MSc Mathematics

Track: Algebra, Geometry and Number Theory

Master thesis

The Hasse Norm Theorem and Norm Equations

by

Bas Korbee

December 12, 2023

Supervisor: dr. Sander Dahmen

Second examiner: prof.dr. Rob de Jeu

Department of Mathematics
Faculty of Sciences

VU UNIVERSITY AMSTERDAM

Abstract

The Hasse norm theorem is one of the first known instances of the local-global principle, sometimes known as the Hasse principle. In this thesis, we will describe the necessary background information required to proof the Hasse norm theorem from an ideal-theoretic approach to class field theory. We will then briefly treat the original proof of Hasse and a semi-modern proof, and highlight the differences between these two. Moreover, we will discuss the many extensions of the Hasse norm theorem discovered over the years and generalise the biquadratic counterexample of Tate to a family of biquadratic fields. Finally, as these two proofs of the Hasse norm theorem are nonconstructive, we will discuss various methods used by modern computer algebra packages to tackle norm equations.

Title: The Hasse Norm Theorem and Norm Equations
Author: Bas Korbee, korbee.bas@vu.nl, 2620725
Supervisor: dr. Sander Dahmen
Second examiner: prof.dr. Rob de Jeu
Date: December 12, 2023

Department of Mathematics
VU University Amsterdam
de Boelelaan 1081, 1081 HV Amsterdam
http://www.math.vu.nl/

Contents

1 Introduction

In his highly influential Zahlbericht published in 1897, Hilbert showed that a nonzero rational number $n \in \mathbb{Q}^*$ is the norm of an element in a quadratic extension $\mathbb{Q}(\sqrt{a})$ of $\mathbb{Q}$ if and only if it is the norm of an element in the corresponding local extension $\mathbb{Q}_p(\sqrt{a})$ of $\mathbb{Q}_p$ for all prime numbers p and infinity [30, Satz 102, p. 173]. That is, an element in a quadratic extension of $\mathbb{Q}$ is a global norm if and only if it is a local norm everywhere. Two years later he generalised his theorem to all quadratic extensions of number fields [29, Satz 65, p. 122] while Fürtwangler proved the statement for all Kummer extensions of number fields of odd prime degree [19, Satz 18, p. 429] in 1913.

The years after Fürtwangler were quiet as World war I began and Germany was one of the only places where algebraic number theory was actively studied. Nevertheless, Takagi worked in isolation in Japan on various questions posed by Hilbert regarding the correspondence of abelian extensions with the so-called ideal groups. He presented his theory, which is now known as class field theory, to the International Congress of Mathematicians in 1920. Using class field theory, Hasse proved in 1930 that an element in a cyclic extension of number fields of prime degree is a global norm if and only if it is a local norm everywhere [28, Teil II, p. 38]. He speculated that the theorem should hold for all abelian extensions, but he was unable to provide a proof.

However, Hasse was too quick on the draw and a year later he retracted his conjecture: the element 3 in $\mathbb{Q}(\sqrt{-3}, \sqrt{-39})$ is a local norm everywhere but is not a global norm [27]. That said, in the same paper he shows using induction that his theorem does hold for cyclic extensions and thus the Hasse norm theorem was born:

> Let L/K be a finite cyclic extension of number fields and $\alpha \in K^*$. Then α is a global norm for L/K if and only if α is a local norm everywhere for L/K.

This result of Hasse now fits into a wider category of results called the local-global principle, which roughly states that problems can sometimes be globally solved by solving them locally everywhere first. The principle is sometimes called the Hasse principle since he proved [26] the first nontrivial instance of the local-global principle, the Hasse-Minkowski theorem, based on the work of Hensel and Minkowski [37]: a quadratic form has a nonzero solution over a number field if and only if it has nonzero solution one everywhere locally. Interestingly, while this result precedes his norm theorem, it can be considered a corollary of the norm theorem; highlighting the strength of the Hasse norm theorem.

In this thesis, we will develop the tools necessary for us to proof the Hasse norm theorem in a classical setting whilst using group cohomology to avoid some tiresome local computations. The original proof of Hasse did not use group cohomology as this field was only developed after World War II. To highlight the effort of Hasse, we will also provide an overview of his original arguments, which, as far as we are aware, have rarely been published in English since his approach has fallen out of favour for the group cohomology approach.

We will start by summarising the basic theory of algebraic number theory in Chapter 2 and quickly move on to the theory of valuations and group cohomology. In Chapter 3 we will provide a brief overview of class field theory. After discussing all of this background material, we will give the two alluded proofs of the Hasse norm theorem in Chapter 4 and briefly discuss how the Hasse-Minkowski theorem can be seen as a consequence of the norm theorem. Finally, we end Chapter 4 by generalising the definition of being a local norm to non-Galois extensions and summarise all the extensions of the Hasse norm theorem that have been found throughout the years.

We have briefly mentioned that the Hasse norm theorem need not hold for abelian extensions, as has been illustrated by Hasse's own counterexample $\mathbb{Q}(\sqrt{-3}, \sqrt{-39})$. Besides this counterexample, another famous counterexample is from Tate [9, Ch. VII, Sec. 11.4] who showed that there are infinitely many integer squares in $\mathbb{Q}(\sqrt{13}, \sqrt{17})$ that are local norms everywhere but not global norms. Using a similar argument as Tate, we derive in Chapter 5 a necessary, yet sufficient, condition for a biquadratic field $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, with $a, b \in \mathbb{Z}$ squarefree and coprime, to satisfy the Hasse norm theorem and find explicit elements that are local norms everywhere but not global norms in the case the condition fails.

Finally, we note that the two provided proofs of the Hasse norm theorem are nonconstructive. As such, we will dedicate Chapter 6 to cover various techniques to solve not only norm equations, but also integral norm equations. These techniques additionally offer an alternative method for finding possible counterexamples to the Hasse norm theorem without using class field theory. We end with a quick discussion and a popular summary aimed at first-year mathematics students.

2 Prerequisites

Before we discuss class field theory and the Hasse norm theorem, we need to explain more clearly what is meant by looking at a number field locally. Moreover, the modern formulation of class field theory uses a fair amount of Galois cohomology. We will therefore dedicate this chapter to these two subjects, together with a brief summary of algebraic number theory as taught in a first-year master course. Because the space is rather limited, we will only provide the statements necessary for the material later on. The interested reader may consult [47] and/or [38, Ch. II] for a fantastic, yet complete, introduction to valuation theory, while [21, Ch. 3] acts as a wonderful introduction to Galois cohomology.

2.1 Basic algebraic number theory

Throughout this thesis, we assume that the reader is familiar with the curriculum of a first-year master course in algebraic number theory. That said, we will give a very brief overview of the subject for the sake of completeness. For the full material, we recommend [46] and/or [38, Ch. I].

A *number field* K is a finite extension of the field of rational numbers $\mathbb{Q}$. Attached to K is a subring O_K called the *ring of integers of* K which is defined as the integral closure of $\mathbb{Z}$ in K, i.e.

$$O_K = \{\alpha \in K \mid \exists f \in \mathbb{Z}[X] \text{ monic s.t. } f(\alpha) = 0\}.$$

The ring of integers is an important object attached to a number field and often finds itself at the center of algebraic number theory. One may ask what sort of properties this ring has (in fact, it is not immediately obvious that it is a ring). A desirable property for a ring to have is that of a unique factorisation domain, but the ring of integers generally does not have this property. However, the property can be recovered by passing to ideals or rather a generalisation of ideals.

We say that a O_K-submodule I of K is a *fractional K-ideal* if there exists some $x \in K^*$ such that $xI \subset O_K$. In other words, I is an ideal of O_K after multiplying by an element of K^*. In turn, we usually refer to an ideal of O_K as an *integral K-ideal*. Now, we say that O_K is a *Dedekind domain* if every nonzero fractional K-ideal can be written uniquely up to reordering as a product of prime O_K-ideals.

Theorem 2.1.1. *Let K be a number field. Then O_K is a Dedekind domain.*

Proof. See [38, Cor. 3.9, p. 22]. □

By the above, the set $\mathcal{I}_K$ of nonzero fractional K-ideals is a free group generated by the prime K-ideals. We can then consider the subgroup $\mathcal{P}_K$ of *principle fractional K-ideals* which are all the nonzero fractional K-ideals generated by a single element $\alpha \in K^*$. The quotient group $\mathrm{Cl}_K = \mathcal{I}_K/\mathcal{P}_K$ is the *class group of K* and is an immensely important invariant of K as shown by the following theorem.

Theorem 2.1.2. *Let K be a number field. Then*

i) Cl_K *is a finite group;*

ii) $\mathrm{Cl}_K = 1$ *if and only if $\mathcal{O}_K$ is a principle ideal domain.*

Proof. The first statement is far from trivial and uses Minkowski's result in the geometry of numbers, see [38, Thm. 6.3, p. 36]. The second statement is rather trivial. Indeed, if $\mathrm{Cl}_K = 1$ then every nonzero fractional K-ideal is principle. Conversely, if $\mathcal{O}_K$ is a principle ideal domain, then every nonzero fractional K-ideal is principle by definition. □

No matter the class group, the study of fractional K-ideals can always be reduced to the study of prime K-ideals. If L is a finite extension of K, then any prime L-ideal $\mathfrak{q}$, i.e. a prime ideal of $\mathcal{O}_L$, can be brought back to a prime K-ideal $\mathfrak{p}$ by setting $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ and we say that $\mathfrak{p}$ *lies below* $\mathfrak{q}$ while $\mathfrak{q}$ *lies above* $\mathfrak{p}$. Conversely, the L-ideal $\mathfrak{p}\mathcal{O}_L$ need not be prime for a prime K-ideal $\mathfrak{p}$. If $\mathfrak{p}\mathcal{O}_L$ is prime, then we say that $\mathfrak{p}$ is *inert* in L/K. If it is not prime, then by Theorem 2.1.1 we know that we can write

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e(\mathfrak{q}_1/\mathfrak{p})} \cdots \mathfrak{q}_n^{e(\mathfrak{q}_n/\mathfrak{p})}$$

for some unique prime L-ideals $\mathfrak{q}_i$ and $e(\mathfrak{q}_i/\mathfrak{p}) \in \mathbb{Z}_{\geq 1}$, and we say that $\mathfrak{p}$ is *split in L/K*. If additionally $e(\mathfrak{q}_i/\mathfrak{p}) \geq 2$ for some i, then $\mathfrak{p}$ is *ramified in L/K*. The number $e(\mathfrak{q}_i/\mathfrak{p})$ is called the *ramification index of $\mathfrak{q}_i$ in $\mathfrak{p}$*.

Besides the ramification index, there is another invariant attached to a prime lying above another prime. Because $\mathcal{O}_K$ is a Dedekind domain by Theorem 2.1.1, the ring $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ for any prime K-ideal $\mathfrak{p}$ is a finite field called the *residue class field of* $\mathfrak{p}$. For any prime L-ideal $\mathfrak{q}$ lying above $\mathfrak{p}$ we therefore have a finite extension of finite fields $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$. Its degree is called the *residue class degree of $\mathfrak{q}$ in $\mathfrak{p}$* and is denoted by $f(\mathfrak{q}/\mathfrak{p})$.

Theorem 2.1.3. *Let L/K be a finite extension of number fields. Then*

i) for all prime K-ideals $\mathfrak{p}$ we have

$$[L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p})$$

summing over all the prime L-ideals above $\mathfrak{p}$;

ii) only finitely many prime K-ideals are ramified in L/K.

Proof. See [38, Prop. 8.2, p. 46] and [38, Thm. 8.4, p. 49] □

2.2 Valuation theory

In a first course on analysis, we have seen that the set of rational numbers is too small to define any notion of continuity. Therefore, we go to the set of real numbers which can be constructed by taking the completion of $\mathbb{Q}$ with respect to the absolute value $|\cdot|$. To generalise this notion to an arbitrary number field K, we first have to define what an absolute value on K is.

Definition 2.2.1. Let K be a field. A *valuation* ϕ on K is a function $\phi : K \to \mathbb{R}_{\geq 0}$ satisfying

i) $\phi(x) = 0$ if and only if $x = 0$;
ii) $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in K$;
iii) there exists a constant $C > 0$ such that for all $x, y \in K$

$$\phi(x + y) \leq C \max\{\phi(x), \phi(y)\}.$$

If ϕ is a valuation on a field K, then ϕ induces a topology on K generated by the open balls

$$\{y \in K \mid \phi(x - y) < \epsilon\}$$

for $x \in K$ and $\epsilon > 0$. This turns K in particular into a *topological field* and we say that two valuations ϕ and ψ on K are *equivalent*, denoted $\phi \sim \psi$, if they induce the same topology.

The smallest value C satisfying iii) is called the *norm* of the valuation ϕ and is often denoted as $\|\phi\|$. By ii) we must have that $\|\phi\| \geq 1$ and we say that ϕ is *non-Archimedean* if $\|\phi\| = 1$ and *Archimedean* otherwise. The non-Archimedean valuations are the most interesting as they exhibit counterintuitive properties. For example, values do not add up in a non-Archimedean field: by repeatedly applying ii) we see that K satisfies the *ultrametric inequality*

$$\phi\left(\sum_{i=1}^{n} x_i\right) \leq \max_i \phi(x_i)$$

for $x_1, \ldots, x_n \in K$.

Example 2.2.2. Let K be a number field. If $\mathfrak{p}$ is a prime K-ideal, then there exists an unique rational prime p such that $\mathfrak{p} \cap \mathbb{Q} = (p)$. For any $x \in K^*$, we can uniquely write $x\mathcal{O}_K$ as a product of prime K-ideals by Theorem 2.1.1. If we define $\mathrm{ord}_{\mathfrak{p}}(x)$ to be the exponent of $\mathfrak{p}$ appearing in the factorisation of $x\mathcal{O}_K$, then we can set

$$\begin{aligned} \phi_{\mathfrak{p}} : K &\to \mathbb{R}_{\geq 0} \\ x &\mapsto p^{-\mathrm{ord}_{\mathfrak{p}}(x)}, \end{aligned}$$

where we take the convention that $\mathrm{ord}_{\mathfrak{p}}(0) = \infty$. It is easy to see that $\phi_{\mathfrak{p}}$ is a non-Archimedean valuation on K.

Similarly, for $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, the function $\phi_\sigma : K \to \mathbb{R}_{\geq 0}$ given by

$$\phi_\sigma(x) = |\sigma(x)|$$

defines an Archimedean valuation on K of norm 2. By taking $K = \mathbb{Q}$, we indeed see that the usual absolute value on $\mathbb{Q}$ is a valuation. In fact, some authors call a valuation on a field K an *absolute value on K* or a *norm on K*. We have, however, opted to use the term valuation to not confuse the reader as the norm and absolute value are already well-established terms in mathematics.

It turns out that the valuations above are actually the only possible valuations on a number field up to equivalence.

Theorem 2.2.3. *Let K be a number field and ϕ a nontrivial valuation on K.*

i) If ϕ is non-Archimedean, then $\phi \sim \phi_\mathfrak{p}$ for some unique prime K-ideal $\mathfrak{p} \subset O_K$.

ii) If ϕ is Archimedean, then $\phi \sim \phi_\sigma$ for some $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

Remark. As a result, an equivalence class of non-Archimedean valuations of any field is called a *finite prime* while an equivalence class of Archimedean valuations is called an *infinite prime*. We will use this terminology somewhat liberally and refer to a finite prime of a number field K, or a finite K-prime, as a prime ideal $\mathfrak{p} \subset O_K$ and an infinite prime of K, or an infinite K-prime, as a field embedding $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Moreover, we will usually use the Fraktur alphabet such as $\mathfrak{p}$ and $\mathfrak{q}$ for finite primes, Greek alphabet such as σ and τ for infinite primes and the Latin alphabet such as v and w for unspecified primes.

Proof. See [47, Thm. 1.20, p. 14]. □

One of the cornerstones of algebra is the Chinese remainder theorem, which states that, given a ring R and a finite collection of pairwise coprime R-ideals $I_1, \ldots, I_n$, the natural map $R \to R/I_1 \times \cdots \times R/I_n$ is surjective. If ϕ is a non-Archimedean valuation on a number field K, then by the above we have $\phi \sim \phi_\mathfrak{p}$ for some finite K-prime $\mathfrak{p}$. Given $\alpha, \beta \in O_K$ and $\epsilon > 0$, the condition $\phi_\mathfrak{p}(\alpha - \beta) < \epsilon$ is then equivalent to the condition $\alpha \equiv \beta \pmod{\mathfrak{p}^n}$ for some $n \in \mathbb{Z}_{\geq 0}$. The next theorem can therefore be viewed as a stronger version of the Chinese remainder theorem.

Theorem 2.2.4 (Weak approximation theorem)**.** *Let $\phi_1, \ldots, \phi_n$ be pairwise inequivalent nontrivial valuations on a field K and let $\beta_1, \ldots, \beta_n \in K$. Then for all $\epsilon > 0$ there exists some $\alpha \in K$ such that for all $i = 1, \ldots, n$*

$$\phi_i(\alpha - \beta_i) < \epsilon.$$

Remark. More succinctly, the image of K under the diagonal map $K \to \prod_{i=1}^n K_i$, where K_i is the field K equipped with the valuation ϕ_i, is dense in the product topology.

Proof. See [47, Thm. 1.17, p. 12]. □

Having defined an analogue of an absolute value on a field K in the form of valuations, we can now define the completion of K with respect to a valuation ϕ and show that this completion satisfies a certain uniqueness property in the same vain that $\mathbb{R}$ does. Recall that a metric space M is complete if all Cauchy sequences converge in M.

Theorem 2.2.5. *Let K be a field and ϕ a valuation on K. Then there exists a field extension K_ϕ/K, called the completion of K with respect to ϕ, such that K_ϕ is complete with respect to some extension of ϕ and K_ϕ contains K as a dense subfield.*

Moreover, if F/K is another field extension that is complete with respect to an extension of ϕ, then there exists an unique continuous K-homomorphism $K_\phi \to F$.

Proof. Let R be the K-algebra consisting of all Cauchy sequences in K and let $\mathfrak{m}$ be the R-ideal consisting of all sequences $(x_n)_{n=1}^\infty$ such that $\lim_n \phi(x_n) = 0$. It can be readily checked that $\mathfrak{m}$ is a maximal ideal and that the field $K_\phi = R/\mathfrak{m}$ with $\phi((x_n)_{n=1}^\infty) = \lim_n \phi(x_n)$ satisfies the desired properties, see [47, Thm. 2.4, p. 20]. □

The definition of the completion K_ϕ is rather nondescriptive as the K-algebra of all Cauchy sequences in K is large. Let us therefore work on another description of complete fields and focus first on the non-Archimedean case. An important property of $\mathbb{R}$ is that any real number has a decimal expansion, i.e. it can be written as a power series $\sum_i a_i 10^i$ with $a_i \in \{0, \dots, 9\}$. It turns out that K_ϕ satisfies a similar property under a mild assumption.

Let ϕ be a non-Archimedean valuation on K. By the ultrametric inequality we see that the subset $A_K \subset K$ given by

$$A_K = \{x \in K \mid \phi(x) \leq 1\}$$

is a subring. Moreover, it is a local ring whose sole maximal ideal $\mathfrak{m}$ is given by

$$\mathfrak{m} = \{x \in K \mid \phi(x) < 1\}.$$

The ring A_K is known as the *valuation ring of ϕ* while the quotient $A_K/\mathfrak{m}$ is known as the *residue class field of ϕ*. Note that, because $K \subset K_\phi$ is dense, the residue class field of ϕ is isomorphic to the residue class field of the extension of ϕ to K_ϕ.

Finally, ϕ is said to be *discrete* if A_K is a discrete valuation ring. In this case, the *uniformizer of ϕ* is the generator of the unique maximal ideal of A_K. Moreover, by a density argument one sees that the extension of ϕ to K_ϕ is also discrete.

Theorem 2.2.6. *Let K be a field and ϕ a nontrivial discrete valuation on K such that K is complete with respect to ϕ. Let $S \subset A_K$ be a set of representatives of the residue class field of ϕ and let π be an uniformizer of ϕ. Then every $x \in K$ can be written as a power series*

$$x = \sum_{i=-\infty}^{\infty} a_i \pi^i$$

with $a_i \in S$ zero for small enough i.

Proof. See [38, Prop. 4.3, p.126]. □

Example 2.2.7. Consider the non-Archimedean valuations over $\mathbb{Q}$. By Theorem 2.2.3 any non-Archimedean (nontrivial) valuation is equivalent to ϕ_p for some prime number p. By the fundamental theorem of arithmetic we see that the valuation ring of ϕ_p is $\mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at the prime ideal (p). Hence ϕ_p is in particular a discrete valuation. Its maximal ideal is $p\mathbb{Z}_{(p)}$ and by exactness of localization we see that the residue class field of ϕ_p is $\mathbb{F}_p$. Now, the completion of $\mathbb{Q}$ with respect to ϕ_p is called the *field of p-adic numbers* and denoted by $\mathbb{Q}_p$. By the above, any p-adic number can be written as a power series

$$\sum_{i=-\infty}^{\infty} a_i p^i$$

where $a_i \in \{0, \dots, p-1\}$ and a_i is zero for small enough i.

More generally, the field $K_{\phi_\mathfrak{p}}$ for a finite K-prime $\mathfrak{p}$ is called the $\mathfrak{p}$-*adic completion of* K and is often written as $K_\mathfrak{p}$ for conciseness. This also satisfies Theorem 2.2.6 since the valuation ring of K is $O_{K,\mathfrak{p}}$, which is discrete by Theorem 2.1.1.

Remark. Note that the terminology of the residue class field of a valuation and the residue class field of a finite K-prime coincide.

The study of polynomials is ubiquitous in algebra and in the case of polynomials over a complete non-Archimedean valued fields, their factorisation can be determined by looking at its factorisation over the residue class field.

Lemma 2.2.8 (Hensel's Lemma)**.** *Let K be a field, ϕ a nontrivial valuation on K such that K is complete with respect to ϕ and κ the residue class field of ϕ. Suppose a polynomial $f \in A_K[x]$ factors over $\kappa[X]$ as*

$$\overline{f} = \overline{g}\overline{h} \in \kappa[x]$$

with $\overline{g}, \overline{h} \in \kappa[x]$ coprime. Then this factorisation can be lifted to a factorisation $f = g \cdot h$ in $A_K[x]$ such that $\deg g = \deg \overline{g}$ and the reduction of g and h in $\kappa[x]$ is $\overline{g}$ and $\overline{h}$, respectively.

Proof. See [38, Lem. 4.6, p. 129]. □

Let us now briefly touch upon the Galois theory of the non-Archimedean completions of number fields. Suppose L/K is a finite Galois extension of number fields with Galois group G and $\mathfrak{p}$ a finite K-prime. Let $\Sigma_\mathfrak{p}$ denote the set of finite L-primes lying above $\mathfrak{p}$. Note that any such prime can be thought of as an extension of the $\mathfrak{p}$-adic valuation on K to L. This set comes equipped with a natural G-action given by $\sigma\mathfrak{q} = \sigma(\mathfrak{q})$ and the stabilizer of a finite L-prime $\mathfrak{q}$ above $\mathfrak{p}$ under this action is called the *decomposition group of* $\mathfrak{q}/\mathfrak{p}$, denoted by $D(\mathfrak{q}/\mathfrak{p})$.

Lemma 2.2.9. *Let L/K be a finite Galois extension of number fields with Galois group G and $\mathfrak{p}$ a finite K-prime. Then G acts transitively on $\Sigma_\mathfrak{p}$.*

Proof. Suppose G does not act transitively on $\Sigma_\mathfrak{p}$ and let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be two L-primes such that $\sigma(\mathfrak{q}_1) \neq \mathfrak{q}_2$ for all $\sigma \in G$. Using the Chinese remainder theorem, find $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv 0 \pmod{\mathfrak{q}_2}$ and $\alpha \equiv 1 \pmod{\sigma^{-1}(\mathfrak{q}_1)}$ for all $\sigma \in G$. Then $N_{L/K}(\alpha) \in \mathfrak{q}_2 \cap K = \mathfrak{p} \subset \mathfrak{q}_1$ and thus $\sigma(\alpha) \in \mathfrak{q}_1$ for some $\sigma \in G$ by the primality of $\mathfrak{q}_1$; contradiction. □

In particular it follows that the ramification index and the residue field degree are independent on the prime above $\mathfrak{p}$. Indeed, write $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$. Then $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{q}_1)^{e_1} \cdots \sigma(\mathfrak{q}_n)^{e_n}$ and thus from the unique factorisation of ideals in $\mathcal{O}_L$ (Theorem 2.1.1) and the transitivity of the Galois action we conclude that $e_1 = \cdots = e_n$. In a similar manner, one can show that the the residue field degree is independent on the prime above. We are therefore permitted to write $e(\mathfrak{p})$ and $f(\mathfrak{p})$ for the ramification index and residue field degree of $\mathfrak{p}$, respectively. Using the summation formula in Theorem 2.1.3 it follows that

$$\#G = g(\mathfrak{p})e(\mathfrak{p})f(\mathfrak{p})$$

where $g(\mathfrak{p})$ is the number of finite L-primes above $\mathfrak{p}$, i.e. the cardinality of $\Sigma_\mathfrak{p}$. In turn, the Orbit-Stabilizer theorem tells us that $\#D(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{p})f(\mathfrak{p})$.

