfrak{b}}{\sigma(\mathfrak{b})}\right] = [\mathfrak{b}]^2.$$ □

Corollary 35. *Let $K = \mathbb{Q}(\sqrt{pq})$ with primes $p, q \equiv 1 \pmod 4$ such that $\left(\frac{p}{q}\right) = 1$. Then the 4-rank of $\mathcal{C}\ell^+(K)$ is $\mathrm{rk}_4(\mathcal{C}\ell^+(K)) = 1$.*

Proof. In Theorem 30 we've seen that $\mathrm{im}(\varphi') = {}_2\mathcal{C}\ell^+(K)$ and that for this specific $K = \mathbb{Q}(\sqrt{pq})$ the order of this last group is 2. It follows that not all of $[\mathfrak{p}]$, $[\mathfrak{q}]$ and $[\mathfrak{pq}]$ are trivial, where $\mathfrak{p}$ and $\mathfrak{q}$ denote the primes above p and q respectively. So either $[\mathfrak{p}]$ or $[\mathfrak{q}]$ is not trivial. By Lemma 34 these classes are both squares, and since both $[\mathfrak{p}]^2 = [p\mathcal{O}_K] = 1$ and $[\mathfrak{q}]^2 = [q\mathcal{O}_K] = 1$, at least one of them is the square of a class of order 4. □

3.4 $\mathbb{Q}(\sqrt{p}, \sqrt{q})$

Finally, for this generalization of Tate's example, set $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, where p and q are prime numbers with $p \equiv q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. Similar to what we did before, set $\mathrm{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau \rangle$ such that $L^\sigma = \mathbb{Q}(\sqrt{p})$, $L^\tau = \mathbb{Q}(\sqrt{q})$ and $K = L^{\sigma\tau} = \mathbb{Q}(\sqrt{pq})$.

Our choice for p and q being congruent 1 modulo 4 is made so that the initial results in Tate's example in section 2.4 still hold true. In the same way as we did there, one obtains:

Lemma 36. *All completions of $L : \mathbb{Q}$ are of degree ≤ 2, the extension $L : K$ is unramified and x^2 is a local norm of $L : \mathbb{Q}$ at every prime for all $x \in \mathbb{Q}^*$.* □

In Lemma 21 of section 2.4 about Tate's example we defined a class of numbers $a \in \mathbb{N}\backslash\{0\}$ whose squares are not global norms. For such an a we constructed an ideal $\mathfrak{a}$ of norm $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = a^2$ whose class in the narrow ideal class group had order 2. The next four lemmas show that we can obtain a similar result in the current setting, without knowing the order of $\mathcal{C}\ell^+(K)$.

For these four lemmas, let r be a prime number such that $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = -1$.

Lemma 37. *The prime number r splits in K: $r\mathcal{O}_K = \mathfrak{r}\mathfrak{r}'$.*

Proof. If $r = 2$ we have $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = -1$, which only occurs when $p, q \equiv 5 \pmod 8$. Then $pq \equiv 1 \pmod 8$ and so 2 splits in K.

For odd r we have $\left(\frac{pq}{r}\right) = \left(\frac{r}{p}\right)\left(\frac{r}{q}\right) = 1$, also implying that r splits in K. □

Lemma 38. *The prime number r is not a norm of $K : \mathbb{Q}$.*

Proof. By the Hasse Norm Theorem, r is a norm of $K : \mathbb{Q}$ if and only if it is a norm locally at every prime. With Hilbert symbols we can easily show, using Theorem 27, that r is not a local norm at p:

$$\left(\frac{r, pq}{p}\right) = \left(\frac{r}{p}\right) = -1.$$

So indeed r is not a norm of $K : \mathbb{Q}$. □

Lemma 39. *Let $\mathfrak{r}$ be a prime of K above r. Then $[\mathfrak{r}]$ is not a square in $\mathcal{C}\ell^+(K)$.*

Proof. Suppose $[\mathfrak{r}]$ is a square in $\mathcal{C}\ell^+(K)$, say $[\mathfrak{r}] = [\mathfrak{a}]^2$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_K$. By Lemma 17 we have $[\mathfrak{a}] = [\sigma(\mathfrak{a})]^{-1}$, so

$$[\mathfrak{r}] = \left[\frac{\mathfrak{a}}{\sigma(\mathfrak{a})}\right].$$

So there exists an $\alpha \in K$ of positive norm such that $\mathfrak{r} = \alpha\frac{\mathfrak{a}}{\sigma(\mathfrak{a})}$. But $\frac{\mathfrak{a}}{\sigma(\mathfrak{a})}$ has norm 1, so

$$r = \mathrm{N}_{\mathbb{Q}}^K(\mathfrak{r}) = \mathrm{N}_{\mathbb{Q}}^K\left(\alpha\frac{\mathfrak{a}}{\sigma(\mathfrak{a})}\right) = \mathrm{N}_{\mathbb{Q}}^K(\alpha\mathcal{O}_K).$$