Lemma 2.2.10. *Let L/K be a finite Galois extension of number fields with Galois group G and $\mathfrak{p}$ a finite K-prime. Then*

i) the completions $L_\mathfrak{q}$ for $\mathfrak{q} \in \Sigma_\mathfrak{p}$ are all isomorphic;
ii) the field extension $L_\mathfrak{q}/K_\mathfrak{p}$ for $\mathfrak{q} \in \Sigma_\mathfrak{p}$ is Galois whose Galois group is isomorphic to $D(\mathfrak{q}/\mathfrak{p})$.

Proof. Given two L-primes $\mathfrak{q}_1, \mathfrak{q}_2 \in \Sigma_\mathfrak{p}$, there exists a $\sigma \in G$ such that $\mathfrak{q}_1 = \sigma\mathfrak{q}_2$ by the transitivity of the Galois action (Lemma 2.2.9). Such a σ induces an isomorphism of fields $L_{\mathfrak{q}_1} \simeq L_{\mathfrak{q}_2}$.

It thus remains to proof *ii*). First note that $L_\mathfrak{q}/K_\mathfrak{p}$ is indeed an extension of fields by Theorem 2.2.5. Now, fix $\mathfrak{q} \in \Sigma_\mathfrak{p}$. Any $\sigma \in D(\mathfrak{q}/\mathfrak{p})$ can be uniquely extended to a $K_\mathfrak{p}$-automorphism of $L_\mathfrak{q}$ since L is dense in $L_\mathfrak{q}$ and σ fixes $\mathfrak{q}$. Hence $\#D(\mathfrak{q}/\mathfrak{p}) \leq \#\operatorname{Aut}_{K_\mathfrak{p}}(L_\mathfrak{q}) \leq [L_\mathfrak{q} : K_\mathfrak{p}]$. If we are able to proof that these inequalities are instead equalities, then we have proven the desired.

Now, we have a natural homomorphism $\Phi : L \otimes_K K_\mathfrak{p} \to \prod_{\mathfrak{r}\in\Sigma_\mathfrak{p}} L_\mathfrak{r}$ of $K_\mathfrak{p}$-algebras. Its image is a complete finite dimensional $K_\mathfrak{p}$-subspace of $\prod_{\mathfrak{r}\in\Sigma_\mathfrak{p}} L_\mathfrak{r}$ hence in particular closed. Moreover, by the weak approximation theorem (Theorem 2.2.4) it is also dense and thus Φ is surjective. Taking $K_\mathfrak{p}$-dimensions on both sides we therefore conclude that $[L : K] \geq \sum_{\mathfrak{r}\in\Sigma_\mathfrak{p}} [L_\mathfrak{r} : K_\mathfrak{p}]$. Hence using Lemma 2.2.9 we find

$$\#G = g(\mathfrak{p})\#D(\mathfrak{q}/\mathfrak{p}) = \sum_{\mathfrak{r}\in\Sigma_\mathfrak{p}} \#D(\mathfrak{r}/\mathfrak{p}) \leq \sum_{\mathfrak{r}\in\Sigma_\mathfrak{p}} [L_\mathfrak{r} : K_\mathfrak{p}] \leq [L : K] = \#G,$$

whence we have equalities throughout; implying $[L_{\mathfrak{r}} : K_{\mathfrak{p}}] = \#D(\mathfrak{r}/\mathfrak{p})$. □

Finally let us discuss the Archimedean case for completeness. It turns out that we already know what the complete Archimedean fields are.

Theorem 2.2.11. *Let K be a complete Archimedean field with respect to a valuation ϕ. Then K is topologically isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.*

Proof. See [47, Thm .2.4, p. 21]. □

If K is a number field, then any Archimedean valuation is induced by a field embedding $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ by Theorem 2.2.3, which we called an infinite K-prime. If σ is real, i.e. its image is contained in $\mathbb{R}$, then the completion K_σ must also be real and we conclude that $K_\sigma \simeq \mathbb{R}$. Otherwise, we must have that $K_\sigma \simeq \mathbb{C}$. For any Galois extension L/K and τ an infinite L-prime extending σ, i.e. $\tau|_K = \sigma$, we therefore have $[L_\tau : K_\sigma] = 1$ unless σ is real while τ is not. In Lemma 2.2.10 we have seen that $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e(\mathfrak{p})f(\mathfrak{p})$ and many authors generalise the ramification index to infinite primes by ways of this equality (note that there is no residue class field). That is to say, $e(\tau/\sigma) = 1$ unless σ is real while τ is not in which case $e(\tau/\sigma) = 2$ and we say that σ is *ramified in* L/K.

2.3 Group (co)homology

A common viewpoint in group theory is that a group can be studied by looking at its representations or, more generally, its modules. The group (co)homology functor neatly packages how precisely a group acts on a module. Historically, cohomology was developed for topological purposes but quickly found applications outside topology such as in class field theory, where it is now ubiquitous. As the field of cohomology is broad, we will only treat the basic definitions. Moreover, we will only consider the case when the group is cyclic as many statements in class field theory can be reduced to this case. For a complete view of cohomology, we refer the reader to [41] and/or [21].

Let G be a group. By a *(left) G-module* we mean an abelian group M equipped with a (left) G-action. Equivalently, it is a (left) $\mathbb{Z}[G]$-module and any types of modules of rings are immediately generalised to G-modules such as free and projective modules. A function $f : M \to N$ of G-modules is a *G-homomorphism* if it is invariant under the G-action and we denote $\mathrm{Hom}_G(M, N)$ as the abelian group of G-homomorphisms between M and N.

Now suppose that $G = \langle \sigma \rangle$ is a finite cyclic group of order n and M a G-module. Define two G-homomorphisms $M \to M$ by

$$N(m) = \sum_{i=0}^{n-1} \sigma^i(m) \quad \text{and} \quad \Delta(m) = m - \sigma(m).$$

These two G-homomorphisms clearly satisfy $N\Delta = \Delta N = 0$ and thus $\ker N \supset \operatorname{im}\Delta$ and $\ker\Delta \supset \operatorname{im} N$.

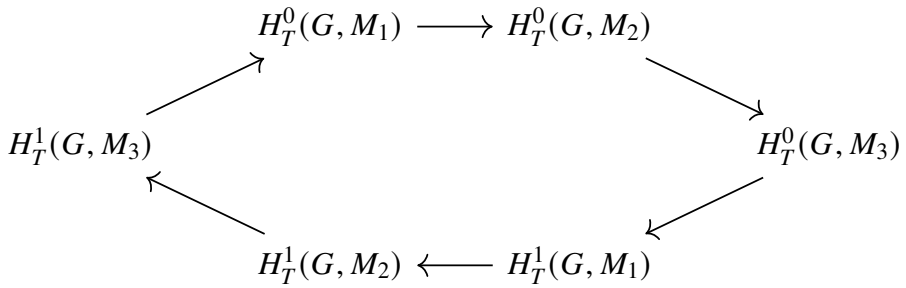
Definition 2.3.1. Let G be a finite cyclic group and M a G-module. The *Tate cohomology groups* $H_T^0(G,M)$ and $H_T^1(G,M)$ of M are the two quotient groups

$$H_T^0(G,M) = \ker\Delta/\operatorname{im} N \quad \text{and} \quad H_T^1(G,M) = \ker N/\operatorname{im}\Delta.$$

Remark. Be warned that the above definition does not generalise to the general case. If one would to treat cohomology in its absolute generality, then one would start with a projective resolution of $\mathbb{Z}$ viewed as a trivial G-module and apply $\operatorname{Hom}_G(-,M)$ to yield an infinite sequence of abelian groups. This sequence need not be exact and the cohomology groups of M are then the quotient groups of the kernel over the image at each level of the sequence. The homology groups of M are similar, except one applies $-\otimes_G M$ to the sequence instead of $\operatorname{Hom}_G(-,M)$. The Tate cohomology groups of M are then a certain combination of the cohomology and homology groups. One does have to be careful though, as this definition depends on the chosen projective resolution of $\mathbb{Z}$. It turns out that it is independent of this choice, but its proof is rather cumbersome. In the end, this definition coincides with our definition when G is cyclic hence we have opted to go the easier route.

Note that both Tate cohomology groups respect G-homomorphisms. That is, given $f \in \operatorname{Hom}_G(M_1,M_2)$, there exists an unique homomorphism of groups $H^0(f) : H_T^0(G,M_1) \to H_T^0(G,M_2)$ (similarly for $H_T^1(G,-)$), explicitly given by $H^0(f)(\overline{m}) = f(\overline{m})$. It is well-defined as N and Δ commute with any G-homomorphism. In short, this means that $H_T^\bullet(G,-)$ is a functor from the category of G-modules to the category of abelian groups. An important property of this functor is that it maps short exact sequences to exact hexagons.

Lemma 2.3.2. *Let G be a cyclic group and let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of G-modules. Then we have an exact hexagon*



of abelian groups.

Proof. Since N commutes with all G-homomorphisms, an application of the Snake lemma yields an exact sequence of abelian groups

$$\begin{aligned} 0 &\to \ker(N|M_1) \to \ker(N|M_2) \to \ker(N|M_3) \\ &\to \operatorname{coker}(N|M_1) \to \operatorname{coker}(N|M_2) \to \operatorname{coker}(N|M_3) \to 0, \end{aligned}$$

where we have written $N|M_1$ as the map N acting on M_1 for clarity. A similar sequence holds for Δ.

We then obtain a commutative diagram

$$\begin{array}{ccccccc} & & \operatorname{coker}(N|M_1) & \longrightarrow & \operatorname{coker}(N|M_2) & \longrightarrow & \operatorname{coker}(N|M_3) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \Delta} \\ 0 & \longrightarrow & \ker(N|M_1) & \longrightarrow & \ker(N|M_2) & \longrightarrow & \ker(N|M_2) \end{array}$$

for which the Snake lemma yields the following exact sequence:

$$H_T^0(G, M_1) \to H_T^0(G, M_2) \to H_0^T(G, M_3) \to H_T^1(G, M_1) \to H_T^1(G, M_2) \to H_1^T(G, M_3).$$

The desired then follows by interchanging the roles of Δ and N in the above argument and splicing the sequences together. □

In the case that both cohomology groups are finite, the Herbrand quotient is an useful computational tool packaging the order of both groups in a single quantity.

Definition 2.3.3. Let G be a finite cyclic group and M a G-module such that both its Tate cohomology groups are finite. The *Herbrand quotient* $q(G, M)$ *of* M is defined as the quantity

$$q(G, M) = \frac{\#H_T^1(G, M)}{\#H_T^0(G, M)}.$$

Just as the cohomology groups respect short exact sequences, so does the Herbrand quotient.

Lemma 2.3.4. *Let G be a finite cyclic group.*

i) If M is a finite G-module, then $q(G, M) = 1$.

ii) If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of G-modules such that the Herbrand quotient of at least two of the modules exists, then the Herbrand quotient of all three exists and moreover

$$q(G, M_2) = q(G, M_1)q(G, M_3).$$

Proof. *ii*) is a straightforward consequence of the behaviour of cardinality of finite groups in exact sequence, i.e. it satisfies an alternating product, together with Lemma 2.3.2 while *i*) follows from the following short exact sequences

$$0 \to \ker(\Delta) \to M \to \operatorname{im}(\Delta) \to 0,$$
$$0 \to \ker(N) \to M \to \operatorname{im}(N) \to 0.$$

□

We end with a fun application to field extensions first shown by Hilbert in his Zahlbericht and later packaged in terms of cohomology by Noether.

Theorem 2.3.5 (Hilbert 90)**.** *Let K be a number field and L a finite cyclic extension of K. Then*

$$H^1_T(\mathrm{Gal}(L/K), L^*) = 1.$$

Proof. The abelian group L^* is written multiplicatively hence the homomorphism N coincides with the norm map $N_{L/K}$. We must therefore show that for any $x \in \ker N_{L/K}$ there exists some $y \in L^*$ such that $x = y\sigma^{-1}(y)$.

Define inductively $a_0 = 1$ and $a_i = x\sigma(a_{i-1})$ for $i \geq 1$. By the linear independence of field characters [13, Thm. 7, p. 569] there exists some $b \in L^*$ such that

$$y = \sum_{i=0}^{n-1} a_i \sigma^i(b) \neq 0,$$

where σ is a generator of $\mathrm{Gal}(L/K)$ and n its order. Since $a_n = 1$ we then have

$$x\sigma(y) = \sum_{i=0}^{n-1} x\sigma(a_i)\sigma^{i+1}(b) = \sum_{i=0}^{n-1} a_{i+1}\sigma^{i+1}(b) = y.$$

□

3 Class field theory

The abelian extensions of $\mathbb{Q}$ are easily described: by the Kronecker-Weber theorem every abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic extension [38, Thm. 1.10, p. 324]. For any other number field besides $\mathbb{Q}$ it need not be that every abelian extension is cyclotomic, e.g. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$. The goal of class field theory is to describe the abelian extensions of any number field (in fact, not only number fields but also local fields). Because the Hasse norm theorem is a corollary of class field theory, it is necessary for us to explain this subject more thorough. However, the branch of class field theory is rather large and it would be unreasonable for us to completely discuss class field theory. As such, we will only explain the bare minimum necessary for us to proof the Hasse norm theorem. The interested reader may consult [31], of which much of this material stems from, and/or [9].

Moreover, there are two possible approaches to class field theory: the ideal-theoretic and the idéle-theoretic approach. In modern times, the former has fallen out of fashion since the latter is broader in-scope. That said, we will use the ideal-theoretic approach as it is more tangible and less abstract than the modern approach.

3.1 Ray class groups

The class group is the quotient group of fractional ideals over the principle fractional ideals and is an important invariant of a number field. The ray class groups are refinements of the class group and are defined in terms of moduli.

Definition 3.1.1. Let K be a number field. A *modulus* $\mathfrak{m}$ *of* K is a tuple $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is an ideal of O_K and $\mathfrak{m}_\infty$ a set of real field embeddings $K \to \mathbb{R}$.

If L/K is an extension of number fields and $\mathfrak{m}$ a modulus of L, then $\mathfrak{m}$ can be considered to be a modulus of K by simply restricting to K. The converse is also possible: if $\mathfrak{m}$ is a modulus of K, then we can naturally extend $\mathfrak{m}$ to a modulus $\mathfrak{m}_L$ of L by letting $\mathfrak{m}_{L,0}$ be $\mathfrak{m}O_L$ and $\mathfrak{m}_{L,\infty}$ be all the field embeddings $L \to \mathbb{R}$ which upon restriction to K lie in $\mathfrak{m}_\infty$. We will often drop the subscript L in $\mathfrak{m}_L$ for the sake of brevity.

Definition 3.1.2. Let K be a number field and $\mathfrak{m}$ a modulus of K. For $\alpha, \beta \in K^*$ we write

$$\alpha \equiv^* \beta \pmod{\mathfrak{m}}$$

if

i) $\mathrm{ord}_{\mathfrak{p}}(\alpha/\beta - 1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$ for all $\mathfrak{p} \mid \mathfrak{m}_0$;
ii) $\tau(\alpha/\beta) > 0$ for all $\tau \in \mathfrak{m}_\infty$.

Note that i) generalizes the usual congruence on O_K to K while ii) tells us that α and β have the same sign under all the embeddings lying in $\mathfrak{m}_\infty$. Moreover, the congruence is multiplicative by definition.

We can use this congruence to refine the class group. For any modulus $\mathfrak{m}$, let $I_K^{\mathfrak{m}}$ be the free group generated by the prime ideals of O_K that do not divide $\mathfrak{m}_0$. Furthermore, let $P_K^{\mathfrak{m}} \subset I_K^{\mathfrak{m}}$ be the subgroup of principle (fractional) ideals generated by α such that $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$.

Definition 3.1.3. Let K be a number field and $\mathfrak{m}$ a modulus of K. The *ray class group* $\mathrm{Cl}_K^{\mathfrak{m}}$ *modulo* $\mathfrak{m}$ is the quotient group

$$\mathrm{Cl}_K^{\mathfrak{m}} = I_K^{\mathfrak{m}} / P_K^{\mathfrak{m}}.$$

Similar to the class group, one can show that the ray class group modulo $\mathfrak{m}$ is a finite group [31, Cor. 1.6, p. 161]. In fact, if one takes $\mathfrak{m}$ to be the trivial modulus of K, then the ray class group modulo $\mathfrak{m}$ happens to be the class group of K.

3.2 Artin map

Let L/K be a finite Galois extension of number fields with Galois group G and fix a finite K-prime $\mathfrak{p}$. In the previous chapter we defined the decomposition group $D(\mathfrak{q}/\mathfrak{p})$ of $\mathfrak{q}/\mathfrak{p}$ for a finite L-prime $\mathfrak{q}$ above $\mathfrak{p}$ to be the stabilizer of $\mathfrak{q}$ under the Galois action on the finite set $\Sigma_{\mathfrak{p}}$ of L-primes above $\mathfrak{p}$. Explicitly

$$D(\mathfrak{q}/\mathfrak{p}) = \{\sigma \in G \mid \sigma\mathfrak{q} = \mathfrak{q}\}.$$

Now write $\kappa(\mathfrak{q})$ and $\kappa(\mathfrak{p})$ for the residue class field of $\mathfrak{q}$ and $\mathfrak{p}$, respectively. Since any $\sigma \in D(\mathfrak{q}/\mathfrak{p})$ fixes $\mathfrak{q}$, it induces an element in $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ given by $\overline{x} \mapsto \sigma(\overline{x})$. We therefore obtain a homomorphism

$$\phi_{\mathfrak{q}/\mathfrak{p}} : D(\mathfrak{q}/\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})).$$

Lemma 3.2.1. *Let L/K be a finite Galois extension of number fields and $\mathfrak{p}$ a finite K-prime. Then*

i) for all $\mathfrak{q} \in \Sigma_{\mathfrak{p}}$ the map $\phi_{\mathfrak{q}/\mathfrak{p}}$ is surjective;
ii) if L/K is abelian, then $\phi_{\mathfrak{q}/\mathfrak{p}}$ only depends on $\mathfrak{p}$.

Proof. For i), let α be a primitive element of $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ and use the Chinese remainder theorem to find some $\beta \in \mathcal{O}_L$ such that $\beta \equiv \alpha \pmod{\mathfrak{q}}$ and $\beta \equiv 0 \pmod{\sigma^{-1}(\mathfrak{q})}$ for all $\sigma \notin D(\mathfrak{q}/\mathfrak{p})$. Define

$$f(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (x - \sigma(\beta)) \in \mathcal{O}_K[x].$$

Note that $f^{\alpha}_{\kappa(\mathfrak{p})} \mid \bar{f}$ in $\kappa(\mathfrak{p})[x]$ and thus if $\alpha \neq 0$ (for $\alpha = 0$ the statement holds trivially)

$$f^{\alpha}_{\kappa(\mathfrak{p})} \mid \prod_{\sigma \in D(\mathfrak{q}/\mathfrak{p})} (x - \sigma(\beta)).$$

It follows that for all $\tau \in \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$, there exists some $\sigma \in D(\mathfrak{q}/\mathfrak{p})$ such that $\tau(\alpha) = \sigma(\beta)$ in $\kappa(\mathfrak{p})$. Hence $\phi_{\mathfrak{q}/\mathfrak{p}}(\sigma) = \tau$.

For ii), it is sufficient to proof that $\tau D(\mathfrak{q}/\mathfrak{p})\tau^{-1} = D(\tau(\mathfrak{q})/\mathfrak{p})$ for $\tau \in G$ as G acts transitively on $\Sigma_{\mathfrak{p}}$ by Lemma 2.2.9 and conjugation is trivial in abelian groups. But this identity is obvious: if $\sigma \in G$ fixes $\mathfrak{q}$ then $\tau\sigma\tau^{-1}$ fixes $\tau(\mathfrak{q})$. Conversely, if σ fixes $\tau(\mathfrak{q})$, then $\tau^{-1}\sigma\tau$ fixes $\mathfrak{q}$. □

The kernel of $\phi_{\mathfrak{q}/\mathfrak{p}}$ is called the *inertia group of* $\mathfrak{q}/\mathfrak{p}$ and is denoted as $I(\mathfrak{q}/\mathfrak{p})$. By the lemma above and the fact that $\#D(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{p})f(\mathfrak{p})$ by Lemma 2.2.9, we find that $\#I(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{p})$ hence $\phi_{\mathfrak{q}/\mathfrak{p}}$ is an isomorphism of groups if and only if $\mathfrak{p}$ is unramified in L/K. Now, the residue field extension $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is an extension of finite fields and much is known about the Galois group of finite field extensions. Indeed, we know that is generated by the Frobenius endomorphism $x \mapsto x^{\mathrm{Char}(\kappa(\mathfrak{p}))}$. Thus, if $\mathfrak{p}$ is unramified in L/K, then there exists an unique element $\mathrm{Frob}(\mathfrak{q}/\mathfrak{p}) \in D(\mathfrak{q}/\mathfrak{p})$, called the *Frobenius element of* $\mathfrak{q}/\mathfrak{p}$, such that $\phi_{\mathfrak{q}/\mathfrak{p}}(\mathrm{Frob}(\mathfrak{q}/\mathfrak{p}))$ is the Frobenius endomorphism in $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$.

Additionally, if L/K is abelian, then the map $\phi_{\mathfrak{q}/\mathfrak{p}}$ is independent on the chosen prime $\mathfrak{q}$ and thus so is the Frobenius element of $\mathfrak{q}/\mathfrak{p}$. Therefore, we are permitted to write $\mathrm{Frob}(\mathfrak{p})$ which leads us to the following crucial map.

Definition 3.2.2. Let L/K be a finite abelian extension of number fields and $\mathfrak{m}$ a modulus of K such that $\mathfrak{m}_0$ contains all ramified primes in L/K. The *Artin map* $\mathrm{Art}^{\mathfrak{m}}_{L/K}$ *of* $\mathfrak{m}$ is the map

$$\begin{aligned} \mathrm{Art}^{\mathfrak{m}}_{L/K} : I^{\mathfrak{m}}_K &\to \mathrm{Gal}(L/K) \\ \mathfrak{p} &\mapsto \mathrm{Frob}(\mathfrak{p}). \end{aligned}$$

3.3 Statement of class field theory

As alluded to earlier, class field theory attempts to describe the abelian extensions of a number field K. There are various approaches one can take to formulate class field theory,

but we will describe it through Artin reciprocity, which basically states that the Artin map induces an isomorphism between the subextensions of an arbitrary finite abelian extension L/K and the subgroups of $I_K^{\mathfrak{m}}$ containing $P_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$ of K.

Theorem 3.3.1 (Artin reciprocity)**.** *Let L/K be a finite abelian extension of number fields. Then there exists a modulus $\mathfrak{m}$ of K, with $\mathfrak{m}_0$ containing all ramified primes in L/K, such that*

i) $\mathrm{Art}_{L/K}^{\mathfrak{m}}$ *is surjective;*

ii) the kernel of $\mathrm{Art}_{L/K}^{\mathfrak{m}}$ *is* $P_K^{\mathfrak{m}} N_{L/K}(I_L^{\mathfrak{m}})$ *and* $\mathrm{Art}_{L/K}^{\mathfrak{m}}$ *induces an isomorphism of groups*

$$\mathrm{Cl}_K^{\mathfrak{m}} / N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}}) \simeq \mathrm{Gal}(L/K).$$

Sketch. The proof is far too large to completely write down in this thesis and as such we will only give the main ingredients. For a full proof we refer to [31].

For the first statement, note that if M is any intermediate extension of L/K then we have a commutative diagram

$$\begin{array}{ccc} I_K^{\mathfrak{m}} & \xrightarrow{\mathrm{Art}_{M/K}^{\mathfrak{m}}} & \mathrm{Gal}(M/K) \\ & \searrow^{\mathrm{Art}_{L/K}^{\mathfrak{m}}} & \uparrow \\ & & \mathrm{Gal}(L/K) \end{array}$$

Moreover, note that $\mathrm{Art}_{M/K}^{\mathfrak{m}}$ is well-defined by the multiplicity of the ramification indices. Let H be the image of $\mathrm{Art}_{L/K}^{\mathfrak{m}}$ and consider its fixed field $M = L^H$. By the diagram above it follows that $\mathrm{Art}_{M/K}^{\mathfrak{m}}$ is trivial. If we were to proof that $\mathrm{Art}_{N/K}^{\mathfrak{m}}$ is nontrivial whenever N/K is nontrivial then we are done since that would imply that $H = \mathrm{Gal}(L/K)$ by Galois theory. Notice that $\mathrm{Art}_{N/K}^{\mathfrak{m}}$ is trivial if and only if $f(\mathfrak{p}) = 1$ for all finite K-primes $\mathfrak{p}$. In other words, $\mathrm{Art}_{N/K}^{\mathfrak{m}}$ is trivial if and only if all unramified finite K-primes are completely split in N/K. The Chebotarev's density theorem [38, Thm. 13.4, p. 545] states that this is impossible if N/K is nontrivial, proving the desired.

The second statement is much harder. One starts by showing that $N_{L/K}(I_L^{\mathfrak{m}}) \subset \ker \mathrm{Art}_{L/K}^{\mathfrak{m}}$, which is rather easy since $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{p})}$ for any L-prime $\mathfrak{q}$ lying above a K-prime $\mathfrak{p}$. Then one proofs the first fundamental inequality $[\mathrm{Cl}_K^{\mathfrak{m}} : N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}})] \leq [L : K]$ with the use of analytical number theory. Combining these two statements, it follows that *ii*) holds if and only if $P_K^{\mathfrak{m}} \subset \ker \mathrm{Art}_{L/K}^{\mathfrak{m}}$. This observation is important as it allows us to reduce Artin reciprocity to the cyclic case. Indeed, by the structure theorem of finite abelian groups we have $\mathrm{Gal}(L/K) \simeq \prod_{i=1}^n H_i$ for some finite cyclic groups H_i. By writing $L_i = L^{H_i}$, it is easy to show that $\mathrm{Art}_{L/K}^{\mathfrak{m}} = \prod_{i=1}^n \mathrm{Art}_{L_i/K}^{\mathfrak{m}}$ and thus $P_K^{\mathfrak{m}} \subset \mathrm{Art}_{L/K}^{\mathfrak{m}}$ if and only if $P_K^{\mathfrak{m}} \subset \mathrm{Art}_{L_i/K}^{\mathfrak{m}}$ for all i.

Artin reciprocity is therefore proven if $P_K^{\mathfrak{m}} \subset \mathrm{Art}_{L/K}^{\mathfrak{m}}$ whenever L/K is a finite cyclic extension. This is done by showing that the second fundamental inequality holds, i.e.

$[\mathrm{Cl}_K^{\mathfrak{m}} : N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}})] \geq [L : K]$. Its proof is far from trivial and requires some more analytical number theory combined with group cohomology to shorten the computations considerably. Finally, the result follows after a very technical lemma due to Artin. □

Remark. The approach above is considered archaic for various reasons. First of all, the use of moduli is cumbersome, requiring a new modulus every time one considers a new extension. Secondly, the modern approach results in a far more powerful statement by describing all the finite abelian extensions with a single isomorphism:

$$\widehat{C_K} \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Here, K^{ab} is the maximal abelian extension of K (inside some fixed separable closure of K) while $\widehat{C_K}$ is the profinite completion of the *idéle class group*. This group is essentially a certain infinite product of the completions of K and hence encompasses all necessary information without having to worry about moduli, see [9, Ch. VII, Sec. 3]. However, a downside of this approach is that it requires a fair amount of topology.

A modulus $\mathfrak{m}$ of K such that Artin reciprocity holds for $(L/K, \mathfrak{m})$ is called an *admissible modulus of* L/K. One can show that the greatest common divisor of two admissible moduli is again admissible, implying the existence of the smallest admissible modulus of L/K. This modulus is called the *conductor of* L/K, derived from the German word *Führer*, and is denoted by $\mathfrak{f}_{L/K}$. Furthermore, one can show that a K-prime, both finite and infinite, divides the conductor if and only if it is ramified in L/K [31, Thm. 11.11, p. 226].

Historically speaking, it was not Artin who first proved the correspondence between subgroups of $I_K^{\mathfrak{m}}$ containing $P_K^{\mathfrak{m}}$ and intermediate extensions of L/K. Rather, he was the first who proved that there is a canonical way of viewing this correspondence. Before him, it was Takagi who proved the correspondence without making it explicit. As Hasse used Takagi's result, rather than Artin's result, let us briefly explain how Takagi formulated the correspondence.

A subgroup $H \subset I_K$ is said to be a *congruence subgroup* if there exists a modulus $\mathfrak{m}$ of K such that $P_K^{\mathfrak{m}} \subset H \subset I_K^{\mathfrak{m}}$. We say that two congruence subgroups H_1 and H_2 are equivalent, written $H_1 \sim H_2$, if there exists a modulus $\mathfrak{n}$ of K such that $H_1 \cap I_K^{\mathfrak{n}} = H_2 \cap I_K^{\mathfrak{n}}$. An equivalence class of congruence subgroups is called an *ideal group*. It can be shown that for every ideal group H there exists a modulus $\mathfrak{f}$ such that H contains a congruence subgroup modulo $\mathfrak{f}$ and every congruence subgroup modulo $\mathfrak{m}$ in H satisfies $\mathfrak{f} \mid \mathfrak{m}$ [31, Lem. 6.2, p. 201]. Fittingly, $\mathfrak{f}$ is called the *conductor of* H.

Definition 3.3.2. Let K be a number field and L a finite abelian extension of K. The ideal group H_L, or $H_{L/K}$, containing the congruence subgroups $\ker \mathrm{Art}_{L/K}^{\mathfrak{m}}$ for all admissible moduli $\mathfrak{m}$ of K is called the *ideal group of* L/K while L is called the *class field* of H_L.

Note that H_L is indeed an ideal group: if $\mathfrak{m}$ and $\mathfrak{n}$ are two admissible moduli of K then $\ker \mathrm{Art}_{L/K}^{\mathfrak{m}} \sim \ker \mathrm{Art}_{L/K}^{\mathfrak{n}}$ since

$$\ker\left(\mathrm{Art}_{L/K}^{\mathfrak{m}}\right) \cap I_K^{\mathfrak{m}\mathfrak{n}} = \ker\left(\mathrm{Art}_{L/K}^{\mathfrak{m}}|_{I_K^{\mathfrak{m}\mathfrak{n}}}\right) = \ker\left(\mathrm{Art}_{L/K}^{\mathfrak{n}}\right) \cap I_K^{\mathfrak{m}\mathfrak{n}}.$$

In turn, the conductor $\mathfrak{f}_{L/K}$ of L/K defined above coincides with the conductor of H_L.

Now, the first result in class field theory due to Takagi states that every ideal group is a class group of some abelian extension while, conversely, every abelian extension is a class field of some ideal group. Artin reciprocity can be used to proof this statement (note that Takagi did it without Artin reciprocity) together with some cumbersome computations, see [31, Thm. 9.9, p. 215].

Theorem 3.3.3. *Let K be a number field. There is a one-to-one, inclusion-reversing correspondence between the finite abelian extension of K and the ideal groups of K given by $L \mapsto H_L$.*

4 Hasse norm theorem

Using class field theory, Hasse managed to proof his norm theorem: an element in a cyclic extension is a norm if and only if it is a norm locally everywhere. In this chapter we will look at this theorem in depth and discuss both his original proof and a semi-modern proof using cohomology to showcase the usefulness of cohomology. Moreover, we will highlight recent developments of the Hasse norm theorem to abelian extensions and briefly elaborate how the Hasse-Minkowski theorem can be seen as a corollary of the Hasse norm theorem.

4.1 A semi-modern proof

Let us start with a semi-modern proof using cohomology which greatly simplifies things.

Lemma 4.1.1. *Let L/K be a finite cyclic extension of number fields with Galois group G, $\mathfrak{m}$ an admissible modulus of K and $\alpha \in K^*$ such that $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$. Then α is a norm from L if and only if (α) is the norm of an ideal from L.*

Sketch. First of all, note that we actually do not need the statements of class field theory. In fact, proving this statement is done while proving Artin reciprocity as it is a consequence of the second fundamental inequality. We therefore opt to not provide a full proof and instead give a brief sketch of the proof. The interested reader may consult [31, Ch. V].

Consider the mapping $f : L^* \to I_L^{\mathfrak{m}}$ where $x \in L^*$ is sent to its $\mathfrak{m}$-free part, i.e. factor $(x) = \mathfrak{ab}$ where $\mathfrak{b}$ is coprime to $\mathfrak{m}$ and set $f(x) = \mathfrak{b}$. Take cohomology to obtain a map $f^0 : H_T^0(G, L^*) \to H_T^0(G, I_L^{\mathfrak{m}})$. By definition, its domain is $K^*/N_{L/K}(L^*)$ while its codomain is $I_K^{\mathfrak{m}}/N_{L/K}(I_L^{\mathfrak{m}})$. If $K_{\mathfrak{m},1} \subset K^*$ denotes the subgroup of all $\beta \in K^*$ such that $\beta \equiv^* 1 \pmod{\mathfrak{m}}$, then a reduction modulo $K_{\mathfrak{m},1}$ yields the following commutative diagram

$$\begin{array}{ccccccccc}
 & & & & \ker g_1 & \longrightarrow & \ker g_2 & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \to & \ker f^0 & \longrightarrow & K^*/N_{L/K}(L^*) & \xrightarrow{f^0} & I_K^{\mathfrak{m}}/N_{L/K}(I_L^{\mathfrak{m}}) & \longrightarrow & \operatorname{coker} f^0 \to 1 \\
 & & & & \downarrow{\scriptstyle g_1} & & {\scriptstyle g_2}\downarrow & & \downarrow \\
1 & \to & \ker \overline{f^0} & \to & K^*/N_{L/K}(L^*)K_{\mathfrak{m},1} & \xrightarrow{\overline{f^0}} & \mathrm{Cl}_K^{\mathfrak{m}}/N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}}) & \to & \operatorname{coker} \overline{f^0} \to 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}$$

where g_1 and g_2 are the natural projection maps. It is easy to see that $\ker g_1 \to \ker g_2$ surjects and thus, in particular, the map $\ker f^0 \to \ker \overline{f^0}$ is surjective and $\operatorname{coker} f^0 \simeq \operatorname{coker} \overline{f^0}$ by the Snake lemma. One can then show that $q(\mathrm{Gal}(L/K), \ker f) = \#\operatorname{coker} f^0/\#\ker f^0$, hence $\ker \overline{f^0}$ and $\operatorname{coker} \overline{f^0}$ are both finite quantities. Setting $a(\mathfrak{m}) = [K^* : N_{L/K}(L^*)K_{\mathfrak{m},1}]$, it thus follows that

$$[L : K] = [\mathrm{Cl}_K^{\mathfrak{m}} : N_{L/K}(\mathrm{Cl}_L^{\mathfrak{m}})] = a(\mathfrak{m})q(\mathrm{Gal}(L/K), \ker f)\#\left(\ker f^0 \cap \ker g_1\right).$$

One then proceeds to prove that $\#(\ker f^0 \cap \ker g_1)$ is actually $[K_{\mathfrak{m},1} \cap \iota^{-1}(N_{L/K}(I_L^{\mathfrak{m}})) : K_{\mathfrak{m},1} \cap N_{L/K}(L^*)]$, where $\iota : L^* \to I_L$ is the natural inclusion. The statement is then proven if this quantity is 1. Equivalently, $a(\mathfrak{m})q(\mathrm{Gal}(L/K), \ker f) = [L : K]$. One can easily show that $q(\mathrm{Gal}(L/K), \ker f) = [L : K]/(\prod_{\mathfrak{p}|\mathfrak{m}} e(\mathfrak{p})f(\mathfrak{p}))$ by using the fact that $\ker f$ fits into a short exact sequence

$$1 \to \mathcal{O}_L^* \to \ker f \to I_{L,\mathfrak{m}_0} \to \mathrm{Cl}_K \to 1$$

where $I_{L,\mathfrak{m}_0} \subset \mathcal{I}_L$ is the subgroup of fractional ideals generated by the L-primes dividing $\mathfrak{m}_0$. Using properties of the Herbrand quotient the equality follows relatively quickly. The bulk of the statement lies primarily in the equality $a(\mathfrak{m}) = \prod_{\mathfrak{p}|\mathfrak{m}} e(\mathfrak{p})f(\mathfrak{p})$, which is proven by showing that it equals the Herbrand quotient of a certain group induced by the $\mathfrak{p}$-adic logarithm □

Now, we say that $\alpha \in K^*$ is a *(global) norm for L/K* if it is the norm of an element in L. Moreover, we say that α is a *local norm at a K-prime v for L/K* if α is the norm of an element in L_w for some L-prime w above v. Note that this is actually independent on the prime w and we will often write N_v for the norm map $N_{L_w/K_v} : L_w^* \to K_v^*$. Finally, we say that α is a *local norm everywhere for L/K* if it is a local norm at every K-prime for L/K.

Theorem 4.1.2 (Hasse norm theorem)**.** *Let L/K be a finite cyclic extension of number fields and $\alpha \in K^*$. Then α is a global norm for L/K if and only if α is a local norm everywhere for L/K.*

Proof. One direction is trivial. Indeed, suppose that α is a global norm and let $\beta \in L^*$ be such that $\alpha = N_{L/K}(\beta)$. Fix a K-prime v and a set of coset representatives $\tau_1, \dots, \tau_g$ of $D(v)$ in $\mathrm{Gal}(L/K)$. Then

$$N_v\left(\prod_{i=1}^{g} \tau_i(\beta)\right) = \prod_{i=1}^{g} \prod_{\sigma \in D(v)} (\sigma \circ \tau_i)(\beta) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta) = N_{L/K}(\beta) = \alpha.$$

The importance of the Hasse norm theorem lies in the converse. Suppose that α is a local norm everywhere for L/K. We first claim that (α) is a norm of an ideal in L. For any finite K-prime $\mathfrak{p}$ write $a_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(\alpha)$. We know that $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{p})}$ if $\mathfrak{q}$ lies above $\mathfrak{p}$, hence (α) is certainly a norm of an ideal if $f(\mathfrak{p}) \mid a_\mathfrak{p}$ for all $\mathfrak{p}$ such that $a_\mathfrak{p} \neq 0$. Fix such a K-prime $\mathfrak{p}$ together with a L-prime $\mathfrak{q}$ above it. Because α is a local norm everywhere for L/K per assumption, there exists some $\beta \in L_\mathfrak{q}$ such that $N_\mathfrak{p}(\beta) = \alpha$. By Theorem 2.2.6, the fractional ideal (β) in $L_\mathfrak{q}$ is simply a power of $\mathfrak{q}$, say $\mathfrak{q}^t$. Therefore

$$\mathfrak{p}^{a_\mathfrak{p}} = (N_\mathfrak{p}(\beta)) = N_\mathfrak{p}(\mathfrak{q}^t) = \mathfrak{p}^{tf(\mathfrak{p})}$$

as fractional ideals of $K_\mathfrak{p}$ and thus $f(\mathfrak{p}) \mid a_\mathfrak{p}$.

We conclude that (α) is the norm of an ideal in L. Our next step is to use the lemma above to find an admissible modulus $\mathfrak{m}$ of K such that $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$ to conclude that α is a global norm. However, there is no freedom in choosing the modulus hence we wish to alter α such that it satisfies the congruence condition.

Fix an admissible modulus $\mathfrak{m}$ of K and write

$$\mathfrak{m} = \prod_i v_i^{b_i}.$$

Moreover, fix an L-prime w_i above each v_i and let $e_i = e(v_i)$ denote the ramification index of v_i. Additionally, let $\beta_i \in L_{w_i}$ be such that $N_{v_i}(\beta_i) = \alpha$. If v_i is finite then L is dense in L_{w_i} and there exists some $\beta_i' \in L$ such that $\beta_i' - \beta_i \in w_i^{e_i b_i}$. If on the the other hand v_i is infinite, then simply set $\beta_i' = \beta_i$. Applying the approximation theorem (Theorem 2.2.4) to the set of L-primes $\{w \mid \exists i, w \mid v_i\}$ we obtain an element $\gamma \in L$ satisfying for all $w \mid v_i$ and i

$$\gamma \equiv^* \begin{cases} \beta_i' \pmod{w_i^{e_i b_i}} & \text{if } w = w_i, \\ 1 \pmod{w^{e_i b_i}} & \text{otherwise.} \end{cases}$$

Now, fix an index i and let $\tau_1, \dots, \tau_g$ be a set of coset representatives of $D(v_i)$ in $\mathrm{Gal}(L/K)$ with $\tau_1 = 1$. Then by construction for $j \neq 1$ we have $\tau_j(\gamma) \equiv^* 1 \pmod{w_i^{e_i b_i}}$.

It thus follows that

$$N_{L/K}(\gamma) = \prod_{j=1}^{g} \prod_{\sigma \in D(v_i)} (\sigma \circ \tau_j)(\gamma) \equiv^* \prod_{\sigma \in D(v_i)} \sigma(\gamma) = N_{v_i}(\gamma) \equiv^* N_{v_i}(\beta_i') \pmod{w_i^{e_i b_i}}.$$

We therefore conclude that $\alpha \equiv^* N_{L/K}(\gamma) \pmod{\mathfrak{m}}$ or equivalently, $\alpha N_{L/K}(\gamma)^{-1} \equiv^* 1 \pmod{\mathfrak{m}}$. We already know that (α) is the norm of an ideal of L and clearly so is $(N_{L/K}(\gamma)^{-1})$. Thus we conclude that $\alpha N_{L/K}(\gamma)^{-1}$ is the norm of an element in L. In other words, α is a global norm by the multiplicity of the norm map. □

4.2 Hasse's proof

The proof of the Hasse norm theorem in the previous section uses the power of cohomology. Interestingly, the theory of cohomology had not been formalised in the time of Hasse so his proof must have been different then the one above (see [51] for an overview of the history of homological algebra). This raises the question: how did he proof his theorem?

Hasse started by defining a symbol, i.e. a function. Let L/K be a finite abelian extension and $\mathfrak{p}$ a finite K-prime. For $\alpha \in K^*$, use the weak approximation theorem (Theorem 2.2.4) to find some $\alpha_0 \in K^*$ such that

$$\alpha_0 \equiv^* \begin{cases} \alpha & \bmod \mathfrak{p}^a \\ 1 & \bmod \frac{\mathfrak{f}}{\mathfrak{p}^a} \end{cases} \tag{4.1}$$

where $a \in \mathbb{Z}_{\geq 0}$ is the exponent of $\mathfrak{p}$ in $\mathfrak{f}$ and $\mathfrak{f}$ denotes the conductor of L/K. If $a = 0$, then we mean by the first congruence that α/α_0 is coprime to $\mathfrak{p}$. Factor the fractional K-ideal (α_0) into prime ideals and let $\mathfrak{a}$ be the factor of (α_0) coprime to $\mathfrak{p}$. By construction we then have that $\mathfrak{a}$ and $\mathfrak{f}$ are coprime and we define a symbol

$$\left(\frac{\alpha, L/K}{\mathfrak{p}}\right) = \mathrm{Art}_{L/K}^{\mathfrak{f}}(\mathfrak{a}) \subset \mathrm{Gal}(L/K).$$

We will often write $(\alpha, L/K)_{\mathfrak{p}}$ inline to be this symbol for the sake of compactness. Moreover, if σ is an infinite K-prime, then we set $(\alpha, L/K)_\sigma$ to be complex conjugation in $\mathrm{Gal}(L_\sigma/K_\sigma) \subset \mathrm{Gal}(L/K)$ if σ is ramified and $\sigma(\alpha) < 0$. Otherwise, we let it be the identity in $\mathrm{Gal}(L/K)$. We have therefore defined a symbol

$$\left(\frac{-, L/K}{v}\right) : K^* \to \mathrm{Gal}(L/K)$$

for all K-primes v called the *norm residue symbol at* v. Observe that the symbol is independent of the choice of α_0 for finite K-primes. Indeed, if we have that α_0' is another

element satisfying the congruence in (4.1) then $(\alpha_0/\alpha_0') \in P_K^{\mathfrak{f}}$. Therefore, if we denote $\mathfrak{a}'$ as the factor of (α_0') coprime to $\mathfrak{p}$, we have

$$\mathrm{Art}_{L/K}^{\mathfrak{f}}(\mathfrak{a}) = \mathrm{Art}_{L/K}^{\mathfrak{f}}\left(\frac{\alpha_0}{\alpha_0'}\mathfrak{a}'\right) = \mathrm{Art}_{L/K}^{\mathfrak{f}}(\mathfrak{a}')$$

by Artin reciprocity (Theorem 3.3.1).

Lemma 4.2.1. *Let L/K be a finite abelian extension of number fields and let v be a K-prime.*

i) For all $\alpha_1, \alpha_2 \in K^*$ we have

$$\left(\frac{\alpha_1\alpha_2, L/K}{v}\right) = \left(\frac{\alpha_1, L/K}{v}\right)\left(\frac{\alpha_2, L/K}{v}\right).$$

ii) If M is any intermediate field of L/K, then for all $\alpha \in K^*$

$$\left(\frac{\alpha, L/K}{v}\right)\Bigg|_M = \left(\frac{\alpha, M/K}{v}\right).$$

iii) If M is any intermediate field of L/K, then for all $\theta \in M^*$

$$\prod_{w|v}\left(\frac{\theta, L/M}{w}\right) = \left(\frac{N_{M/K}(\theta), L/K}{v}\right)$$

where the product ranges over all M-primes w lying above v.

Proof. The only nontrivial statement is *iii*) and we refer to Hasse [28, Teil II, p. 28] as it is rather involved to proof. □

The name of the symbol seems to suggest that it is related to the local norm at v for L/K but it is not entirely obvious how. For infinite primes this relation is clear: we have $(\alpha, L/K)_\sigma = 1$ if and only if α is a local norm at σ for L/K. Indeed, if σ is unramified then α is always a local norm at σ for L/K and, moreover, the norm residue symbol at v is the identity. Furthermore, if σ is ramified, then α is a local norm at σ for L/K if and only if $\sigma(\alpha) > 0$; coinciding with the definition of the norm residue symbol.

Lemma 4.2.2. *Let L/K be a finite abelian extension of number fields, $\alpha \in K^*$ and v a K-prime. Then*

$$\left(\frac{\alpha, L/K}{v}\right) = 1 \iff \alpha \text{ is a local norm at } v \text{ for } L/K.$$

Sketch. We only have to consider the case when $v = \mathfrak{p}$ for a finite K-prime $\mathfrak{p}$. The proof is rather long so we will only sketch the approach of Hasse [28, Teil II, Satz 2, p. 33].

An element $\gamma \in K^*$ is said to be a norm residue modulo a modulus $\mathfrak{m}$ of K if there exists some $\beta \in L^*$ such that $\gamma \equiv^* N_{L/K}(\beta) \pmod{\mathfrak{m}}$. We will show that $(\alpha, L/K)_\mathfrak{p} = 1$ if and only if α is a norm residue modulo $\mathfrak{p}^r$ for all $r \geq 0$, which proves the desired after passing to a $\mathfrak{p}$-adic limit.

First, suppose that α is a norm residue modulo all powers of $\mathfrak{p}$. Then α is in particular a norm residue modulo $\mathfrak{p}^a$, where $\mathfrak{p}^a$ is the $\mathfrak{p}$-th power in $\mathfrak{f}$, and there exists some $\beta \in L^*$ such that $\alpha \equiv^* N_{L/K}(\beta) \pmod{\mathfrak{p}^a}$. Apply the weak approximation theorem (Theorem 2.2.4) on L to find some $\beta_0 \in L^*$ satisfying the congruence in (4.1). Then by construction we have $\alpha_0 \equiv^* N_{L/K}(\beta_0) \pmod{\mathfrak{f}}$. If $\mathfrak{b}$ denotes the factor of (β_0) coprime to $\mathfrak{f}$, then, in particular, $(\alpha_0/N_{L/K}(\beta_0))N_{L/K}(\mathfrak{b}) = \mathfrak{a}$ and hence $\mathrm{Art}_{L/K}^\mathfrak{f}(\mathfrak{a}) = 1$ by Artin reciprocity. Therefore $(\alpha, L/K)_\mathfrak{p} = 1$.