So $\mathrm{N}_{\mathbb{Q}}^K(\alpha) = r$, which contradicts Lemma 38. □

Lemma 40. *Let $a \in \mathbb{N} \setminus \{0\}$ be a product of prime numbers such that $\left(\frac{r}{p}\right) = -1$ for all prime divisors $r \mid a$, and $\left(\frac{a}{q}\right) = -1$. Then there exists an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ with norm $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = a^2$, such that $[\mathfrak{a}]$ is not a fourth power in $\mathcal{C}\ell^+(K)$.*

Proof. Write $a = r_1 \cdots r_n s_1 \cdots s_m$, where r_i and s_j are prime numbers such that $\left(\frac{r_i}{q}\right) = -1$ and $\left(\frac{s_j}{q}\right) = 1$ for all $1 \le i \le n$ and $1 \le j \le m$. Then n is odd, since $\left(\frac{a}{q}\right) = -1$.

By Lemma 37, each r_i splits in K: $r\mathcal{O}_K = \mathfrak{r}_i\mathfrak{r}_i'$, and by Lemma 39 the classes of these $\mathfrak{r}_i$ are not squares in $\mathcal{C}\ell^+(K)$.

Every s_j remains prime in K: $s_j = 2$ is only possible when $p \equiv 5 \pmod 8$ and $q \equiv 1 \pmod 8$. Then $pq \equiv 5 \pmod 8$ and so 2 remains prime. For odd s_j we have $\left(\frac{pq}{s_j}\right) = \left(\frac{s_j}{p}\right)\left(\frac{s_j}{q}\right) = -1$, so also then s_j remains prime.

Take

$$\mathfrak{a} = \mathfrak{r}_1^2 \cdots \mathfrak{r}_n^2 s_1\mathcal{O}_K \cdots s_m\mathcal{O}_K.$$

Then indeed $\mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a}) = a^2$, so what's left to show is that $[\mathfrak{a}]$ is not a fourth power in $\mathcal{C}\ell^+(K)$.

First, note that every class $[s_j\mathcal{O}_K]$ is trivial in $\mathcal{C}\ell^+(K)$. So $[\mathfrak{a}] = [\mathfrak{r}_1 \cdots \mathfrak{r}_n]^2$. We will show that $[\mathfrak{r}_1 \cdots \mathfrak{r}_n]$ is not a square, from which it follows that $[\mathfrak{a}]$ is not a fourth power.

Let D be the subgroup of $\mathcal{C}\ell^+(K)$ consisting of all elements of odd order. By Corollaries 32 and 35 we have $\mathrm{rk}_2(\mathcal{C}\ell^+(K)) = \mathrm{rk}_4(\mathcal{C}\ell^+(K)) = 1$, which implies that $\mathcal{C}\ell^+(K)/D \cong C_{2^k}$ for some $k \ge 2$. The squares of C_{2^k} form a subgroup of index 2, and since the elements of odd order of $\mathcal{C}\ell^+(K)$ are also squares – if $[\mathfrak{a}]^{2l+1} = 1$, then $[\mathfrak{a}] = [\mathfrak{a}^{l+1}]^2$ – we see that also the squares of $\mathcal{C}\ell^+(K)$ form a subgroup of index 2. So since every $[\mathfrak{r}_i]$ is not a square and n is odd, indeed also $[\mathfrak{r}_1 \cdots \mathfrak{r}_n]$ is not a square, which concludes the proof. □

Lemma 41. *Let $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$ be a prime ideal such that $[\mathfrak{p}]$ is not a square in $\mathcal{C}\ell^+(K)$. Then $\mathrm{Gal}(L : K)$ is generated by the Frobenius automorphism $\varphi_{\mathfrak{p}}^{(L)}$ of $\mathfrak{p}$ in L and $\mathfrak{p}$ remains prime in L.*

Proof. Since $L : K$ is unramified, the Frobenius automorphism $\varphi_{\mathfrak{p}}^{(L)}$ is defined for every prime ideal of $\mathcal{O}_K$. We can apply Corollary 3 to get a surjective homomorphism $\mathcal{C}\ell(K) \to \mathrm{Gal}(L : K)$. Combining this with the surjection $\mathcal{C}\ell^+(K) \to \mathcal{C}\ell(K), [\mathfrak{a}] \mapsto [\mathfrak{a}]$, like we did in Proposition 22, yields a surjective homomorphism $\mathcal{C}\ell^+(K) \to \mathrm{Gal}(L : K)$ generated by sending the prime ideals of $\mathcal{O}_K$ to their Frobenius automorphisms of L. Since $\mathrm{Gal}(L : K)$ is of order 2, the non-trivial element is not a square. So all classes that are a square in $\mathcal{C}\ell^+(K)$ are in the kernel of this homomorphism. As we've seen in the proof of Lemma 40, those squares of $\mathcal{C}\ell^+(K)$ form a subgroup of index 2, so since the homomorphism is surjective, the non-squares are mapped to the non-trivial element of $\mathrm{Gal}(L : K)$. So indeed $\varphi_{\mathfrak{p}}^{(L)}$ generates $\mathrm{Gal}(L : K)$. But then the decomposition group $Z_{\mathfrak{p}}^{(L)}$ of $\mathfrak{p}$ in L, which is generated by $\varphi_{\mathfrak{p}}^{(L)}$, equals $\mathrm{Gal}(L : K)$. So $\mathfrak{p}$ does not split in $L : K$. Because $L : K$ is unramified, this means that $\mathfrak{p}$ remains prime in L. □