The converse is much harder and we need the following fact: if N_r denotes the group of elements of K that are norm residues modulo $\mathfrak{p}^r$ then $[K^* : N_r] \leq e(\mathfrak{p})f(\mathfrak{p})$ [28, Teil II, p. 30]. Let $J \subset K^*$ denote the kernel of the norm residue symbol $(-, L/K)_\mathfrak{p}$ at $\mathfrak{p}$. By the paragraph above we have that $N_r \subset J$ and the desired follows if this is an equality. Moreover, it is sufficient to proof that $D(\mathfrak{p}) \subset H$, where H is the image of $(-, L/K)_\mathfrak{p}$, since $\#D(\mathfrak{p}) = e(\mathfrak{p})f(\mathfrak{p})$ by Lemma 2.2.9. To show this, let $\sigma \in D(\mathfrak{p})$. By Artin reciprocity there exists some ideal $\mathfrak{b}$ coprime to $\mathfrak{f}$ such that $\mathrm{Art}_{L/K}^\mathfrak{f}(\mathfrak{b}) = \sigma$. Now denote $Z = L^{D(\mathfrak{p})}$ and $T = L^{I(\mathfrak{p})}$. By the classification theorem, $\mathfrak{b} \in H_Z$. Observe that $\mathfrak{p}$ is completely split in Z hence $\mathfrak{p} \in H_Z$. On the other hand, $\mathfrak{p}$ is not completely split in T and thus $\mathfrak{p} \notin H_T$ yet $\mathfrak{p}^{f(\mathfrak{p})} \in H_T$. Thus there exists some $b \in \mathbb{Z}_{\geq 0}$ such that $\mathfrak{p}^b\mathfrak{b} \in H_T$.

Now, T is the largest intermediate field of L/K such that $\mathfrak{p}$ is unramified in T/K. As such, H_T is the smallest ideal group such that $\mathfrak{p}$ does not divide its conductor. It can then be shown that $H_T = H_L P_K^{\mathfrak{f}/\mathfrak{p}^a}$ and thus there exist some $\zeta \in K^*$ with $\zeta \equiv^* 1 \pmod{\mathfrak{f}/\mathfrak{p}^a}$ and $\mathfrak{a} \in H_L$ such that

$$\mathfrak{p}^b\mathfrak{b} = \mathfrak{a}(\zeta).$$

By construction we then have $\mathrm{Art}_{L/K}^\mathfrak{f}(\mathfrak{b}) = (\zeta, L/K)_\mathfrak{p}$, proving the desired. □

Remark. The proof of the lemma above shows in particular that we have a surjection

$$\left(\frac{-, L/K}{\mathfrak{p}}\right) : K^* \to D(\mathfrak{p})$$

whose kernel is precisely all the elements of K^* that are local norms. Interestingly, this map is still ubiquitous in local class field theory, albeit it is constructed in a completely different manner. Indeed, local class field theory states that there is a canonical isomorphism

$$\theta_\mathfrak{p} : K_\mathfrak{p}^*/N_\mathfrak{p}(L_\mathfrak{p}^*) \to D(\mathfrak{p})$$

called the *local Artin map*, which is constructed completely abstractly from Tate's theorem in group cohomology, see [36] or [23]. The norm residue symbol at $\mathfrak{p}$ is then simply the composition of the inclusion $K^* \to K_{\mathfrak{p}}^*$ with the local Artin map.

The norm residue symbol at v therefore tells us something abstractly, i.e. whenever an element is a local norm at v, while its definition is rather explicit. It was hence this symbol that allowed Hasse to proof his norm theorem.

Theorem 4.2.3. *Let L/K be a finite cyclic extension of number fields and $a \in K^*$. Then*

$$\alpha \text{ is a global norm } \iff \left(\frac{\alpha, L/K}{v}\right) = 1 \text{ for all } K\text{-primes } v.$$

Proof. Hasse proceeds by induction on the degree of L/K, where the base case is when the degree is prime. For sake of brevity, we will skip the base case and refer the reader to [27, Teil II, p. 38] for the proof. Hence assume that the statement holds for all cyclic extensions M of K that are either of prime degree or whose degree is less than L/K. Note that one direction is always trivial: if α is a global norm then it is in particular a norm residue modulo all finite primes and their powers, and thus $(\alpha, L/K)_v = 1$ by the proof of Lemma 4.2.2.

For the converse, suppose that $(\alpha, L/K)_v = 1$ for all K-primes v and let M be any intermediate field of L/K such that M/K is of prime degree ℓ. Then by Lemma 4.2.1 *ii*) we have $(\alpha, M/K)_v = 1$ for all K-primes v. The induction hypothesis then states that α is a global norm of M/K, i.e. there exists some $\theta_0 \in M^*$ such that $\alpha = N_{M/K}(\theta_0)$. More specifically, Hilbert 90 (Theorem 2.3.5) states that a general solution to this equation is given by

$$\theta = \theta_0 \omega \sigma^{-1}(\omega)$$

with $\omega \in M^*$ and σ the generator of $\mathrm{Gal}(M/K)$. Our goal now is to choose ω in such a manner that $(\theta, L/M)_w = 1$ for all M-primes w as the induction hypothesis then states that θ is a global norm of L/M, implying that α is a global norm of L/K. It is easy to see that this is independent of the infinite primes and we only have to consider the finite M-primes.

Fix a finite M-prime $\mathfrak{q}$ and let $\mathfrak{p}$ be the K-prime below $\mathfrak{q}$. Since the degree of M/K is prime, $\mathfrak{p}$ is completely split, completely ramified or inert. In the latter two cases, $\mathfrak{q}$ is the only M-prime above $\mathfrak{p}$ and by applying Lemma 4.2.1 *iii*) we therefore conclude

$$\left(\frac{\theta, L/M}{\mathfrak{q}}\right) = \left(\frac{N_{L/M}(\theta), L/K}{\mathfrak{p}}\right) = \left(\frac{\alpha, L/K}{\mathfrak{p}}\right) = 1,$$

independent on the choice of ω. The only possible obstructions are hence the M-primes that lie above a completely split K-prime. We consider two cases: 1) $\mathfrak{q} \mid (\theta_0)$ or $\mathfrak{q}$ is ramified in L/M and 2) $\mathfrak{q} \nmid (\theta_0)$ and $\mathfrak{q}$ is unramified in L/M.

Let us first tackle the former. Note that $\mathfrak{p}\mathcal{O}_L = \prod_{i=0}^{\ell-1} \sigma^i(\mathfrak{q})$ by Lemma 2.2.9. Applying Lemma 4.2.1 *i*) and *iii*) yields $(\theta, L/M)_\mathfrak{q} = 1$ if and only if

$$\left(\frac{\omega, L/M}{\sigma^i(\mathfrak{q})}\right) = \left(\frac{\omega, L/M}{\sigma^{i-1}(\mathfrak{q})}\right)\left(\frac{\theta_0, L/M}{\sigma^i(\mathfrak{q})}\right)^{-1}$$

for all $i \in \{1, \dots, \ell - 1\}$. By the definition of the norm residue symbol, such an equality holds under a certain congruence condition modulo $\sigma^i(\mathfrak{q})$. As there are only finitely many primes that are either ramified in L/M or divide θ_0, we can find an ω simultaneously satisfying the equality above.

So it is left to show that with the above choice of ω we have $(\theta, L/M)_\mathfrak{q} = 1$ for all unramified $\mathfrak{q}$ lying above a completely split K-prime not dividing θ_0. Note that if $\mathfrak{q}$ is unramified and does not divide θ, then $(\theta, L/M)_\mathfrak{q} = 1$. Hence we only need to consider the unramified primes dividing $\omega\sigma^{-1}(\omega)$. Write $(\omega) = \mathfrak{t}\mathfrak{m}$ with $\mathfrak{m}$ coprime to $\mathfrak{f}_{L/M}$. Because L/K is cyclic, there exists a K-prime $\mathfrak{c}$ that is inert in L/K. Such a prime does not map to 1 under the Artin map of L/M and thus in particular there exists some $a \in \mathbb{Z}_{\geq 1}$ such that $\mathrm{Art}_{L/M}^{\mathfrak{f}_{L/M}}(\mathfrak{m}\mathfrak{c}^a) = 1$. By Artin reciprocity (Theorem 3.3.1) it follows that $\mathfrak{m}\mathfrak{c}^a = \mathfrak{r}\gamma$ for some $\gamma \equiv^* 1 \pmod{\mathfrak{f}_{L/M}}$ and $\mathfrak{r}$ some M-prime.

Now update θ by setting $\theta = \theta_0(\omega\gamma)\sigma^{-1}(\omega\gamma)$. As before we have $(\theta, L/M)_\mathfrak{q} = 1$ for all M-primes $\mathfrak{q}$ except possibly for those that lie above a completely split K-prime. If $\mathfrak{q}$ lies above a completely split K-prime and is either ramified or divides θ_0, then the equality $\mathfrak{r}\gamma = \mathfrak{m}\mathfrak{t}$ states that $(\gamma\sigma^{-1}(\gamma), L/M)_\mathfrak{q} = 1$ and thus in particular $(\theta, L/M)_\mathfrak{q} = 1$. If on the other hand $\mathfrak{q}$ is unramified and divides $\omega\gamma\sigma^{-1}(\gamma\omega)$, then $(\theta, L/M)_\mathfrak{q}$ can only differ from 1 when $\mathfrak{q} \mid \mathfrak{r}\sigma(\mathfrak{r})$. Yet $(\theta, L/M)_\mathfrak{r} = 1 = (\theta, L/M)_{\sigma(\mathfrak{r})}$, proving the desired. □

As one can see, the original proof by Hasse is complicated and we have even skipped some major details. By using modern tools such as cohomology, the semi-modern proof greatly reduces the complexity of the proof while still using the ideal-theoretic setup of class field theory. That said, if one uses the idélic approach to class field theory, the Hasse norm theorem is an immediate consequence of the cohomology of the idéle class group, see [38, Ch. VI, Cor. 4.5, p. 384] and/or [36, Ch. VIII, Thm. 3.1, p. 234].

4.3 Further developments

The study of the local-global principle for field norms did not end with Hasse's norm theorem; many authors tried, successfully, to proof the Hasse norm theorem for noncyclic extension or even non-Galois extensions. However, one does have to be slightly careful when generalising the property of being a local norm everywhere in non-Galois extensions as the completions need not be isomorphic and can depend on the chosen prime above.

Definition 4.3.1. Let L/K be a finite extension of number fields, $\alpha \in K^*$ and v a K-prime. We say that α is a *local norm at v for L/K* if

$$\alpha = \prod_{w|v} N_{L_w/K_v}(\beta_w)$$

for some $\beta_w \in L_w^*$ as w ranges over all L-primes lying over v.

Moreover, α is a *local norm everywhere for L/K* if α is a local norm at all K-primes for L/K.

Note that this coincides with the definition for Galois extensions L/K: all completions are isomorphic by Lemma 2.2.10 and we can simply take all but one β_w to be 1.

On this note, one may wonder why we did not define being a local norm in a more natural way, i.e. α is a local norm at a prime v for L/K if for all L-primes w there exists some $\beta_w \in L_w^*$ such that $x = N_{L_w/K_v}(\beta_w)$. This, however, introduces some problems. Since we are studying a local-global phenomenon, it would certainly be wise for the trivial direction, i.e. global norm implies being a local norm everywhere, to be true. If we had defined being a local norm in the above manner, then this would not be true. Take for example $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, which has two nonreal embeddings. As such, -1 is not a local norm at the infinite prime for $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, yet it is a global norm since $N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(-1) = -1$. Our definition does not have this issue as by the proof of Theorem 4.1.2 we have for all $\beta \in L^*$

$$N_{L/K}(\beta) = \prod_{w|v} N_{L_w/K_v}(\beta)$$

for all K-primes v and thus being a global norm implies being a local norm everywhere.

Definition 4.3.2. Let L/K be a finite extension of number fields. We say that the *Hasse norm principle (HNP)* holds for L/K if any $\alpha \in K^*$ that is a local norm everywhere for L/K is a global norm for L/K.

Using the definition of being a local norm, it is quite easy to relate the validity of the HNP in an extension to the validity of the HNP in one of its superextensions under some mild assumptions.

Lemma 4.3.3. *Let $M/L/K$ be a tower of finite extensions of number fields such that $n = [M : L]$ and $m = [L : K]$ are coprime. Then the HNP holds for L/K if the HNP holds for M/K.*

Proof. Suppose that α is a local norm everywhere for L/K and fix a K-prime v. Then there exists $\beta_w \in L_w$, where w ranges over all L-primes lying over v, such that

$$\alpha = \prod_{w|v} N_{L_w/K_v}(\beta_w).$$

But then as u ranges over all M-primes lying over v we have

$$\prod_{u|v} N_{M_u/K_v}(\beta_w) = \prod_{w|v} \prod_{u|w} N_{L_w/K_v}(\beta_w)^{[M_u:L_w]} = \prod_{w|v} N_{L_w/K_v}(\beta_w)^n = \alpha^n$$

hence α^n is a global norm for M/K and there exists some $\gamma \in M^*$ such that $N_{M/K}(\gamma) = \alpha^n$. Now, there exists some $r, s \in \mathbb{Z}$ such that $mr + ns = 1$ since m and n are coprime by assumption. It follows that

$$N_{L/K}(\alpha^r N_{M/L}(\gamma^s)) = \alpha^{mr+ns} = \alpha.$$

□

Remark. A more general statement by Gurak [24] states that if M/K is abelian, then the HNP holds for any subextension of M/K if the HNP holds for M/K. The proof relies on the idélic formulation of the Hasse norm principle, hence we will not treat it here.

Lemma 4.3.4. *Let L/K and M/K be finite extensions of number fields such that their degrees $n = [L : K]$ and $m = [M : K]$ are coprime. Let Ω/K denote the compositum of L/K and M/K inside some fixed separable closure. Then the HNP holds for Ω/K if and only if the HNP holds for both L/K and M/K.*

Proof. If the HNP holds for Ω/K then so does the HNP hold for both L/K and M/K by Lemma 4.3.3. For the converse, suppose that α is a local norm everywhere for Ω/K and fix a K-prime v. Thus there exists a collection $\gamma_u \in \Omega_u$, where u ranges over all the Ω-primes lying above v, such that $\alpha = \prod_{u|v} N_{\Omega_u/K_v}(\gamma_u)$. We can then write

$$\alpha = \prod_{w|v} \prod_{u|w} N_{M_w/K_v}(N_{\Omega_u/M_w}(\gamma_u)) = \prod_{w|v} N_{M_w/K_v}\left(\prod_{u|w} N_{\Omega_u/M_w}(\gamma_u)\right).$$

Hence α is a local norm everywhere for M/K and by assumption there exists some β_M such that $N_{M/K}(\beta_M) = \alpha$. Similarly, by considering the tower $\Omega/L/K$ there exists some β_L such that $N_{L/K}(\beta_L) = \alpha$. Now, let $r, s \in \mathbb{Z}$ be such that $mr + ns = 1$. Then

$$N_{\Omega/K}(\beta_L^r \beta_M^s) = N_{L/K}(N_{\Omega/L}(\beta_L^r)) N_{M/K}(N_{\Omega/M}(\beta_M^s)) = \alpha^{mr+ns} = \alpha.$$

□

Besides these simple lemmas, there are also concrete cases where the HNP is known to hold. The following list is due to Macedo and Newton [35].

Theorem 4.3.5. *Let L/K be a finite extension of number fields and N/K the normal closure of L/K. Then the HNP is known to hold for L/K if one of the following holds:*

i) L/K *is cyclic (Hasse norm theorem);*
ii) $[L : K]$ *is prime [5];*
iii) $[L : K] = n$ *and* $\mathrm{Gal}(N/K) \simeq S_n$ *[50] or* D_n *[4];*
iv) $[L : K] = n \geq 5$ *and* $\mathrm{Gal}(N/K) \simeq A_n$ *[34].*

We would also like to highlight recent work by Oki [39] on the failure of the HNP: if d is a squarefree composite number that is divisible by at least one of 3, 55, 91 or 95, then there exists a finite extension L/K of number fields of degree d such that the HNP fails to hold for L/K.

Additionally, there are more analytical result regarding the validity of the HNP. For a nontrivial finite abelian group G and a number field K we mean by a G-extension of K an abelian extension L/K such that $\mathrm{Gal}(L/K) \simeq G$. Frei, Loughran and Newton [17] showed that, when G is noncyclic, there always exists some G-extension of K which does not satisfy the HNP. Moreover, they [18] proved that 100% of all G-extensions of K satisfy the HNP, when ordered by conductor. That is, the limit of all G-extensions of K that do not satisfy the HNP tends to zero as the conductor tends to infinity. We remark that the ordering is important here; the authors could only establish similar results when ordered by discriminant if $G/G[p]$ is cyclic, where p is the smallest prime divisor of $\#G$. Nonetheless, this limit ordered by discriminant was later further investigated by Koymans and Rome [33] and they succeeded in proving that this limit at least exists for all G.

4.4 Hasse-Minkowski

Earlier, we have explained that the Hasse norm theorem is an instance of the local-global principle. One of the most popular instances of the local-global principle is the Hasse-Minkowski theorem which states that quadratic forms over a number field is isotropic if and only if it is isotropic locally everywhere. In this section we will follow [9, Ex. 4, p. 357] to show that the Hasse-Minkowski theorem is actually a consequence of the Hasse norm theorem. Do note, however, that the Hasse-Minkowski theorem was proven a few years prior to the Hasse norm theorem: first in 1890 by Minkowski over $\mathbb{Q}$ [37] and later in 1924 by Hasse over any number field [26].

Let K be a number field. Recall that a quadratic form q over K of degree n is a homogeneous polynomial of degree 2 in n variables, i.e.

$$q(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$$

for $a_{ij} \in K$. Since K is of characteristic zero, we can complete the square and assume

without loss of generality that any such quadratic form q is given by a diagonal form

$$q(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i^2$$

for $a_i \in K$. Finally, we say that q is isotropic if there exists some nonzero $x \in K^n$ such that $q(x) = 0$. More generally, we say that q represents $c \in K^*$ if there exists some $x \in K^n$ such that $q(x) = c$.

If q is a quadratic form over K, then q is a quadratic form over K_v for all K-primes v as $K \subset K_v$. Thus q is clearly isotropic locally everywhere if q is isotropic over K. The Hasse-Minkowski theorem states that the converse is also true. For the proof we use the following lemmas to relate the property of a quadratic form being isotropic with the property of certain elements being norms.

Lemma 4.4.1. *Let K be a number field and let $q = x_1^2 - bx_2^2 - cx_3^2$ be a quadratic form over K of degree 3 such that $b, c \neq 0$. Then the following are equivalent:*

i) q is isotropic;
ii) c is a norm of an element in $K(\sqrt{b})$.

Proof. The statement is clear if b is a square so suppose that b is not a square. If $(x_1, x_2, x_3) \in K^3$ is a nonzero solution to $q(x_1, x_2, x_3) = 0$ then $x_3 \neq 0$ as b is not a square and thus c is the norm of $x_1/x_3 + x_2/x_3\sqrt{b}$. Conversely, if c is the norm of an element in $K(\sqrt{b})$, say $x_1 + x_2\sqrt{b}$, then $q(x_1, x_2, 1) = 0$. □

Lemma 4.4.2. *Let K be a number field and let $q = x_1^2 - bx_2^2 - cx_3^2 + acx_4^2$ be a quadratic form over K of degree 4 such that $a, b, c \neq 0$. Then the following are equivalent:*

i) q is isotropic;
ii) c is a product of a norm of an element in $K(\sqrt{a})$ and a norm of an element in $K(\sqrt{b})$;
iii) c as an element of $K(\sqrt{ab})$ is a norm of an element in $L = K(\sqrt{a}, \sqrt{b})$.

Proof. *i)* and *ii)* are clearly equivalent as $q(x_1, x_2, x_3, x_4) = 0$ for $x_1, x_2, x_3, x_4 \in K$ not all zero if and only if $N_{K(\sqrt{b})/K}(x_1 + x_2\sqrt{b})N_{K(\sqrt{a})/K}(x_3 + x_4\sqrt{a})^{-1} = c$.

For the equivalence of *ii)* and *iii)*, note that $\mathrm{Gal}(L/K) \simeq V_4$ and write ρ, σ and τ as the three nontrivial elements of $\mathrm{Gal}(L/K)$ fixing $\sqrt{ab}$, $\sqrt{a}$ and $\sqrt{b}$, respectively. In this setting, we have that c is a product of a norm in $K(\sqrt{a})$ and a norm in $K(\sqrt{b})$ if and only if there exists some $x, y \in L^*$ with $\sigma(x) = x$ and $\tau(y) = y$ such that $xy\rho(xy) = c$. But then $N_{L/K(\sqrt{ab})}(xy) = c$, proving that *ii)* implies *iii)*. Conversely, suppose that $c \in K(\sqrt{ab})$ is the norm of an element in L, say z. Then $z\rho(z) = c$ by definition and by setting $u = c^{-1}\sigma(z)z$ we see that

$$\sigma(u) = u \quad \text{and} \quad u\rho(u) = 1.$$

In other words, $u \in K(\sqrt{a})$ and $N_{K(\sqrt{a})/K}(u) = 1$. Thus by Hilbert 90 (Theorem 2.3.5) there exists some $x \in K(\sqrt{a})$ with $\rho(x)x^{-1} = u$. But then $xy\rho(xy) = c$, proving the desired. □

Theorem 4.4.3 (Hasse-Minkowski)**.** *Let q be a quadratic form over a number field K. Then q is isotropic over K if and only if q is isotropic locally everywhere.*

Proof. We proceed by induction on the degree n of q and split into five different cases: $n = 1, 2, 3, 4$ and $n \geq 5$. The statement is trivial for $n = 1$. For $n = 2$ we note that any quadratic form of degree 2 is of the form $q = x_1^2 - bx_2^2$ with b nonzero. Such a quadratic form is isotropic if and only if b is a square in K hence the Hasse-Minkowski theorem follows for $n = 2$ if we can proof that squares satisfy the local-global principle. Clearly, if b is a square in K then it is a square locally everywhere. Conversely, if b is a square locally everywhere, then $K_v(\sqrt{b}) = K_v$ for all K-primes v. It follows that all primes are completely split and hence $\mathrm{Gal}(K(\sqrt{b})/K) = 1$ by Chebotorev's density theorem [38, Thm. 13.4, p.545].

For $n = 3$ and 4 we can reduce to the Hasse norm theorem by using Lemma 4.4.1 and Lemma 4.4.2. Indeed, as $K(\sqrt{b})/K$ and $K(\sqrt{a}, \sqrt{b})/K(\sqrt{ab})$ are cyclic extension of degree 2 the result immediately follows.

The final case concerning $n \geq 5$ is a simple induction argument. Write $q = ax_1^2 + bx_2^2 - g$ for some quadratic form g over K of degree $n - 2 \geq 3$. Let S be the finite set of K-primes that are infinite, divide 2 or divide one of the coefficients of g. It is easy to see that outside of S the quadratic form g represents everything (Reduce to the case of degree 3 and note that g is isotropic over the residue field by a similar argument as in Lemma 4.4.1. Then apply Hensel's Lemma 2.2.8). For the K-primes v in S, we notice that K_v^{*2} is a dense subset of K_v^* and hence by the weak approximation theorem (Theorem 2.2.4) there exists some $x_1, x_2 \in K^*$ such that g represents $c = ax_1^2 + bx_2^2 \neq 0$ over K_v for all $v \in S$. Hence g represents c in particular everywhere locally. In turn, the quadratic form $cx^2 - g$ of degree $n - 1$ is isotropic over K by induction, hence so is q. □

5 Abelian counterexamples

Hasse originally asserted that his norm theorem should hold for abelian extensions but was unable to provide a proof as his result relied on various technical lemmas that were only proven for cyclic extensions [28, p. 38]. In 1931, he retracted his statement and provided a counterexample [27]: the element 3 in the biquadratic field $\mathbb{Q}(\sqrt{-3}, \sqrt{-39})$ is a local norm everywhere but not a global norm. In 1967, Tate gave another counterexample of a biquadratic field not satisfying the HNP [9, Ex. 5.3, p. 360]: there exist infinitely many rational squares, such as 5^2, 7^2 and 10^2, that are local norms everywhere for $\mathbb{Q}(\sqrt{13}, \sqrt{17})/\mathbb{Q}$ but are not global norms. In this chapter we will mirror the approach by Tate to give a necessary, yet sufficient, condition for certain biquadratic fields to satisfy the HNP. Moreover, we will explicitly give elements that are local norms everywhere but not global norms in the case the condition fails to hold.

5.1 Biquadratic fields

A quartic Galois extension of $\mathbb{Q}$ is the smallest possible Galois counterexample to the Hasse norm theorem as all Galois extensions of degree two and three are cyclic. The biquadratic fields are a particular class of quartic extensions that are easy to work with as the splitting behavior of primes in these extensions can be completely determined by their quadratic subfields.

Definition 5.1.1. A *biquadratic field* is a quartic Galois extension of $\mathbb{Q}$ whose Galois group is the Klein four-group V_4. Explicitly, it is of the form $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ for some nonzero squarefree integers a and b.

An important property of a biquadratic field is that its only nontrivial subfields are quadratic fields and quadratic fields are easy to deal with as shown by the next lemma.

Lemma 5.1.2. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field with $D \in \mathbb{Z}$ squarefree. Then*

i)

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

ii) for an odd rational prime $p \in \mathbb{Z}$ we have

$$p \text{ is } \begin{cases} \textit{ramified} & \textit{if } \left(\frac{D}{p}\right) = 0, \\ \textit{split} & \textit{if } \left(\frac{D}{p}\right) = 1, \\ \textit{inert} & \textit{if } \left(\frac{D}{p}\right) = -1. \end{cases}$$

iii) for 2 we have

$$2 \textit{ is } \begin{cases} \textit{ramified} & \textit{if } D \equiv 2, 3 \pmod 4, \\ \textit{split} & \textit{if } D \equiv 1 \pmod 8, \\ \textit{inert} & \textit{if } D \equiv 5 \pmod 8. \end{cases}$$

Proof. The minimal polynomial of an element $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ is given by $x^2 - 2x + a^2 - Db^2$. Hence $\alpha \in O_K$ if and only if $2a, a^2 - Db^2 \in \mathbb{Z}$ and it is an easy exercise to show that this gives the desired characterisation of *i*).

For *ii*) and *iii*), note that the behavior of any rational prime $p \in \mathbb{Z}$ in K depends on the splitting of the polynomial $x^2 - D$, or $x^2 + x + \frac{1-D}{4}$ if $D \equiv 1 \pmod 4$, in $\mathbb{F}_p[x]$ by *i*). For odd p we have, in both cases, that this polynomial has a double root in $\mathbb{F}_p$ if p divides D, two distinct roots if D is a quadratic residue modulo p and no roots if D is not a quadratic residue modulo p, yielding the desired criterion. Moreover, $x^2 - D \equiv (x+1)^2 \pmod 2$ hence 2 is ramified in K if $D \equiv 2, 3 \pmod 4$. Additionally, if $D \equiv 1 \pmod 4$, then the polynomial $x^2 + x + \frac{1-D}{4}$ has two distinct roots in $\mathbb{F}_2$ if $D \equiv 1 \pmod 8$ and has no roots if $D \equiv 5 \pmod 8$. □

By using the splitting behaviour of a rational prime p in quadratic fields as determined in the lemma above, we can completely derive its splitting behaviour in biquadratic fields. In turn, we can conclude precisely when the HNP holds for a specific family of biquadratic fields.

Theorem 5.1.3. *Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ be a biquadratic field such that $a, b \in \mathbb{Z}$ are coprime. Then the HNP fails to hold for $L/\mathbb{Q}$ if and only if*

i) $a \equiv b \equiv 1 \pmod 4$ or at least one of a and b is 1 modulo 8;

ii) for all odd primes $p \mid a$

$$\left(\frac{b}{p}\right) = 1;$$

iii) for all odd primes $p \mid b$

$$\left(\frac{a}{p}\right) = 1.$$

Proof. By an observation of Tate, a biquadratic field fails the HNP if and only if all the decomposition groups are cyclic [9, Sec. 11.4, p. 199]. As this requires the cohomology of the idéle class group, we will not proof this observation. The criterion written down is then translating this equivalence to a condition on a and b.

Let p be any rational prime and recall that the decomposition group $D(p)$ of p is independent on the L-prime above p by Lemma 3.2.1. Then $D(p)$ is cyclic if and only if p is split in at least one of the three quadratic subfields of L, which we denote by $K_a = \mathbb{Q}(\sqrt{a})$, $K_b = \mathbb{Q}(\sqrt{b})$ and $K_{ab} = \mathbb{Q}(\sqrt{ab})$

First, suppose that p is odd. If p does not divide a or b, then p is always split in at least one of the three quadratic subfields K_a, K_b and K_{ab} by Lemma 5.1.2. On the other hand, if p divides a then p is ramified in K_a and K_{ab}. Hence $D(p)$ is cyclic if and only if p is split in K_b, which yields *ii*) after applying Lemma 5.1.2. By interchanging the roles of a and b, the third condition follows immediately (note that a prime cannot divide both a and b by coprimality).

The situation is slightly more complex when considering the even prime 2. If $a \equiv b \equiv 1 \pmod 4$ then $ab \equiv 1 \pmod 8$ hence p is split in K_{ab} by Lemma 5.1.2 and $D(p)$ is cyclic. Similarly, if at least one of a and b is 1 modulo 8, then 2 is split in at least one of K_a and K_b and thus $D(p)$ is cyclic. Conversely, suppose that $D(2)$ is cyclic. Then 2 is split in at least one of the quadratic subfields and thus at least one of a, b and ab is 1 modulo 8 by Lemma 5.1.2. This coincides with the condition in *i*) except possibly when $a \equiv b \equiv 3, 7 \pmod 8$. However, we claim that this is in contradiction with *ii*) and *iii*). Indeed, if *ii*) and *iii*) hold while $a \equiv b \equiv 3, 7 \pmod 8$ then by quadratic reciprocity we have

$$1 = \prod_{q|b} \left(\frac{a}{q}\right) = \left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right) = -\prod_{p|a} \left(\frac{b}{p}\right) = -1.$$

□

Remark. Note that not all biquadratic fields are of the form $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ with a and b coprime and squarefree. For example, $\mathbb{Q}(\sqrt{6}, \sqrt{10})$ is not of that form as $\mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{10})$ are linearly disjoint. Nonetheless, one can formulate a similar, albeit messy, condition for the general case $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ by taking care of the primes that divide both a and b separately, but we have opted against treating this for the sake of simplicity.

5.2 Explicit counterexamples in biquadratic fields

The previous theorem gives a necessary and sufficient condition when a biquadratic field $L/\mathbb{Q}$ fails the Hasse norm principle. Following the approach by Tate [9, Ex. 5.3, p. 360] it is possible in such a case to explicitly find an element in L that is a local norm everywhere

but not a global norm. This uses the quadratic Hilbert symbol, which, historically, is the forefather of Hasse's norm residue symbol for quadratic extensions of $\mathbb{Q}$.

Definition 5.2.1. For any rational prime number p we define the *quadratic Hilbert symbol* $(\cdot,\cdot)_p$ to be the function

$$(\cdot,\cdot)_p : \mathbb{Q}_p^* \times \mathbb{Q}_p^* \to \{\pm 1\}$$
$$(a,b) \mapsto \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a nontrivial solution over } \mathbb{Q}_p, \\ -1 & \text{otherwise.} \end{cases}$$

Note that by Lemma 4.4.1 we could have also defined $(a,b)_p = 1$ if and only if b is a norm of an element in $\mathbb{Q}_p(\sqrt{a})$ and -1 otherwise. Using this definition, it is immediate that Hasse's norm residue symbol is a generalization of the quadratic Hilbert symbol.

To define the quadratic Hilbert symbol for all primes of $\mathbb{Q}$, we set

$$(a,b)_\infty = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0, \\ -1 & \text{if } a < 0 \text{ and } b < 0. \end{cases}$$

Lemma 5.2.2. *Let v be a prime of $\mathbb{Q}$ and $a, b \in \mathbb{Q}^*$. Then*

i) $(\cdot,\cdot)_v$ *is bilinear;*

ii) if $v = p$ for some rational prime p with $a = p^\alpha u$ and $b = p^\beta w$ for some $u, w \in \mathbb{Q}^*$ coprime to p, then

$$(a,b)_p = \begin{cases} (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{u}{p}\right)^\beta \left(\frac{w}{p}\right)^\alpha & \text{if } p \neq 2, \\ (-1)^{\frac{(u-1)(w-1)}{4} + \alpha\frac{w^2-1}{8} + \beta\frac{u^2-1}{8}} & \text{if } p = 2. \end{cases}$$

iii) we have $(a,b)_v = 1$ for all but finitely many primes v and moreover

$$\prod_v (a,b)_v = 1,$$

where the product ranges over all the primes of $\mathbb{Q}$.

Proof. We will skip the proof and refer the interested reader to [43, Ch. III]. The proof is not hard but rather a nuisance requiring some arithmetic. □

Remark. The equality in *iii*) is called the *Hilbert product formula* and is, interestingly, equivalent to the quadratic reciprocity law.

Now, let us return to the problem at hand and let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ be a biquadratic field failing the HNP in the sense of Theorem 5.1.3. Write K_a, K_b and K_{ab} as the three unique quadratic subfields $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$, respectively, of L. Moreover, let S_a, S_b

and S_{ab} be the set of $\mathbb{Q}$-primes that are completely split in K_a, K_b and K_{ab}, respectively. Here, we include the prime at infinity in all three subsets. For any $x \in \mathbb{Q}^*$, set

$$\phi(x) = \prod_{v \in S_a} (b, x)_v,$$

which is well-defined by Lemma 5.2.2

Lemma 5.2.3. *Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ be a biquadratic field with $a, b \in \mathbb{Z}$ coprime and squarefree such that $L/\mathbb{Q}$ fails the HNP as described in Theorem 5.1.3. Let $x \in \mathbb{Q}^*$. Then*

$$\phi(x) = -1 \iff x^2 \text{ is a local norm everywhere but not a global norm.}$$

Proof. The proof is quite long but it boils down to showing the following:

1) We have a string of equalities

$$\phi(x) = \prod_{v \in S_a} (b, x)_v = \prod_{v \in S_a} (ab, x)_v = \prod_{v \in S_b} (a, x)_v = \prod_{v \in S_b} (ab, x)_v = \prod_{v \in S_{ab}} (a, x)_v = \prod_{v \in S_{ab}} (b, x)_v.$$

2) Let $N_a = N_{K_a/\mathbb{Q}}(K_a^*)$ denote the elements of $\mathbb{Q}$ that are norms of K_a and likewise N_b and N_{ab} for K_b and K_{ab}, respectively. Then

$$N_a N_b N_{ab} = \{x \in \mathbb{Q}^* \mid x^2 \in N_{L/\mathbb{Q}}(L^*)\}.$$

Suppose that the two statements above have been proven. The first statement shows that $N_a N_b N_{ab} \subset \ker \phi$. Indeed, it is sufficient to proof that $\phi(N_a) = 1$. For $y \in N_a$ we have $(a, y)_p = 1$ for all finite primes p of $\mathbb{Q}$ by definition and it possibly only differs from 1 at the prime at infinity. Yet $a < 0$ implies $y > 0$ and thus $(a, y)_\infty = 1$, proving the desired.

Now, let $H \subset \mathbb{Q}^*$ be the subgroup of all elements of $\mathbb{Q}^*$ that are local norms everywhere for $L/\mathbb{Q}$, where we quotient out by the elements of $\mathbb{Q}^*$ that are global norms for $L/\mathbb{Q}$. Consider the map $\Psi : \mathbb{Q}^* \to H$ given by $\Psi(x) = x^2$. By Theorem 5.1.3, all local extensions are at most quadratic hence Ψ is well-defined. The second statement then tells us that Ψ factors through $N_a N_b N_{ab}$. Moreover, a relatively easy application of the cohomology of idéles shows that $\#H = 2$ (we will skip this as it requires too much background material. The proof is relatively simple however, see [9, Sec. 11.4, p. 199].). It therefore follows that either $\ker \phi = N_a N_b N_{ab}$ or $\ker \phi = \mathbb{Q}^*$, yielding the desired.

It therefore remains to show that the two statements above hold. By symmetry, it is sufficient for 1) to show that $\prod_{v \in S_a} (ab, x)_v = \prod_{v \in S_b} (ab, x)_v$. Now, note that $S_a \cup S_b \cup S_{ab}$ contains all the primes of $\mathbb{Q}$ as at least one of a, b and ab is a quadratic residue modulo p

(Lemma 5.1.2). Moreover, we have $(ab, x)_v = 1$ for all $v \in S_{ab}$ and $S_a \cap S_b \subset S_{ab}$. By applying the Hilbert product formula in Lemma 5.2.2 it then follows that

$$1 = \prod_{v \in S_a} (ab, x)_v \prod_{v \in S_b} (ab, x)_v \prod_{v \in S_a \cap S_b} (ab, x)_v^{-1} = \prod_{v \in S_a} (ab, x)_v \prod_{v \in S_b} (ab, x)_v,$$

proving the desired.

The final statement is an application of Hilbert 90 (Theorem 2.3.5). First, note that clearly $N_a N_b N_{ab} \subset \{x \in \mathbb{Q}^* \mid x^2 \in N_{L/\mathbb{Q}}(L^*)\}$, since for any $z \in K_a$ we have $N_{K_a/\mathbb{Q}}(z)^2 = N_{L/\mathbb{Q}}(z)$ (likewise for K_b and K_{ab}). For the converse, let $x \in \mathbb{Q}^*$ be such that $x^2 = N_{L/\mathbb{Q}}(y)$ for some $y \in L^*$. Write σ_a, σ_b and σ_{ab} as the elements of $\mathrm{Gal}(L/\mathbb{Q})$ fixing K_a, K_b and K_{ab}, respectively. The element $N_{L/K_a}(y)/x \in K_a$ has norm 1 hence by Hilbert 90 there exists some $z_a \in K_a$ such that

$$\frac{z_a}{\sigma_{ab}(z_a)} = \frac{N_{L/K_a}(y)}{x}.$$

Repeating this argument for K_b yields another element $z_b \in K_b$ such that

$$\frac{z_b}{\sigma_{ab}(z_b)} = \frac{N_{L/K_b}(y)}{x}.$$

Now let $z_{ab} = z_a \sigma_b(y)/z_b$. This satisfies $\sigma_{ab}(z_{ab}) = z_{ab}$ implying that $z_{ab} \in K_{ab}$ by Galois theory. Moreover

$$z_{ab}\sigma_a(z_{ab}) = \frac{z_a^2 \sigma_b(y) N_{L/K_b}(y) \sigma_{ab}(y)}{z_b^2 x} = \frac{z_a^2 \sigma_b(y)}{z_b^2 \sigma_a(y)} x = \frac{z_a \sigma_{ab}(z_a)}{z_b \sigma_{ab}(z_b)} x$$

Therefore

$$x = N_{K_{ab}/\mathbb{Q}}(z_{ab}) N_{K_b/\mathbb{Q}}(z_b) N_{K_a/\mathbb{Q}}(z_a^{-1}) \in N_a N_b N_{ab}.$$

□

The above lemma shows that if there exists some $x \in \mathbb{Q}^*$ such that $\phi(x) = -1$ then its square x^2 is a local norm everywhere but not a global norm. Using the explicit formula of $(\cdot, \cdot)_p$ as given in Lemma 5.2.2 we can easily create such an x.

Theorem 5.2.4. *Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ be a biquadratic field such that $a, b \in \mathbb{Z}$ are coprime and $L/\mathbb{Q}$ fails the HNP as described in Theorem 5.1.3. Suppose without loss of generality that $a \equiv 1 \pmod 4$. Let x be a squarefree positive integer that is a product of primes q such that*

$$\left(\frac{q}{a}\right) = -1.$$

Then x^2 is a global norm if and only if

$$\left(\frac{b}{x}\right) = 1.$$

Proof. By Lemma 5.2.3 it is sufficient to show that $\phi(x) = \left(\frac{b}{x}\right)$. Now, $(b,x)_v = 1$ for all $\mathbb{Q}$-primes v except possibly when $v \mid 2bx$ by Lemma 5.2.2. Moreover, by quadratic reciprocity we have that $\left(\frac{a}{q}\right) = 1$ for all odd primes $q \mid x$ and thus the only possible factor dividing both b and x is 2. But $2 \mid b$ implies that $a \equiv 1 \pmod 8$, hence $\left(\frac{2}{a}\right) = 1$. Thus b and x are coprime and we find using Lemma 5.2.2

$$\phi(x) = \epsilon \prod_{\substack{v \mid b \\ v \text{ odd}}} (b,x)_v = \epsilon \prod_{v \mid b'} \left(\frac{x}{v}\right) = \epsilon \left(\frac{x}{b'}\right),$$

where $\epsilon = (b,x)_2$ if 2 is split in K_a and 1 otherwise, and b' is the odd part of b. Now, if 2 is not split in K_a, then $a \equiv 5 \pmod 8$ and thus $b \equiv 1 \pmod 4$ by Lemma 5.1.3. Quadratic reciprocity then tells us that $\phi(x) = \left(\frac{b}{x}\right)$.

On the other hand, if 2 is split in K_a, then $a \equiv 5 \pmod 8$ and thus x is odd. It follows that

$$\phi(x) = (-1)^{\frac{(b'-1)(x-1)}{4} + \beta\frac{x^2-1}{8}} \left(\frac{x}{b'}\right) = (-1)^{\frac{(b'-1)(x-1)}{4}} \left(\frac{x}{2}\right)^{\beta} \left(\frac{x}{b'}\right)$$

where $\beta = 0$ if b is odd and 1 otherwise. The coefficient in the front coincides with the coefficient in the law of quadratic reciprocity and the result immediately follows. □

Example 5.2.5.

1) Let $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, the original counterexample of the Hasse norm theorem provided by Tate. Then 13 is a quadratic residue modulo 17 and 17 is a quadratic residue modulo 13 hence $L/\mathbb{Q}$ fails the HNP. From Theorem 5.2.4 it follows that $5^2, 7^2, 10^2, 11^2, 31^2, \ldots$ are all elements that are local norms everywhere but not global norms.
2) Let $L = \mathbb{Q}(\sqrt{141}, \sqrt{385})$. We have $141 = 3 \cdot 47$ and $385 = 5 \cdot 7 \cdot 11$ and it can be readily checked that 141 is a quadratic residue modulo 5, 7 and 11 while 385 is a quadratic residue modulo 3 and 47. Thus $L/\mathbb{Q}$ fails the HNP and a quick search yields that $13^2, 17^2, 31^2, 53^2, 59^2, \ldots$ are all elements that are local norms everywhere but not global norms.
3) Consider $L = \mathbb{Q}(\sqrt{58}, \sqrt{154})$ and note that 154 and 58 are not coprime. However, we have that $58 \cdot 154/4 \equiv 1 \pmod 8$ hence $D(2)$ is cyclic by Lemma 5.1.2. Moreover, 58 is a quadratic residue modulo 7 and 11 while 154 is a quadratic residue modulo 29. As such, all decomposition groups are cyclic and $L/\mathbb{Q}$ fails the HNP by the proof of Theorem 5.1.3. Now, Theorem 5.2.4 need not apply in this case as 54 and 158 are not coprime. Nonetheless, Lemma 5.2.3 still applies as we have only used the fact that all decomposition groups of L are cyclic. It therefore follows that for $x \in \mathbb{Z}_{>0}$,

its square x^2 is not a global norm if and only if

$$(154,x)_7(154,x)_{11}\prod_{\substack{p\mid x,p\neq 2,7,11\\ \left(\frac{58}{p}\right)=1}}(154,x)_p=-1.$$

If we mimic the approach of earlier and let x be a product of primes p such that $\left(\frac{58}{p}\right)\neq 1$, then the product above is empty. Hence the square of such an x is not a global norm but a local norm everywhere if and only if $\left(\frac{x}{77}\right)=-1$. Examples include $2^2,5^2,26^2,29^2,\ldots$ after a quick computation.

Note that the problem of generalising Theorem 5.2.4 in its current form lies in the fact that, in general, a biquadratic extension $\mathbb{Q}(\sqrt{a}/\sqrt{b})/\mathbb{Q}$ for which the HNP does not hold need not satisfy the clean congruence conditions on a and b as established in Theorem 5.1.3. Therefore we can not use quadratic reciprocity to get rid of the coefficients appearing in the formula of $\phi(x)$. Nonetheless, one can still easily calculate $\phi(x)$ using Lemma 5.2.2 on a case-by-case basis as illustrated above and find integers whose squares are not global norms but are local norms everywhere (if, of course, such elements exist).

6 Explicit methods for solving norm equations

We have thus far only treated the Hasse norm theorem with its extensions and biquadratic counterexamples. It states that the equation $N_{L/K}(x) = a$ for a given extension of number fields L/K satisfying Theorem 4.3.5 and $a \in K^*$ is soluble in $x \in L^*$ if and only if it is everywhere locally soluble. However, the proof is nonconstructive as it does not explicitly generate a global solution from the local solutions. Nonetheless, there are still various methods for solving such equations; one due to Simon [44] which finds two computable finitely generated abelian groups for which the discrete logarithm problem is relatively easy.

Furthermore, if a is an integral element of K, then we can naturally restrict the equation above to integral elements $x \in \mathcal{O}_L$. In the final section of this chapter we will discuss two methods for solving this problem algorithmically: one simple method involving the class group and another due to Fincke and Pohst [15], which reduces the equation to an enumeration problem in quadratic forms.

6.1 Representing groups

Since we are going to compute finitely generated abelian groups, let us first briefly describe how this can be done from a computational perspective. We will only write down the basic definitions and theorems without proof. For a complete exposition, see [11, Ch. 4] and [10, Ch. 2].

While we are working with abelian groups, we will write every group multiplicatively since the only groups we consider are subgroups of K^* for a number field K. Following the literature we will therefore write matrix-vector multiplication multiplicatively. That is, given a row vector X consisting of n elements $g_1, \ldots, g_n$ of a group G together with an integer matrix R with n rows, the row vector $Y = XR$ has elements $Y_j = \prod_i g_i^{R_{i,j}}$.

Definition 6.1.1. Let G be a finitely generated abelian group, $X = (g_1, \ldots, g_n)$ a row vector of elements of G and R an $n \times m$ integer matrix. We say that (X, R) is a *system of generators and relations for* G if the g_i's are generators of G and if any relation between the g_i's is a linear combination with integer coefficients of the columns of R.

Example 6.1.2. Let G be the free abelian group generated by a, b and c such that

$$\begin{cases} a^3c^7 &= b^5, \\ ab^2 &= c^{11}, \\ a^3b &= c^5. \end{cases}$$

The tuple $((a, b, c), R)$ where R is given by

$$\begin{pmatrix} 3 & 1 & 3 \\ -5 & 2 & 1 \\ 7 & -11 & -5 \end{pmatrix}$$

is a system of generators and relations for G.

Not all system of generators and relations for a finitely generated abelian group G are equal. By the structure theorem of finitely generated abelian groups we know that there exists $r \in \mathbb{Z}_{\geq 0}$ and $d_1, \ldots, d_m \in \mathbb{Z}_{\geq 1}$ such that $d_{i+1} \mid d_i$ and $G \simeq \mathbb{Z}^r \times \prod_i \mathbb{Z}/d_i\mathbb{Z}$. If we let $e_1, \ldots, e_r$ be the generators of the free part of G and $g_1, \ldots, g_m$ the generators of the torsion part of G, then a canonical choice of a system of generators and relations is $((e_1, \ldots, e_r, g_1, \ldots, g_m), D_G)$ where D_G is the $(r+m) \times (r+m)$ diagonal matrix whose diagonal is $(0, \ldots, 0, d_1, \ldots, d_m)$. Fortunately, every system of relations and generators can be transformed into the form above through the so-called Hermite and Smith normal forms.

Definition 6.1.3. Let $A = (a_{i,j})$ be an $m \times n$ integer matrix. We say that A is in *Hermite normal form* (HNF) if there exists some $r \leq n$ and a strictly increasing map $f : [r+1, n] \to [1, m]$ such that

i) the first r columns of A are zero;
ii) For all $r+1 \leq j \leq n$ we have $a_{f(j),j} \geq 1$, $a_{i,j} = 0$ if $i > f(j)$ and $0 \leq a_{f(i),j} \leq a_{f(i),i}$ if $i < j$.

Note that a square matrix is in HNF if it is upper triangular, the leading coefficient of each row is positive and all other elements in the row are positive and strictly smaller than the leading coefficient.

Definition 6.1.4. Let $A = (a_{i,j})$ be an $m \times m$ integer matrix. We say that A is in *Smith normal form* (SNF) if A is a diagonal matrix such that $a_{i+1,i+1} \mid a_{i,i}$ for all $1 \leq i \leq m$.

The matrix D_G in the canonical choice of a system of generators and relations in the paragraph above is, in particular, in SNF.