Proposition 42. *Let $a \in \mathbb{N} \setminus \{0\}$ be as in Lemma 40. Then a^2 is not a global norm of $L : \mathbb{Q}$.*

Proof. Suppose there is a $\gamma \in L^*$ with norm $\mathrm{N}_{\mathbb{Q}}^L(\gamma) = a^2$. Then $\mathrm{N}_{\mathbb{Q}}^K(\mathrm{N}_K^L(\gamma\mathcal{O}_L)) = a^2 = \mathrm{N}_{\mathbb{Q}}^K(\mathfrak{a})$, so

$$\mathrm{N}_{\mathbb{Q}}^K\left(\frac{\mathfrak{a}}{\mathrm{N}_K^L(\gamma\mathcal{O}_L)}\right) = 1.$$

Then by Lemma 19 there exists a fractional ideal $\mathfrak{b} \in \mathbb{I}(K)$ such that $\frac{\mathfrak{a}}{\mathrm{N}_K^L(\gamma\mathcal{O}_K)} = \frac{\mathfrak{b}}{\sigma(\mathfrak{b})}$.

$\mathrm{N}_K^L(\gamma\mathcal{O}_L)$ represents the trivial class of $\mathcal{C}\ell^+(K)$ and $[\sigma(\mathfrak{b})]^{-1} = [\mathfrak{b}]$, so $[\mathfrak{a}] = [\mathfrak{b}]^2$. Since by Lemma 40 $[\mathfrak{a}]$ is not a fourth power, $[\mathfrak{b}]$ is not a square in $\mathcal{C}\ell^+(K)$.

This implies that there must exist a prime divisor $\mathfrak{p}$ of $\mathfrak{b}$ such that $v_p(\mathfrak{b})$ is odd and $v_{\sigma(\mathfrak{p})}(\mathfrak{b})$ is even, with $[\mathfrak{p}]$ not a square in $\mathcal{C}\ell^+(K)$. Then also $v_{\mathfrak{p}}(\frac{\mathfrak{a}\sigma(\mathfrak{b})}{\mathfrak{b}}) = v_{\mathfrak{p}}(\mathrm{N}_K^L(\gamma\mathcal{O}_L))$ is odd. But by Lemma 41 we know that $\mathfrak{p}$ remains prime in L and thus that $v_{\mathfrak{p}}(\mathrm{N}_K^L(\gamma\mathcal{O}_L))$ has to be even. So we have a contradiction and conclude that a^2 indeed is not a global norm of $L : \mathbb{Q}$. □

Bibliography

[1] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press Inc., London, 1967.

[2] A. Fröhlich and M.J. Taylor, *Algebraic Number Theory*, Cambridge studies in advanced mathematics, Volume 27, Cambridge University Press, Cambridge, 1991.

[3] C.F. Gauss, *Disquisitiones Arithmeticae*, Lipsiae, 1801; English translation by A.A. Clarke, *Disquisitiones Arithmeticae*, Yale University Press, New Haven, Conn., 1965.

[4] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II*, Jahresbericht der Deutschen Mathematiker-Vereinigung, Ergänzungsband 6, 1930; Reprint Physica-Verlag, 1965.

[5] H. Hasse, *Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, page 64–69, 1931.

[6] H. Hasse, *Zahlentheorie*, 3rd edition, Akademie-Verlag, Berlin, 1969; English translation H. Hasse, *Number Theory*, Springer-Verlag, Berlin, 1980.

[7] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, Volume 4, page 175–546, 1897.

[8] G.J. Janusz, *Algebraic Number Fields, Second Edition*, Graduate Studies in Mathematics, Volume 7, American Mathematical Society, 1996.

[9] W. Jehne, *On Knots in Algebraic Number Theory*, Journal für die reine und angewandte Mathematik, Volume 311/312, page 214–254, 1979.

[10] F.J. Keune, *Number Fields,* to be published.

[11] E.E. Kummer, *Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke*, Journal für die reine und angewandte Mathematik, Volume 50, page 212–232, 1855.

[12] F. Lemmermeyer, *The Development of the Principal Genus Theorem*, The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae, page 529–561, Springer-Verlag, Berlin, 2007.

[13] L. Rédei and H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Journal für die reine und angewandte Mathematik, Volume 170, page 69–74, 1934.

[14] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen. I.*, Journal für die reine und angewandte Mathematik, Volume 175, page 100–107, 1936.

[15] J.-P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France, Paris, 1970; English translation J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.