Theorem 6.1.5. *Let A be an $m \times n$ matrix.*

i) There exists an unique $m \times n$ integer matrix H in HNF such that $H = AU$ for some $U \in \mathrm{GL}_n(\mathbb{Z})$.

ii) If $m = n$ then there exists an unique $m \times m$ integer matrix S in SNF such that $S = VAU$ for some $V \in \mathrm{GL}_m(\mathbb{Z})$ and $U \in \mathrm{GL}_m(\mathbb{Z})$.

The matrix H' spanned by the nonzero columns of H will be called the HNF of A while S will be called the SNF of A.

Proof. We will omit the proof and refer the reader to [10, Alg. 2.4.4, p. 69] for *i)* and [10, Alg. 2.4.14, p. 78] for *ii)*, which acts as both a proof and an algorithm to compute H and S. □

Remark.

i) The HNF can be seen as an analogue of the reduced echelon form of matrices over fields. Right multiplication by an invertible matrix states that the HNF of A can easily be retrieved by suitable elementary column operations of determinant ± 1. In contrast, the additional left multiplication of an invertible matrix in the SNF allows for both row and column operations and is hence slightly more involved to compute.

ii) Be aware that the definitions of both forms vary from book to book. Some authors define the SNF in reverse while others define the HNF to be lower triangular. In the end, these can all be seen to be equivalent after a suitable change in U and V.

The above allows us to compute a canonical choice of a system of generators and relations for a finitely generated abelian group G. Indeed, given a system of generators (X, R) for G we simply take the SNF R' of R and set $X' = XU^{-1}$, where U is the invertible matrix found in the theorem above. Then (X', R') is a system of generators and relations for G corresponding to the structure retrieved from the structure theorem of finitely generated abelian groups. In practice, one should make sure that R is of full rank, or else R' is not well-defined. This amounts to deleting trivial relations which is often straightforward.

Example 6.1.6. Let G be as in Example 6.1.2 with the computed system of relations and generators $((a, b, c), R)$ for G where R is given by

$$\begin{pmatrix} 3 & 1 & 3 \\ -5 & 2 & 1 \\ 7 & -11 & -5 \end{pmatrix}.$$

Let R_i denote the i-th column of R. Notice that $2(-5) + (-1)(-11) = 1$ and thus the act of (simultaneously) replacing R_2 with $-5R_2 + 11R_3$ and R_3 with $2R_3 - R_2$ kills the -11 and yields us

$$\begin{pmatrix} 3 & 28 & 5 \\ -5 & 1 & 0 \\ 7 & 0 & 1 \end{pmatrix} = R \begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & -1 \\ 0 & 11 & 2 \end{pmatrix}.$$

Similarly we can kill the 7 by subtracting the third column from the first column seven times

$$\begin{pmatrix} -32 & 28 & 5 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = R \begin{pmatrix} 1 & 0 & 0 \\ 7 & -5 & -1 \\ -14 & 11 & 2 \end{pmatrix}.$$

Finally, the -5 can be killed by adding the second column to the first column five times and we arrive at the HNF H of R

$$\begin{pmatrix} 108 & 28 & 5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = R \begin{pmatrix} 1 & 0 & 0 \\ -18 & -5 & 1 \\ 41 & 11 & 2 \end{pmatrix}.$$

Now, we can easily diagonalise H by adding multiples of its third and second row to its first row

$$\begin{pmatrix} 108 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -28 & -5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} H = \begin{pmatrix} 1 & -28 & -5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} R \begin{pmatrix} 1 & 0 & 0 \\ -18 & -5 & 1 \\ 41 & 11 & 2 \end{pmatrix},$$

yielding the SNF of R. Thus G is isomorphic to $\mathbb{Z}/108\mathbb{Z}$ and it is generated by the first component of $(a, b, c)U^{-1}$, i.e. $ab^{-5}c^7$.

6.2 Relative norm equations

An idea of Simon [44] was to reduce a relative norm equation $N_{L/K}(x) = a$ in such manner that both a and x are units of K and L, respectively. Here, we mean by an unit of K an unit of $\mathcal{O}_K$, the group of which we denote by U_K to be inline with the literature. Since U_K and U_L are finitely generated abelian groups by Dirichlet's unit theorem, this yields a linear system of equations in terms of the generators of U_K, which in turn is much easier to control and solve. However, a priori, a need not be an unit and the preimage of an unit need not be an unit itself. The go-to counterexample to the latter is the equation $N_{\mathbb{Q}(\sqrt{34}/\mathbb{Q})}(x) = -1$, which is insoluble in U_L but soluble in L. We must therefore enlarge the units in such a manner that this cannot occur; bringing us to the notion of S-units.

Definition 6.2.1. Let K be a number field and S a finite set of finite K-primes.

i) We say that an element $x \in K^*$ is an *S-integer* if $\operatorname{ord}_{\mathfrak{p}} x \geq 0$ for all $\mathfrak{p} \notin S$. The ring of S-integers will be denoted by $\mathcal{O}_{K,S}$.

ii) We say that an element $x \in K^*$ is an *S-unit* if $\operatorname{ord}_{\mathfrak{p}} x = 0$ for all $\mathfrak{p} \notin S$. The group of S-units will be denoted by $U_{K,S}$.

We clearly have $\mathcal{O}_K \subset \mathcal{O}_{K,S} \subset K$ and, similarly, $U_K \subset U_{K,S} \subset K^*$. Moreover, if L/K is a finite extension of number fields and S a finite set of finite K-primes, then we can extend S naturally to a finite set T of finite L-primes by taking all the L-primes lying above S. We will then write $\mathcal{O}_{L,S}$ and $U_{L,S}$ for $\mathcal{O}_{L,T}$ and $U_{L,T}$, respectively, for ease of notation.

Definition 6.2.2. Let L/K be an extension of number fields and S_0 a finite set of finite K-primes. We say that S_0 is *suitable for* L/K if for all finite sets $S \supset S_0$

$$N_{L/K}(L^*) \cap U_{K,S} = N_{L/K}(U_{L,S}).$$

That is, every S-unit of K that is the norm of an element in L is actually the norm of an S-unit of L.

We can use the notion of suitability to solve $N_{L/K}(x) = a$ in $x \in L^*$ for fixed $a \in K^*$. We first pick a suitable subset S_0 for L/K and let S_a be the set of finite K-primes dividing $a\mathcal{O}_K$. Then a is by definition an S-unit of K for the set $S = S_0 \cup S_a$. Moreover, any preimage of a under $N_{L/K}$ is necessarily an S-unit of L by the suitability of S_0. Thus, in particular, we have that $N_{L/K}(x) = a$ is soluble in $x \in L^*$ if and only if it is soluble in $x \in U_{L,S}$. The S-unit groups $U_{L,S}$ and $U_{K,S}$ are much easier to deal with as they are finitely generated abelian groups. Indeed, if $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, then each $u \in U_{K,S}$ has an ideal factorisation $u\mathcal{O}_K = \prod_i \mathfrak{p}_i^{a_i}$ for $a_i \in \mathbb{Z}$. Such a factorisation is unique up to multiplication by an unit in K, i.e. up to U_K. Hence $U_{K,S}/U_K$ is in particular free of rank s and whence $U_{K,S}$ is finitely generated by Dirichlet's unit theorem. A similar statement holds for $U_{L,S}$. We will show that computing the generators of these groups is relatively easy and thus we can calculate the action of $N_{L/K}$ on the generators of $U_{L,S}$, resulting in a system of linear equations to solve.

What follows is a relatively easy algorithm, due to Cohen [11, Ch. 7.4], to compute the S-unit group of a number field. It relies on a few key algorithms in computational algebraic number theory such as the computation of the class group. Since we do not wish to reinvent the wheel, we treat these algorithms as black boxes and assume that various invariants of a number field can, and are, computed. More specifically, we assume that the following items can be computed for a number field K:

1) The ring of integers of K [10, Alg. 6.1.8, p. 311] together with an algorithm for factoring ideals into prime ideals [10, Alg. 4.8.17, p. 203].
2) The class group of K together with an algorithm, called the principal ideal algorithm, which factors a given fractional ideal in terms of the generators of the class group and a principal fractional ideal [12].
3) The unit group U_K of K [12] together with a discrete logarithm algorithm [11, Alg. 5.3.10, p. 254]. That is, given an unit ϵ, it finds integers $x_i \in \mathbb{Z}$ such that $\epsilon = \prod_i \epsilon_i^{x_i}$ where the ϵ_i's are generators of U_K.

Algorithm 6.2.3 (S-unit group)**.** Let K be a number field, $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ a subset of finite K-primes and $\mathrm{Cl}_K = (B, D_B)$ the class group of K in SNF, where $B = (\mathfrak{b}_1, \ldots, \mathfrak{b}_m)$ are K-ideals and $D_B = \mathrm{diag}(b_1, \ldots, b_m)$ their corresponding orders in Cl_K. This algorithm computes algebraic integers γ_i for $1 \leq i \leq s$ such that

$$U_{K,S} = U_K \times \prod_{i=1}^{s} \langle \gamma_i \rangle.$$

1) For each $j \in \{1, \dots, s\}$ use the principal ideal algorithm to compute $p_{i,j} \in \mathbb{Z}$ such that
$$\overline{\mathfrak{p}_j} = \prod_{i=1}^{m} \mathfrak{b}_i^{p_{i,j}} \quad \text{in } \mathrm{Cl}_K$$
and let $P = (p_{i,j})$.
2) Compute the HNF of $(P \mid D_B)$ and let U denote a corresponding transformation matrix. Here, $(P \mid D_B)$ denotes the horizontal concatenation of P with D_B.
3) Let U_1 be the first s rows and columns of U. Compute the HNF H of U_1 and set $(\mathfrak{a}_1, \dots, \mathfrak{a}_s) = (\mathfrak{p}_1, \dots, \mathfrak{p}_s)H$
4) Use the principal ideal algorithm to compute a generator γ_j of $\mathfrak{a}_j$ for each j and output the γ_j's

Remark. Observe that if $\mathfrak{p}$ is principle, then a generator of $U_{K,\{\mathfrak{p}\}}/U_K$ is simply a generator of $\mathfrak{p}$.

Theorem 6.2.4. *Let K be a number field and $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ a finite set of finite K-primes. Then Algorithm 6.2.3 correctly calculates the S-unit group $U_{K,S}$ of K.*

Proof. Consider both B and S as row vectors. Then $\alpha \in U_{K,S}$ if and only if there exists some column vector $X \in \mathbb{Z}^s$ such that $\alpha \mathcal{O}_K = SX$. Taking the ideal class it thus follows $SX = 1$ in Cl_K. Equivalently, $BPX = 1$ by the definition of P. In particular, PX is a relation for Cl_K in terms of the generators in B and there exists some column vector $Y \in \mathbb{Z}^m$ such that $PX = D_B Y$ or, equivalently, $\left(\frac{X}{-Y}\right) \in \ker(P \mid D_B)$, where $\left(\frac{X}{-Y}\right)$ denotes the vertical concatenation of X over $-Y$. Now, note that $(P \mid D_B)U = (0|W)$ where W is some $m \times m$ square matrix in HNF. It thus follows that the first s columns of U generate the kernel of $(P \mid D_B)$. In particular, there exists some column vector $Z \in \mathbb{Z}^s$ such that $X = U_1 Z$.

Putting this all together, we find that $\alpha \in U_{K,S}$ if and only if there exists some column vector $Z \in \mathbb{Z}^s$ such that $\alpha \mathcal{O}_K = SU_1 Z$. Observe that we can safely replace U_1 with its HNF H as they only differ by an unimodular matrix which corresponds in a change in Z. Thus, if $(\mathfrak{a}_1, \dots, \mathfrak{a}_s) = SH$, then the above states that $\mathfrak{a}_i$'s generate $U_{K,S}/U_K$ under the condition that all of them are principal, which is not immediately clear. Moreover, even if they are all principal, we must check whether there are no trivial relations between the $\mathfrak{a}_i$'s to ensure the rank of $U_{K,S}/U_K$ is indeed s.

To show that the $\mathfrak{a}_i$'s are principal, note that
$$B(P \mid D_B) = (BP \mid BD_B) = (\alpha_1 \mathfrak{p}_1, \dots, \alpha_s \mathfrak{p}_s, \beta_1, \dots, \beta_m)$$
for some $\alpha_j, \beta_i \in K^*$. If $\left(\frac{U_1}{U_2}\right)$ denotes the first s columns of U, then after right multiplying by these columns we get
$$(\mathcal{O}_K, \dots, \mathcal{O}_K) = (\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_m) \left(\frac{U_1}{U_2}\right) \cdot SU_1$$

and thus the ideals in SU_1 are in particular principal and so are the $\mathfrak{a}_i$'s. Finally, we claim that there are no nontrivial relations between the generators γ_j. Suppose to the contrary that $\prod_{j=1}^{s} \gamma_j^{z_j}$ lies in U_K for some integers $z_j \in \mathbb{Z}$. If $Z = (z_j) \in \mathbb{Z}^s$ denotes the column vector of the z_j's, then $SHZ = \mathcal{O}_K$ and thus $\prod_j \mathfrak{p}_j^{x_j} = \mathcal{O}_K$ for some $x_j \in \mathbb{Z}$. But S consists of distinct prime ideals hence $x_j = 0$. Moreover, it is easy to see that U_1 has nonzero determinant and hence so does H. It therefore follows that $Z = 0$ and thus $\gamma_1, \ldots, \gamma_s$ generate $U_{K,S}/U_K$. □

Example 6.2.5. Consider the quadratic field $L = \mathbb{Q}(\alpha)$ with $\alpha^2 = 10455$. Since $10455 \equiv 3 \pmod 4$ we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ by Lemma 5.1.2. Moreover, we can use SageMath [48], or any modern computer algebra package, to calculate the class group of K

$$\mathrm{Cl}_K \simeq (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^2$$

generated by $\mathfrak{b}_1 = (7, \alpha + 5), \mathfrak{b}_2 = (6, \alpha + 3)$ and $\mathfrak{b}_3 = (15, \alpha)$. Let $\mathfrak{p}_1 = (23, \alpha + 6)$ and $\mathfrak{p}_2 = (31, \alpha + 15)$ be two primes above 23 and 31, respectively, and consider $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. Following Algorithm 6.2.3, we calculate with the method `ideal_class_log()` of SageMath the discrete logarithms of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in Cl_K

$$\overline{\mathfrak{p}_1} = \mathfrak{b}_1^2\mathfrak{b}_2\mathfrak{b}_3 \quad \text{and} \quad \overline{\mathfrak{p}_2} = \mathfrak{b}_1\mathfrak{b}_3.$$

Our next step is to compute the HNF of the matrix

$$\begin{pmatrix} 2 & 1 & 6 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 \\ 1 & 1 & 0 & 0 & 2 \end{pmatrix}$$

together with a transformation matrix U. We find

$$\begin{pmatrix} 2 & 1 & 6 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 \\ 1 & 1 & 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 & 1 & 0 \\ -4 & 6 & 2 & -1 & 1 \\ 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 1 & -3 & -1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $s = 2$, $U_1 = \begin{pmatrix} 2 & 0 \\ -4 & 6 \end{pmatrix}$ with its HNF being equal to $H = \begin{pmatrix} 6 & 2 \\ 0 & 2 \end{pmatrix}$. We therefore conclude that $U_{K,S}/U_K$ is generated by the generators of the principal ideals

$$\mathfrak{p}_1^6 \quad \text{and} \quad \mathfrak{p}_1^2\mathfrak{p}_2^2,$$

which turns out to be $875\alpha + 90292$ and $91\alpha + 9332$, respectively. As an aside, the fundamental unit of a real quadratic field $\mathbb{Q}(\sqrt{D})$ can be easily computed by looking at the convergents of $\sqrt{D}$ [2, Thm. 3.3.4, p.38]. Thus

$$U_{K,S} \simeq \langle -1 \rangle \times \langle 4\alpha + 409 \rangle \times \langle 875\alpha + 90292 \rangle \times \langle 91\alpha + 9332 \rangle.$$

Remark. Note that SageMath has a built-in method `S_unit_group()` to calculate the S-unit group of a number field. Behind the scenes it uses the same algorithm.

It is important to store the matrix H for future use as it allows us to easily calculate a discrete logarithm in $U_{K,S}$. Indeed, any $u \in U_{K,S}$ factors as $u\mathcal{O}_K = \prod_j \mathfrak{p}_j^{f_j}$ for some integers $f_i \in \mathbb{Z}$. If we let $F = (f_j) \in \mathbb{Z}^s$ be the column vector of the f_j's then the column vector $Z = H^{-1}F$ has integer coefficients such that $u = u' \prod_j \gamma_j^{z_j}$ by the definition of the γ_j's for some $u' \in U_K$. We can then calculate u' and perform a discrete logarithm in U_K to yield us a factorisation of u in terms of the generators of $U_{K,S}$.

This important observation together with the remarks earlier brings us to the following algorithm that determines whether a given norm equation has a solution and if so, produces a solution. Its validity is clear from our previous discussion.

Algorithm 6.2.6 (Solving norm equations)**.** Let L/K be a finite extension of number fields and $\alpha \in K^*$. This algorithm determines whether there exists an $x \in L^*$ such that $N_{L/K}(x) = \alpha$ and if so, produces such an x.

1) Find a suitable subset S for L/K.
2) Factor $\alpha\mathcal{O}_K$ into K-primes and set $S = S \cup \{\mathfrak{p}\}$ for each K-prime $\mathfrak{p}$ occurring in this factorisation.
3) Using Algorithm 6.2.3, compute S-units $\epsilon_0, \ldots, \epsilon_n$ of K and S-units $\eta_0, \ldots, \eta_m$ of L such that
$$U_{K,S} = \prod_{i=0}^{n} \langle \epsilon_i \rangle \quad \text{and} \quad U_{L,S} = \prod_{j=0}^{m} \langle \eta_j \rangle,$$
where ϵ_0 and η_0 generate the torsion group of $U_{K,S}$ and $U_{L,S}$, respectively.
4) Using the discrete logarithm algorithm in $U_{K,S}$ discussed above, compute exponents a_i and $b_{i,j}$ such that
$$\alpha = \prod_{i=0}^{n} \epsilon_i^{a_i} \quad \text{and} \quad N_{L/K}(\eta_j) = \prod_{i=0}^{n} \epsilon_i^{b_{i,j}} \quad \text{for } j = 0, \ldots, m.$$
5) Solve the linear system
$$\sum_{j=0}^{m} b_{0,j} x_j \equiv a_0 \pmod{\omega_K} \quad \text{and} \quad \sum_{j=1}^{m} b_{i,j} x_j = a_i \quad \text{for } i = 1, \ldots, n$$
in $x_0, \ldots, x_n \in \mathbb{Z}$, where ω_K is the order of the torsion group of U_K.
6) If the linear system has no solution in $\mathbb{Z}$, then the norm equation has no solution. Else return $x = \prod_{j=0}^{m} \eta_j^{x_j}$.

Remark.

i) The exponents a_0 and $b_{0,j}$ are only defined modulo ω_K which is why we have one congruence relation in the linear system. Moreover, since the norm of a torsion unit is again torsion, we have $b_{i,0} = 0$ for all $i = 1, \ldots, n$.

ii) Note that the modular linear equation $\sum_{j=0}^{m} b_{0,j}x_j \equiv a_0 \pmod{\omega_K}$ in $(m+1)$-variables is equivalent to the linear equation $x_{m+1}\omega_K + \sum_{j=0}^{m} b_{0,j}x_j = a_0$ in $(m+2)$-variables. As such all solutions, modulo units of L of relative norm 1, can be determined by computing the preimage of $(a_0, \ldots, a_n)$ under the matrix

$$\begin{pmatrix} b_{0,0} & \ldots & b_{0,n} \\ \vdots & \ddots & \vdots \\ b_{m,0} & \ldots & b_{m,n} \\ \omega_K & \ldots & 0 \end{pmatrix}.$$

This can be done by computing the integer kernel, see [11, Alg. 4.1.23, p. 185].

To apply Algorithm 6.2.3 in practice however, we must first find a suitable subset S for any extension L/K. In the Galois case there is a rather natural construction of such a subset. The injection $\iota : K \to L$ induces a natural homomorphism $\iota : \mathrm{Cl}_K \to \mathrm{Cl}_L$. Its cokernel is called the *relative pseudo-class group*, denoted by $\mathrm{Cl}_i(L/K)$.

Lemma 6.2.7. *Let L/K be a finite extension of number fields.*

i) If L/K is Galois, then a generating set S_0 of K-primes for $\mathrm{Cl}_i(L/K)$ is a suitable subset for L/K.

ii) If L/K is non-Galois and N/K denotes the Galois closure of L/K, then a generating set S_0 of K-primes for $\mathrm{Cl}_i(N/K)$ containing all the ramified primes in L/K is a suitable subset for L/K.

Proof. Let $S \supset S_0$ be any finite set of finite K-primes. We always have $N_{L/K}(U_{L,S}) \subset U_{K,S}$ and it thus remains to proof the converse. We will only proof i) as ii) is rather cumbersome; a full proof can be found in [44, Prop. 5.6].

Suppose $\alpha \in N_{L/K}(L^*) \cup U_{K,S}$. Then there exists $x, y \in \mathcal{O}_{L,S}$ such that $\alpha = N_{L/K}(x/y)$, or equivalently, $N_{L/K}(y)\alpha = N_{L/K}(x)$. Now, write the prime decomposition of $y\mathcal{O}_L$ as $\prod_i \mathfrak{q}_i$ for $\mathfrak{q}_i \in S$, with possible repetition. For any fixed i we have that $\mathfrak{q}_i \mid N_{L/K}(x\mathcal{O}_L)$ since α is an S-unit. Furthermore, note that $N_{L/K}(x\mathcal{O}_L) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x\mathcal{O}_L)$ and thus there exists some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}_i) \mid x\mathcal{O}_L$ by primality of $\mathfrak{q}_i$. In fact, by induction we have that for all i there exists some $\sigma_i \in \mathrm{Gal}(L/K)$ such that $\prod_i \sigma_i(\mathfrak{q}_i) \mid x\mathcal{O}_L$.

By assumption S_0 generates the relative pseudo-class group $\mathrm{Cl}_i(L/K)$ and thus so does S. Therefore for all i there exists an element $\beta_i \in L^*$, an K-ideal $\mathfrak{a}_i$ and an L-ideal $\mathfrak{b}_i$ consisting solely of L-primes above S such that

$$\mathfrak{q}_i = \beta_i \mathfrak{a}_i \mathfrak{b}_i.$$

Now, define $u \in L^*$ by

$$u = \frac{x}{y} \frac{\prod_i \beta_i}{\prod_i \sigma_i(\beta_i)}$$

which satisfies $N_{L/K}(u) = \alpha$. We claim that u is an S-unit hence proving the desired. Suppose not and that there exists some finite L-prime $\mathfrak{q}$ not above S such that $\mathrm{ord}_{\mathfrak{q}}\, u \neq 0$. Then for any K-prime $\mathfrak{p}$ below $\mathfrak{q}$ we have $\mathfrak{p} \mid N_{L/K}(\mathfrak{q}) \mid N_{L/K}(u) = \alpha$, a contradiction. □

Remark.

i) In view of Algorithm 6.2.6, it is important to find a suitable subset that is as small as possible to reduce its complexity. Simon [44, Cor. 5.7, Cor. 4.7] proofs the suitability of certain smaller subsets with the help of cohomology.

ii) It is necessary to pass to the Galois closure in the non-Galois case. Take for example $L = \mathbb{Q}(\alpha)$ with $\alpha^4 - 2\alpha^3 - 19\alpha^2 + 18\alpha + 81 = 0$ and $K = \mathbb{Q}$. Then L/K is non-Galois with trivial class group and thus the empty subset is a suitable subset for L/K if $i)$ were to apply to non-Galois extensions. It can then be shown that every unit of L has norm 1 and thus we conclude that $N_{L/K}(x) = -1$ is non-soluble in L.
However, the Galois closure of L has class group isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and is generated by any prime above 23 (or 41, 113, 193, ...). We then see that we have a 23-unit in L of negative norm

$$N_{L/K}\left(\frac{25}{9}\alpha^3 + \frac{31}{9}\alpha^2 - \frac{241}{9}\alpha - 21\right) = -23^4$$

or, similarly, a 41-unit in L of negative norm

$$N_{L/K}\left(\frac{79}{9}\alpha^3 - \frac{311}{9}\alpha^2 - \frac{718}{9}\alpha + 305\right) = -41^4.$$

It follows that $N_{L/K}(x) = -1$ is actually soluble in L; highlighting that a suitable subset for a non-Galois extension L/K depends on the Galois closure of L in K.

iii) On the same note, it is not as easy as simply taking a generating set of the class group of the Galois closure. Take for example $L = \mathbb{Q}(\beta)$ with $\beta^4 - 2\beta^3 - 12\beta^2 + 13\beta + 13 = 0$ and $K = \mathbb{Q}$. Then L/K is non-Galois and has a trivial class group just like its Galois closure. Moreover, all units of L have norm 1. Thus if we were to ignore the ramified primes in L/K then we would conclude that $N_{L/K}(x) = -1$ is insoluble in L. Yet 3 is ramified in L/K and there exists a 3-unit of negative norm in L

$$N_{L/K}\left(\frac{5}{3}\beta^3 - 3\beta^2 - 15\beta + \frac{77}{3}\right) = -3^4$$

and thus $N_{L/K}(x) = -1$ is actually soluble in L. Code for generating this example and the previous one can be found in [32].

Example 6.2.8. Consider the biquadratic field $L = \mathbb{Q}(\sqrt{22}, \sqrt{89})$ and the norm equation $N_{L/\mathbb{Q}}(x) = 19^2$. Before applying the algorithm, let us first identify L with $\mathbb{Q}(\alpha)$, where α is such that $\alpha^4 - 2\alpha^3 - 87\alpha^2 + 88\alpha - 22 = 0$, by sending the generator $\beta = \sqrt{22} + \sqrt{89}$ of L to $-\frac{3}{268}\beta^3 + \frac{599}{268}\beta + \frac{1}{2}$. The reason for this identification is that the ring of integers of L is then monogenic and generated by α, which makes the calculations much neater.

To determine S_{19}, we factor the minimal polynomial f of α modulo 19, yielding us

$$f \pmod{19} \equiv (x^2 + 18x + 12)(x^2 + 18x + 14) \pmod{19}$$

and thus $19\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 = (19, \alpha^2 + 18\alpha + 12)$ and $\mathfrak{p}_2 = (19, \alpha^2 + 18\alpha + 14)$. Moreover, we note that both of these prime ideals are not principal and in fact that the class group of L is of order 2. Hence we can continue the algorithm with $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$.

The computation of $U_{\mathbb{Q},S}$ is easy as it is simply generated by $\epsilon_0 = -1$ and $\epsilon_1 = 19$. We therefore focus our attention on $U_{L,S}$. Since neither $\mathfrak{p}_1$ nor $\mathfrak{p}_2$ is principal, we get the matrix $P = \begin{pmatrix} 1 & 1 \end{pmatrix}$. Thus we calculate a transformation matrix U for the HNF of $\begin{pmatrix} 1 & 1 & 2 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 2 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Hence $U_1 = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix}$, whose HNF is given by $H = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$. We conclude that $U_{L,S}/U_L$ is generated by the generators of $\mathfrak{p}_1^2$ and $\mathfrak{p}_1\mathfrak{p}_2$, which we find are $\eta_4 = 6\alpha^3 - 30\alpha^2 - 702\alpha - 377$ and $\eta_5 = 19$. Furthermore, we use SageMath to calculate the following generators for U_L

$$-1, -2\alpha + 1, 84\alpha^3 - 126\alpha^2 - 7350\alpha + 3893 \quad \text{and} \quad 212\alpha^3 - 318\alpha^2 - 18656\alpha + 9881,$$

which we label as η_0, η_1, η_2 and η_3, respectively.

The norms of η_4 and η_5 are straightforward to calculate as they coincide with the norm of the ideals $\mathfrak{p}_1^2$ and $\mathfrak{p}_1\mathfrak{p}_2$, which are both of norm $19^4 = \epsilon_0^0\epsilon_1^4$. Moreover, the norm of η_0 is simply 1 while the norms of η_1, η_2 and η_3 are ± 1 as they are units. It thus follows that any S-unit $u \in \mathcal{O}_{L,S}$ satisfies $4 \mid \operatorname{ord}_{19} N_{L/\mathbb{Q}}(u)$ and thus we conclude that there exists no element in L of norm 19^2.

As a sidenote, observe that L actually satisfies Theorem 5.1.3 since $89 \equiv 1 \pmod 8$, 22 is a quadratic residue modulo 89 and 89 a quadratic residue modulo 11. Therefore, we could have used Theorem 4.1.2 to conclude that 19^2 is not a global norm as 22 is not a quadratic residue modulo 19 and as 19 is not a quadratic residue modulo 89.

Example 6.2.9. Consider $L = \mathbb{Q}(\zeta_9)$, $K = \mathbb{Q}(\zeta_3)$ and the relative norm equation $N_{L/K}(x) = 2 + \zeta_3$. Clearly L/K is Galois and it is well known that the cyclotomic fields $\mathbb{Q}(\zeta_n)$ have trivial class group for $n \leq 22$. Moreover, the K-ideal $\mathfrak{p} = (\zeta_3 + 2)$ is prime since it is of

norm 3. Thus a suitable subset for L/K is $S = \{\mathfrak{p}\}$. Note though that $\mathfrak{p}$ splits as $\mathfrak{p} = \mathfrak{q}^3$ in L where $\mathfrak{q} = (\zeta_9^4 - 1)$.

Nonetheless, we see that the generators of $U_{K,S}/U_K$ and $U_{L,S}/U_L$ are the generators of the principal ideals $\mathfrak{p}$ and $\mathfrak{q}$, respectively, since the class groups are trivial. Furthermore, K is totally imaginary so its unit group is finite of order 6 generated by $-\zeta_3$. Similarly, the unit group of L is isomorphic to $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}^2$ and is generated by $-\zeta_9$, $\zeta_9 + 1$ and $\zeta_9^5 + \zeta_9$.

Now, observe that

$$N_{L/K}\left(y_0 + y_1\zeta_9 + y_2\zeta_9^2\right) = y_0^3 - y_2^3 + \zeta_3\left(y_1^3 - y_2^3 - 3y_0y_1y_2\right)$$

for all $y_0, y_1, y_2 \in K$. We can thus calculate the norms of the S-units of L

$$\begin{aligned} N_{L/K}(-\zeta_9) &= -\zeta_3 & N_{L/K}(1 + \zeta_9) &= 1 + \zeta_3, \\ N_{L/K}(\zeta_9 + \zeta_9^5) &= -1 & N_{L/K}(-1 + \zeta_9^4) &= -1 + \zeta_3. \end{aligned}$$

Since $-1 + \zeta_3 = \zeta_3(2 + \zeta_3)$ and $(-\zeta_3)^5 = 1 + \zeta_3$, we have reduced the norm equation $N_{L/K}(x) = 2 + \zeta_3$ to the following system of linear equations

$$\begin{cases} x_0 + 5x_1 + 3x_2 + 4x_3 \equiv 0 \pmod 6, \\ x_3 = 1. \end{cases}$$

Thus we immediately see that $(-\zeta_9)^4(\zeta_9^4 + 1) = (-\zeta_3 - 1)\zeta_9^2 - \zeta_3\zeta_9$ is an element of L of relative norm $\zeta_3 + 2$. In fact, it is the only one modulo units of L of relative norm 1. In [32] one can find the code for not only generating this example, but also for solving the more general version $N_{L/K}(x) = a + b\zeta_3$ with $a, b \in \mathbb{Z}$.

6.3 Integral norm equations

If L/K is a finite extension of number fields, then the norm of any integral element $x \in \mathcal{O}_L$ in L is an integral element in K. As such, it is not only natural to ask whether a given (relative) norm equation $N_{L/K}(x) = a$ has a solution in L, but also whether it has a solution in $\mathcal{O}_L$ when $a \in \mathcal{O}_K$. In the following, we highlight two possible approaches: a class group method and the Fincke-Pohst method.

6.3.1 Class group method

First, factor $a\mathcal{O}_K = \prod_i \mathfrak{p}_i^{v_i}$ into its prime factorisation. For any L-prime $\mathfrak{q}_{i,j}$ above $\mathfrak{p}_i$ we have that $N_{L/K}(\mathfrak{q}_{i,j}) = \mathfrak{p}_i^{f(\mathfrak{q}_{i,j}/\mathfrak{p}_i)}$. Letting $f_{i,j} = f(\mathfrak{q}_{i,j}/\mathfrak{p}_i)$, it thus follows that the norm

equation has solutions in integral K-ideals if and only if there exists $x_{i,j} \in \mathbb{Z}_{\geq 0}$ such that

$$\sum_j f_{i,j} x_{i,j} = v_i \tag{6.1}$$

for all i, where the solution is then given by the ideal $\prod_{i,j} \mathfrak{q}_{i,j}^{x_{i,j}}$. However, this does not imply that there are solutions in $\mathcal{O}_L$ as this ideal need not be principal. That said, the condition that this ideal is principal can be put in terms of the class group. Indeed, if the SNF of Cl_L is given by a collection of L-ideals $(\mathfrak{b}_k)_k$ whose corresponding orders are $(b_k)_k$, then there exist $a_{i,j,k}$'s such that

$$\overline{\mathfrak{q}_{i,j}} = \prod_k \mathfrak{b}_k^{a_{i,j,k}}$$

in Cl_L for all i, j. Hence $\prod_{i,j} \mathfrak{q}_{i,j}^{x_{i,j}}$ is principal if and only if for all k

$$\sum_{i,j} a_{i,j,k} x_{i,j} \equiv 0 \pmod{b_k} \tag{6.2}$$

Thus if $(x_{i,j})$ is a simultaneous solution to (6.1) and (6.2), then the ideal $\prod_{i,j} \mathfrak{q}_{i,j}^{x_{i,j}}$ is principal and any generator $y \in \mathcal{O}_L$ of this ideal satisfies $N_{L/K}(y) = \epsilon a$ for some $\epsilon \in U_K$. We can then determine whether there exists an unit $\eta \in U_L$ whose norm is ϵ. If it does exist, then y/ϵ is an integral solution to $N_{L/K}(x) = a$. If it does not exist, then $N_{L/K}(x) = a$ has no integral solutions.

Algorithm 6.3.1 (Solving integral norm equations)**.** Let L/K be a finite extension of number fields, $a \in \mathcal{O}_K$ and $\mathrm{Cl}_L = (B, D_B)$ the class group of L in SNF, where $B = (\mathfrak{b}_1, \ldots, \mathfrak{b}_m)$ are L-ideals and $D_B = \mathrm{diag}(b_1, \ldots, b_m)$ their corresponding orders in Cl_L. This algorithm determines whether there exists an $x \in \mathcal{O}_L$ such that $N_{L/K}(x) = a$ and if so, produces such an x.

1) Factor $a\mathcal{O}_K = \prod_i \mathfrak{p}_i^{v_i}$ into prime ideals.
2) For each i, determine all L-primes $\mathfrak{q}_{i,j}$ above $\mathfrak{p}_i$ and set $f_{i,j} = f(\mathfrak{q}_{i,j}/\mathfrak{p}_i)$.
3) For all i, j, use the principal ideal algorithm to compute $a_{i,j,k} \in \mathbb{Z}$ such that

$$\overline{\mathfrak{q}_{i,j}} = \prod_{k=1}^{m} \mathfrak{b}_i^{a_{i,j,k}} \quad \text{in } \mathrm{Cl}_L.$$

4) Determine a solution $(x_{i,j})$ with $x_{i,j} \in \mathbb{Z}_{\geq 0}$ to the system of linear equations

$$\sum_{i,j} a_{i,j,k} x_{i,j} \equiv 0 \pmod{b_k} \quad \forall k \quad \text{and} \quad \sum_j f_{i,j} x_{i,j} = v_i \quad \forall i.$$

Terminate if no solutions exists.

5) Use the principal ideal algorithm to compute a generator $y \in O_L$ of the ideal $\prod_{i,j} \mathfrak{q}_{i,j}^{x_{i,j}}$ and set $\epsilon = N_{L/K}(y)/a$.
6) Determine whether there exists an unit η of L such that $N_{L/K}(\eta) = \epsilon$. If not, terminate. Else return y/η.

Remark.

1. Note that each $x_{i,j}$ satisfies $0 \leq x_{i,j} \leq v_i/f_{i,j}$ hence there are in particular only finitely many solutions to the system in 4). It is therefore easy to determine all integral solutions to the norm equation, modulo units of norm 1, by simply determining all solutions of the system in 4) and repeating 5) and 6) for each of these solutions.
2. We can use 4) and 5) of Algorithm 6.2.6 with $S = \emptyset$ in 6) to find the desired unit η.

Example 6.3.2. Consider $L = \mathbb{Q}(\alpha)$ with $\alpha^5 - 2\alpha^4 - \alpha^3 + 9\alpha^2 - 11\alpha + 8 = 0$, $K = \mathbb{Q}$ and the integral norm equation $N_{L/K}(x) = 9610000$. We factor $9610000 = 2^4 \cdot 5^4 \cdot 31^2$ in $\mathbb{Z}$, label the factors $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$, respectively, and in turn, factor each of these primes in O_L to yield us

$$\begin{aligned}
\mathfrak{p}_1 O_L &= (2, \alpha^3 + \alpha^2 - 2\alpha + 3)(2, \alpha)(2, \alpha + 1), \\
\mathfrak{p}_2 O_L &= (5, \alpha^3 - \alpha^2 - \alpha + 7)(5, \alpha + 2)^2, \\
\mathfrak{p}_3 O_L &= (31, \alpha^3 + 13\alpha^2 - 10\alpha - 3)(31, \alpha^2 - 15\alpha - 13).
\end{aligned}$$

We label the L-primes $\mathfrak{q}_{i,j}$ from left to right and top to bottom. We then find that the $f_{i,j}$'s are given by

$$\begin{pmatrix} 3 & 1 & 1 \\ 3 & 1 & - \\ 3 & 2 & - \end{pmatrix}.$$

Now, the class group of L is cyclic of order 6 and generated by $\mathfrak{q}_{3,2}$. We thus see that the $a_{i,j,k}$'s are given by $(5, 4, 3, 2, 2, 5, 1)$, ordered as $a_{1,1,1}, a_{1,2,1}, a_{1,3,1}, a_{2,1,1}, \ldots$, and any integral solution is equivalent to a nonnegative solution $(x_{i,j})$ in the system of linear equations

$$\begin{aligned}
3x_{1,1} + x_{1,2} + x_{1,3} &= 4, \\
3x_{2,1} + x_{2,2} &= 4, \\
3x_{3,1} + 2x_{3,2} &= 2,
\end{aligned}$$

subject to the constraint

$$5x_{1,1} + 4x_{1,2} + 3x_{1,3} + 2x_{2,1} + 2x_{2,2} + 5x_{3,1} + x_{3,2} \equiv 0 \pmod 6$$

It is immediate that $x_{3,1} = 1$ and $x_{3,2} = 0$ and either $x_{2,1} = x_{2,2} = 1$ or $x_{2,1} = 0$ and $x_{2,2} = 4$. In the former case we find just a single solution for $(x_{1,1}, x_{1,2}, x_{1,3})$: $(0, 1, 3)$; while in the latter case we find two: $(0, 3, 1)$ and $(1, 1, 0)$. Finally, we calculate a generator of the ideal corresponding to each of these three solutions

$$\begin{cases} -9\alpha^4 + 16\alpha^3 + 22\alpha^2 - 75\alpha + 74, \\ 2\alpha^4 - 6\alpha^3 + 11\alpha^2 - 5\alpha + 16, \\ -5\alpha^4 + \alpha^3 + 18\alpha^2 - 35\alpha + 6. \end{cases}$$

One can check that each of these elements has norm 9610000 and thus they form a complete set of integral elements in L of norm 9610000 modulo units of norm 1.

Example 6.3.3. Consider $L = \mathbb{Q}(\alpha)$ with $\alpha^2 = 506$, $K = \mathbb{Q}$ and the integral norm equation $N_{L/K}(x) = 279 = 3^2 \cdot 31$. By Lemma 5.2.3 we know that 3 is inert in L/K while 31 splits in L/K and factors as

$$31\mathcal{O}_L = (31, \alpha + 14)(31, \alpha + 17).$$

Writing these prime factors as $\mathfrak{q}_1$ and $\mathfrak{q}_2$, respectively, it follows that the only ideals of norm 279 are $3\mathfrak{q}_1$ and $3\mathfrak{q}_2$. However, the class group of L is nontrivial and both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are nonprincipal and thus no integral element of norm 279 exists.

Interestingly, 279 is a norm of an element in $\mathbb{Z}_p[\alpha]$ for all p. Indeed for $p \neq 2, 3, 11, 23, 31$ the sets $\{x^2 - 279 \mid x \in \mathbb{F}_p\}$ and $\{506y^2 \mid y \in \mathbb{F}_p\}$ both contain $\frac{p+1}{2}$ elements and thus have a nontrivial intersection. A point $(x, y) \neq (0, 0)$ in the intersection can then be lifted to $(x, y) \in \mathbb{Z}_p^2$ by use of Hensel's lemma 2.2.8, which satisfies $N_{L_p/K_p}(x + y\alpha) = 279$. For $p = 11, 23$ we note that 279 is a quadratic residue modulo p and thus there exists some $x \in \mathbb{Z}_p$ such that $N_{L_p/K_p}(x) = 279$ by (again) Hensel's lemma. Similarly, 31 is a quadratic residue modulo 3 so $279 = 3^2 \cdot 31$ is a local norm at 3. Moreover, 506 is a quadratic residue modulo 31 so all elements are local norms at 31. Finally, for $p = 2$ we simply calculate that $724073 + \alpha$ has norm 279 in $\mathbb{Q}_p$. This shows that even in the most nontrivial case the Hasse norm theorem need not hold for integral elements. Nonetheless, the Hasse norm theorem still applies and by using Algorithm 6.2.6 we find a nonintegral element of L of norm 279

$$N_{L/K}\left(\frac{249}{31}\alpha - \frac{5625}{31}\right) = 279.$$

6.3.2 Fincke-Pohst

The above method is certainly useful in situations where the class group of L is known. However, class group computations are relatively hard. A method by Fincke and Pohst [15, 16] circumvents these computations by translating the problem into the problem of finding short vectors to positive definite quadratic forms. Simultaneously, they devised a

simple, yet effective, algorithm for enumerating these short vectors, which is now known as the Fincke-Pohst algorithm or Fincke-Pohst enumeration. While their method was later generalised to relative norm equations [14], we will only treat the absolute case.

Let us first discuss the enumeration algorithm. Suppose we have a positive definite quadratic form q in n variables. Then for any $C > 0$ there exists only finitely many integral vectors $x \in \mathbb{Z}^n$ such that

$$q(x) \leq C.$$

To find all these vectors, write $q(x) = \sum_{i=1}^{n} q_{i,i}(x_i + \sum_{j=i+1}^{n} q_{i,j}x_j)^2$ for some $q_{ij} \in \mathbb{R}$. The existence of these $q_{i,j}$'s are guaranteed as q is positive definite. Now, look at the n-th term of the summation. The inequality above states that $q_{n,n}x_n^2 \leq C$ and hence we obtain the bound $\lceil -\sqrt{C/q_{n,n}} \rceil \leq x_n \leq \lfloor \sqrt{C/q_{n,n}} \rfloor$. Any such value of x_n yields another bound on x_{n-1}. Indeed, by looking at the last two terms of the summation, we have

$$q_{n-1,n-1}(x_{n-1} + q_{n-1,n}x_n)^2 + q_{n,n}x_n^2 \leq C$$

and thus

$$\left\lceil -\sqrt{\frac{C - q_{n,n}x_n^2}{q_{n-1,n-1}}} - q_{n-1,n}x_n \right\rceil \leq x_{n-1} \leq \left\lfloor \sqrt{\frac{C - q_{n,n}x_n^2}{q_{n-1,n-1}}} - q_{n-1,n}x_n \right\rfloor.$$

Continuing in this fashion, we obtain a bound on x_i based on the values of $x_{i+1}, \ldots, x_n$. Specifically, if we write $T_i = C - \sum_{j=i+1}^{n} q_{j,j}(x_j + \sum_{k=j+1}^{n} q_{j,k}x_k)^2$ and $S_i = \sum_{j=i+1}^{n} q_{i,j}x_j$, then

$$\left\lceil -\sqrt{\frac{T_i}{q_{i,i}}} - S_i \right\rceil \leq x_i \leq \left\lfloor \sqrt{\frac{T_i}{q_{i,i}}} - S_i \right\rfloor.$$

This allows us to exhaust all possibilities by enumeration, hence obtaining the following algorithm.

Algorithm 6.3.4 (Fincke-Pohst)**.** Let $C \in \mathbb{R}_{>0}$ and let q be a positive definite quadratic form in n variables given by

$$q(x) = \sum_{i=1}^{n} q_{i,i}\left(x_i + \sum_{j=i+1}^{n} q_{i,j}x_j\right)^2.$$

This algorithm returns all $x \in \mathbb{Z}^n$ such that $q(x) \leq C$.

1) Set $i = n$, $T_i = C$ and $U_i = 0$.
2) Set $Z = \sqrt{T_i/q_{i,i}}$, $L_i = \lceil -Z - S_i \rceil$ and $U_i = \lfloor Z - S_i \rfloor$.
3) For all integers x_i in $[L_i, U_i]$:
    - If $i = 1$, output x if x is nonzero and terminate otherwise.

- Else set $T_{i-1} = T_i - q_{i,i}(x_i + S_i)^2$, $i = i - 1$ and $S_i = \sum_{j=i+1}^{n} q_{i,j}x_j$, and go back to 2).

Remark.

i) Note that for any $x \in \mathbb{Z}^n$ satisfying $q(x) \leq C$, we also have $q(-x) \leq C$. For practicality, this algorithm only returns one of x and $-x$.

ii) In practice, one would use the LLL-algorithm to greatly reduce the bounds on the x_i's, see [16, Algorithm 2.12] and/or [10, Algorithm 2.77, p.105].

Now that we can easily enumerate over all short vectors of a positive definite quadratic form, it remains to show that the original problem at hand, i.e. solving integral absolute norm equations, can be translated into an enumeration problem. Before we start, we will need the following technical lemma.

Lemma 6.3.5. *Let $\gamma \in \mathbb{R}_{>0}$ and define two functions $h, g : \mathbb{R}_{>1} \to \mathbb{R}$ by*

$$h(t) = \frac{t}{t-1} + \frac{1}{\log t} \quad \text{and} \quad g(t) = (1 - h(t))t^{h(t)} + h(t)t^{h(t)-1}.$$

Then for any $m, n \in \mathbb{Z}_{\geq 1}$ there exists an unique $\lambda_{m,n} \in \mathbb{R}_{>1}$ such that

$$g(\lambda_{m,n}) = \left(1 + \frac{\gamma}{m}\right)^{\frac{2}{n}}.$$

Proof. Note that $0 < h(t) < 1$ for all t and moreover that the function $f : (0,1) \times \mathbb{R}_{>1} \to \mathbb{R}$ defined by $f(y,z) = (1-y)z^y + yz^{y-1}$ is strictly increasing for fixed $y \in (0,1)$, while for fixed $z \in \mathbb{R}_{>1}$ it has precisely one maximum given by $y = h(z)$. Hence g is strictly increasing and the claim then follows as $\lim_{t \to 1^+} g(t) = 1$. □

Let L be a number field of degree n. Our goal is to solve $N_{L/\mathbb{Q}}(x) = m$ in $x \in \mathcal{O}_L$ for fixed $m \in \mathbb{Z}_{\geq 2}$, or, equivalently after considering units in L of norm -1, $|N_{L/\mathbb{Q}}(x)| = m$ (this algorithm requires the unit group U_L hence taking $m = 1$ is nonsense). The insight of Fincke and Pohst was that any solution of this equation is associate to a solution whose conjugates are bounded (recall that two elements $x, y \in \mathcal{O}_L$ are associate if they differ by an unit of L, i.e. $x = \epsilon y$ for some $\epsilon \in U_L$). In what follows, we have ordered the field embeddings $\sigma_1, \ldots, \sigma_n$ of L into $\mathbb{C}$ in such a manner that $\sigma_1, \ldots, \sigma_s$ are real while σ_{s+j} and σ_{s+j+t} are conjugate for $1 \leq j \leq t$.

Theorem 6.3.6. *Let L be a number field of degree n, $m \in \mathbb{Z}_{\geq 1}$, $\gamma \in \mathbb{R}_{>0}$ and $\lambda = \lambda_{m,n}$ as in Lemma 6.3.5, and $\epsilon_1, \ldots, \epsilon_{s+t-1}$ the fundamental units of L. Then any $y \in \mathcal{O}_L$ satisfying $|N_{L/\mathbb{Q}}(x)| = m$ is associate to $x \in \mathcal{O}_L$ such that*

$$\frac{\sqrt[n]{m}}{R_i} \leq |\sigma_i(x)| \leq \sqrt[n]{m} R_i \quad \forall i = 1, \ldots, n,$$

where $R_i = \exp(\frac{1}{2}\sum_{j=1}^{s+t-1} |\log(|\sigma_i(\epsilon_j)|)|)$. *Moreover,* x *satisfies*

$$\sum_{i=1}^{n} \lambda^{r_i} |\sigma_i(x)|^2 \leq n(m+\gamma)^{\frac{2}{n}}, \tag{6.3}$$

where $(r_1, \ldots, r_n) \in \mathbb{Z}^n$ *satisfies*

i) $\sum_{i=1}^{n} r_i = 0$*;*

ii) $\left\lfloor \frac{-2\log R_i}{\log \lambda} \right\rfloor \leq r_i \leq \left\lceil \frac{2\log R_i}{\log \lambda} \right\rceil$ *for all* $i = 1, \ldots, n$*;*

iii) for all $j = 1, \ldots, t$ *we have* $r_{s+j} = r_{s+t+j}$*, with at most one exception, say* j'*, which satisfies* $r_{s+j'} = r_{s+j'+t} - 1$.

Sketch. The proof is quite cumbersome so let us only provide a brief sketch. The existence of x we will skip entirely; it is a consequence of Dirichlet's unit theorem [40, Thm 4.2, p. 409]. The second part of the theorem, i.e. the conditions on the tuple $(r_1, \ldots, r_n)$, can be found in full detail in [40, Thm 3.8, p. 338].

Define $z_i = m^{-n/2}|\sigma_i(x)|^2$ for $i = 1, \ldots, n$. By definition this satisfies

$$\prod_{i=1}^{n} z_i = m^{-2} N_{L/\mathbb{Q}}(x)^2 = 1$$

and thus there exist $r_i \in \mathbb{Z}$ and $\eta_i \in \mathbb{R}$ such that $z_i = \lambda^{-r_i+\eta_i}$ and

$$\begin{aligned} 0 &= \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} \eta_i, \\ r_{s+j} &= r_{s+t+j}, \quad \eta_{s+j} = \eta_{s+t+j} \quad \forall j = 1, \ldots, t. \end{aligned}$$

While a priori we may not have that $|\eta_n| < 1$, we can alter the η_i's and r_i's in such a manner that $|\eta_i| < 1$ for all i. More specifically, such that $\eta_i \in [\zeta - 1, \zeta]$ for all i, where $\zeta = \max_i |\eta_i|$. This alteration will not change the value of the summation, but will possibly alter the equality $r_{s+j} = r_{s+t+j}$ for some $j = 1, \ldots, t$. However, it can be shown that it will only alter the equality for at most one index by 1; which in turn shows both *i)* and *iii)*. Moreover, we have $R_i^{-2} \leq z_i \leq R_i^2$ by assumption on $\sigma^i(x)$ and thus

$$-2\log R_i \leq \log z_i = (-r_i + \eta_i)\log \lambda \leq 2\log R_i,$$

yielding the desired bound on r_i since $|\eta_i| < 1$. Furthermore, by convexity of λ^t for

$t \in [\zeta - 1, \zeta]$ we have

$$\begin{aligned}
\sum_{i=1}^{n} \lambda^{r_i} |\sigma_i(x)|^2 &= m^{\frac{n}{2}} \sum_{i=1}^{n} \lambda^{\eta_i}, \\
&\leq m^{\frac{n}{2}} \sum_{i=1}^{n} \left((1 - (\zeta - \eta_i))\lambda^{\zeta} + (\zeta - \eta_i)\lambda^{\zeta - 1} \right), \\
&= m^{\frac{n}{2}} \sum_{i=1}^{n} \left((1 - \zeta)\lambda^{\zeta} + \zeta \lambda^{\zeta - 1} \right), \\
&= m^{\frac{n}{2}} n f(\zeta, \lambda), \\
&\leq m^{\frac{n}{2}} n g(\lambda), \\
&= n(m + \gamma)^{\frac{n}{2}},
\end{aligned}$$

where g and f are defined as in Lemma 6.3.5. □

Finally, observe that (6.3) defines a positive definite quadratic form. Indeed, fix any integral basis $\alpha_1, \ldots, \alpha_n$ of L and define a matrix $B(r_1, \ldots, r_n) = (b_{i,j}) \in \mathbb{R}^{n \times n}$ by

$$b_{i,j} = \begin{cases} \lambda^{r_i/2} \sigma_i(\alpha_j) & 1 \leq i \leq s, \\ \sqrt{\lambda^{r_i} + \lambda^{r_{i+t}}} \mathrm{Re}(\sigma_i(\alpha_j)) & s + 1 \leq i \leq s + t, \\ \sqrt{\lambda^{r_i} + \lambda^{r_{i-t}}} \mathrm{Im}(\sigma_{i-t}(\alpha_j)) & s + t + 1 \leq i \leq n. \end{cases}$$

Then it is easy to see that for $x = \sum_{i=1}^{n} x_i \alpha_i$ with $x_i \in \mathbb{Z}$ we have

$$\begin{pmatrix} x_1 & \ldots & x_n \end{pmatrix} B(r_1, \ldots, r_n)^T B(r_1, \ldots, r_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} \lambda^{r_i} |\sigma_i(x)|^2.$$

We can then apply the Fincke-Pohst algorithm (Algorithm 6.3.7) to the quadratic form q associated to the matrix $B(r_1, \ldots, r_n)^T B(r_1, \ldots, r_n)$ to find all vectors $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ satisfying $q(x_1, \ldots, x_n) \leq n(m + \gamma)^{2/n}$. For each such a vector, we compute the absolute value of the norm of $\sum_{i=1}^{n} x_i \alpha_i$ and check if it is equal to m. Repeating this process for all tuples $(r_1, \ldots, r_n)$ yields the following algorithm.

Algorithm 6.3.7 (Solving integral norm equations using Fincke-Pohst)**.** Let L be a number field of degree n, $m \in \mathbb{Z}_{\geq 2}$, $\gamma \in \mathbb{R}_{>0}$ and $\epsilon_1, \ldots, \epsilon_{s+t-1}$ the fundamental units of L. This algorithm computes all nonassociate solutions $x \in \mathcal{O}_L$ to $|N_{L/\mathbb{Q}}(x)| = m$.

1) Using any root-finding algorithms, e.g. Newton's method, compute $\lambda = \lambda_{m,n}$ as given in Lemma 6.3.5.

2) Determine all tuples $(r_1, \ldots, r_n) \in \mathbb{Z}^n$ subject to *i*)-*iii*) of Theorem 6.3.6.
3) Set $R = \{\}$. For each tuple $(r_1, \ldots, r_n)$ found in 2) do:
   - Compute the matrix $B(r_1, \ldots, r_n)$.
   - Apply the Fincke-Pohst algorithm (Algorithm 6.3.7) to the quadratic form associated to the matrix $B(r_1, \ldots, r_n)^T B(r_1, \ldots, r_n)$ with $C = n(m + \gamma)^{2/n}$.
   - For each vector $(x_1, \ldots, x_n)$ found above, set $x = \sum_{i=1}^{n} x_i \alpha_i$ and compute the absolute value of the norm of x. If it is m, set $R = R \cup \{x\}$
4) Use the discrete log algorithm in U_L to determine if any two elements of R are associate and if so, remove one of them from R.
5) Return R.

Remark.

i) The results of Theorem 6.3.6 hold for any order of rank n and thus the algorithm can in theory be applied to solve $|N_{L/\mathbb{Q}}(x)| = m$ where x is restricted to some order of rank n [15, Lem. 1]. According to Fieker et all [14], a similar result for orders of smaller rank is unknown.

ii) Moreover, the results of Theorem 6.3.6 also hold on the weaker condition that $\epsilon_1, \ldots, \epsilon_{s+t-1}$ are independent units of L [15, Lem. 1]. The algorithm can therefore be applied by just calculating a full set of independent units of L, which is a considerably easier problem [8]. Be warned, however, that under this weaker assumption it is impossible to perform 4). Hence the user should then be content with a complete set of elements of given absolute norm where some elements may or may not be associate. Furthermore, the bounds R_i are then larger and thus there will be more tuples $(r_1, \ldots, r_n)$, increasing the computational complexity.

iii) The algorithm depends on a parameter γ which a priori can be chosen freely. On one hand we want γ to be as small as possible since that would reduce the bound on the quadratic form (6.3). On the other hand, a small choice of γ implies a small λ; which in turn yields a larger bound on the tuples $(r_1, \ldots, r_n)$. To balance this dichotomy, Fincke and Pohst [40, p. 342] propose the following: define y_* by

$$y_* = \min_{x>1} \left\{ \log(x)^{1-s-t} g(x)^{n/2} \right\}$$

and let λ be the argmin of this minimum. Then they set

$$\gamma = (y_* \log(x)^{s+t-1} - 1)m.$$

It is easy to see that (γ, λ) is valid in the sense of Lemma 6.3.5. They showed experimentally that this choice of γ will generally result in less computational time. As such, we will mirror their choice of γ in the rest of this section.

iv) Unlike the previous algorithm for solving integral norm equations (Algorithm 6.3.1), this algorithm is not natively implemented in SageMath. Since we have used SageMath throughout this thesis, we have implemented the algorithm in SageMath for the

sake of completeness [32]. Note that the algorithm is available in Magma but this lacks transparency as Magma is, unfortunately, proprietary.

Example 6.3.8. Let $L = \mathbb{Q}(\alpha)$ with $\alpha^2 = 130$ and consider the integral norm equation $|N_{L/\mathbb{Q}}(x)| = 30$. The fundamental unit of L is given by $5\alpha + 57$ and thus R_1 and R_2 are both approximately 4.736. We calculate the recommended (γ, λ) above to be approximately $(20.915, 8.315)$ and thus r_1 and r_2 both lie in $[-3, 3]$. It is then easy to see that

$$\{(k, -k) \in \mathbb{Z}^2 \mid -3 \leq k \leq 3\}$$

are the only tuples satisfying the conditions in Theorem 6.3.6. For each of these tuples (r_1, r_2) we apply the Fincke-Pohst algorithm to the associated matrix $B(r_1, r_2)$ to find all short vectors smaller than $2 \cdot (20.915 + 30) \approx 102$. For $(r_1, r_2) = (-3, 3)$ we find the element $-7\alpha + 80$, for $(-1, 1)$ the element $\alpha - 10$, for $(1, -1)$ the element $\alpha + 10$ and finally for $(3, -3)$ the element $7\alpha + 80$. From these, $\alpha - 10$ is associate to $7\alpha + 80$ while $\alpha + 10$ is associate to $-7\alpha + 80$ because

$$5\alpha + 57 = \frac{7\alpha + 80}{\alpha - 10} \quad \text{and} \quad \frac{-7\alpha + 80}{\alpha + 10} = (5\alpha + 57)^{-1}.$$

Thus $\{\alpha + 10, \alpha - 10\}$ is a full set of nonassociate integral elements of absolute norm 30.

In the absolute case, we have now got two algorithms to our disposal for solving integral norm equations (in fact, in both relative and absolute case but for the Fincke-Pohst method we have only considered the absolute case). It is then natural to ask whether there are any advantages, or disadvantages, of using one over the other. While Fincke-Pohst avoids the class group computation, it still requires the unit group (or at least a complete set of independent units), whose computation is closely related to the class group computation [10, Alg. 6.5.9, p. 357]. Thus the main computational difference between the two methods is that the class group method requires factoring while the Fincke-Pohst method requires enumeration of vectors. Since factoring small numbers is relatively fast, one would suspect that the class group method is, in general, much faster than the Fincke-Pohst method. For example, applying the Fincke-Pohst method to the equation in Example 6.3.2 requires 43 quadratic forms and to make matters worse, the first quadratic form has around 1.6 million short vectors. Experimental results confirm this suspicion (Figure 6.1).

However, observe that our choice of λ is independent of m and thus enumerating the short vectors of the quadratics forms in (6.3) not only yields all elements of absolute norm m, but all elements of absolute norm smaller than or equal to m. As such, the Fincke-Pohst method looks ideal for solving $|N_{L/\mathbb{Q}}(x)| \leq m$ since no additional work is necessary. On the other hand, there seems to be no simple way to scale the class group method to solve $|N_{L/\mathbb{Q}}(x)| \leq m$, except to apply the method iteratively to all integers smaller than or equal to m. If we compare the performance of the two methods for the same equation, then they

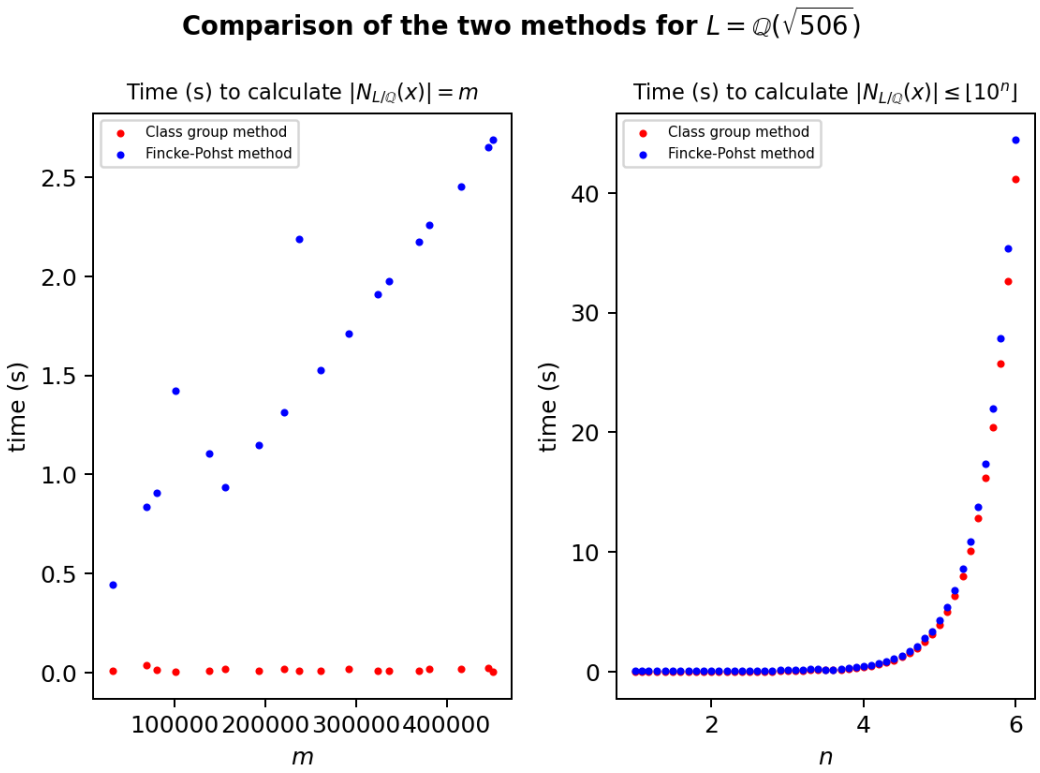


Figure 6.1: A comparison of the Fincke-Pohst method and the class group method for two integral equations over the quadratic field $L = \mathbb{Q}(\sqrt{506})$. The class group method here is the default method `elements_of_norm` in SageMath while the Fincke-Pohst method is a simple implementation in Python [32]. All programs ran on an AMD Ryzen 3 5300U at 3.9GHz.

are much closer in performance than previously (Figure 6.1). While this seems to suggest that the class group method still clears the Fincke-Pohst method, do keep in mind that class group method here is the native function `L.elements_of_norm(m)` of SageMath, which is implemented in C. The Fincke-Pohst method is our quick implementation in Python, which is generally much slower than C.

This result seems to be inline with modern computer algebra packages. While SageMath and PARI do not have built-in functions for solving $|N_{L/\mathbb{Q}}(x)| \leq m$, Magma does and applies the Fincke-Pohst method. On the other hand, SageMath, PARI and Magma all have built-in functions for solving $N_{L/\mathbb{Q}}(x) = m$ and all of them apply the class group method to do so.

7 Discussion

Throughout this thesis, we have treated the Hasse norm theorem and briefly discussed its many extensions discovered over the years. Moreover, we have proved that the theorem does not apply to a family of biquadratic fields and hence showed that the theorem in general need not hold for abelian extensions. Because the proof of the Hasse norm theorem is non-constructive, we have furthermore dedicated the last chapter to a series of algorithms for solving not only norm equations over fields, but also norm equations over rings of integers.

Nonetheless, there is still substantial work that could be done to extend the results of this thesis. As a starter, taking the idéle-theoretic approach to class field theory [22, 38, 9] allows us investigate the extensions of the Hasse norm theorem more thoroughly since virtually all modern literature uses this approach. On the algorithmic side, we note that there are other methods for solving norm equations [20, 1], but these are not used by any modern computer algebra packages. More importantly, we stress that a generalisation of the norm equations we treated can be found in the literature. Specifically, one can ask whether given a finite extension of number fields L/K, an element $\alpha \in K$, an integer $m \leq [L : K]$ and K-independent elements $\beta_1, \ldots, \beta_m \in L$, does there exist an integer solution $x_1, \ldots, x_m \in \mathbb{Z}$ to the equation

$$N_{L/K}(x_1\beta_1 + \ldots x_m\beta_m) = \alpha.$$

Such equations are called norm forms and not much is known about them. They are, however, presumed to be very hard to solve and, interestingly enough, cryptographic schemes have been introduced based on this premise [7]. Schmidt showed that such equations only have finitely many solutions provided the β_i's satisfy a certain condition [42]. Moreover, Győry and Papp [25] provided explicit bounds on the integers x_i under the assumption that $[L : K(\beta_1, \ldots, \beta_{m-1})] \geq 3$. This assumption was made as the equation can then be reduced to a Thue equation and thus results by Baker could be applied [45]. An explicit example applying the method of Győry and Papp was written down by Bennett [6]. Finally, Vojta showed in his PhD thesis [49] that there is an effective solution when $m = 3$, L a totally complex Galois number field and $K = \mathbb{Q}$. This result has recently been generalised to totally complex non-Galois number fields by Bajpai [3].

8 Popular summary

Suppose that we wish to solve the equation

$$x^2 - 506y^2 = 2 \quad \text{for } x, y \in \mathbb{Z}.$$

If we reduce the equation modulo 11, which divides 506, then we see that we have no solution since 2 is not a square modulo 11. It follows that the equation at hand has no solution since any solution will yield a solution modulo 11. This technique of reducing an equation modulo a prime is valuable to have as it sometimes allows us to easily proof that an equation has no solution. Suppose on the other hand that we wish to solve

$$x^2 - 506y^2 = 279 \quad \text{for } x, y \in \mathbb{Z}.$$

We can apply the same reduction technique but no matter how many primes p we try, we always have a solution modulo p. It is therefore tempting to say that the equation does have a solution by somehow combining the solutions modulo all primes. This thought process is known as the local-global principle, where equations may be solved globally, in our case over the integers, by first solving them locally everywhere, in our case modulo primes (actually, prime powers to be precise).

Unfortunately, the local-global principle need not hold for all equations and many mathematicians try to proof that the principle holds for a certain family of equations and if not, try to determine why it fails. The equations above are not chosen randomly and actually arise as norms on number fields. More specifically, the left-hand side of both equations is precisely the norm on the number field $\mathbb{Q}(\sqrt{506}) = \{a + b\sqrt{506} \mid a, b \in \mathbb{Q}\}$. A number field is a subset of the complex numbers which contains $\mathbb{Q}$ and is closed under multiplication, addition, negation and inversion. Number fields are ubiquitous in algebraic number theory and mathematicians have added more structure to them in the form of the Galois group and the ring of integers with its unit group and class group. These structures make it easier to study the norm on number fields and it was Hasse in 1930 who showed that they abide the local-global principle under some strong conditions.

The number field $\mathbb{Q}(\sqrt{506})$ does satisfy these strong conditions, so we must be able to find a solution to the second equation. However, the situation is slightly more complex and the theorem only guarantees a solution in $\mathbb{Q}$ not $\mathbb{Z}$ (Example 6.3.3). We must therefore explain what is exactly meant by looking at $\mathbb{Q}$, or more generally a number field, locally. After treating this, together with some more necessary background material, we will dive

into both a modern proof and the original proof by Hasse. Finally, we note that these proofs of Hasse's theorem are nonconstructive. That is, they do not explicitly give us a method to recover the global solution from the local solutions. We will hence explore several methods for solving these types of equations by using the aforementioned structures on number fields.

References

[1] P. Alvanos and D. Poulakis. Solving Norm Form Equations over Number Fields. In *Conference on Algebraic Informatics*, pages 136–146, Thessaloniki, Greece, 2009. Springer.

[2] T. Andreescu and D. Andrica. *Quadratic Diophantine equations*. Developments in Mathematics. Springer, New York, NY, 2015.

[3] P. Bajpai. Effective methods for norm-form equations. *Mathematische Annalen*, 387:1271–1288, 2023.

[4] H.-J. Bartels. Zur Arithmetik von Diedergruppenerweiterungen. *Mathematische Annalen*, 256(4):465–473, 1981.

[5] H.-J. Bartels. Zur arithmetik von Konjugationsklassen in algebraischen Gruppen. *Journal of Algebra*, 70(1):179–199, 1981.

[6] M. A. Bennett. Solving Norm Form Equations Via Lattice Basis Reduction. *Rocky Mountain Journal of Mathematics*, 26(3):815–837, 1996.

[7] A. Bérczes, J. Ködmön, and A. Pethő. A one-way function based on norm form equations. *Periodica Mathematica Hungarica*, 49(1):1–13, 2004.

[8] J. Buchmann and A. Petho. Computation of independent units in number fields by dirichlet's method. *Mathematics of Computations*, 52(185):149–159, 1989.

[9] J. W. S. Cassels and A. Fröhlich. *Algebraic Number Theory*. Proceedings of an Instructional Conference, Academic Press, 1967.

[10] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, Berlin, Heidelberg, 1993.

[11] H. Cohen. *Advanced Topics in Computional Number Theory*. Graduate Texts in Mathematics. Springer, New York, 2000.

[12] H. Cohen, F. Diaz y Diaz, and M. Olivier. Subexponential Algorithms for Class Group and Unit Computations. *Journal of Symbolic Computation*, 24(3-4):433–441, 1997.

[13] D. Dummit and R. Foote. *Abstract Algebra*. Wiley, 2003.

[14] C. Fieker, A. Jurk, and M. Pohst. On solving relative norm equations in algebraic number fields. *Mathematics of Computations*, 66(217):399–410, 1997.

[15] U. Fincke and M. Pohst. A procedure for determining algebraic integers of given norm. In *Proceedings of the European Computer Algebra Conference*, pages 194–202, 1983.

[16] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–471, 1985.

[17] C. Frei, D. Loughran, and R. Newton. The Hasse norm principle for abelian extensions. *American Journal of Mathematics*, 140(6):1639–1685, 2018.

[18] C. Frei, D. Loughran, and R. Newton. Number fields with prescribed norms (with an appendix by Yonatan Harpaz and Olivier Wittenberg). *Commentarii Mathematici Helvetici*, 97(1):133–181, 2022.

[19] P. Furtwängler. Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern. *Mathematische Annalen*, 74:413–429, 1913.

[20] D. A. Garbanati. An algorithm for finding an algebraic number whose norm is a given rational number. *Journal für die reine und angewandte Mathematik*, 1980(316):1–13, 1980.

[21] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[22] G. Gras. *Class Field Theory*. Springer Monographs in Mathematics. Springer, Berlin, Heidelberg, 2002.

[23] P. Guillot. *A Gentle Course in Local Class Field Theory: Local Number Fields, Brauer Groups, Galois Cohomology*. Cambridge University Press, 2018.

[24] S. Gurak. The Hasse norm principle in non-abelian extensions. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1978(303-304):314–318, 1978.

[25] K. György and Z. Z. Papp. Effective estimates for the integer solutions of norm form and discriminant form equations. *Publicationes Mathematicae Debrecen*, 25:311–325, 1978.

[26] H. Hasse. Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper. *Journal für die reine und angewandte Mathematik*, 1924(153):113–130, 1924.

[27] H. Hasse. Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols. *Journal für die reine und angewandte Mathematik*, 1930(162):134–144, 1930.

[28] H. Hasse. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. Physica-Verlag HD, 1965.

[29] D. Hilbert. Über die Theorie des relativquadratischen Zahlkörpers. *Mathematische Annalen*, 51:1–127, 1899.

[30] D. Hilbert. *Die Theorie der algebraischen Zahlkörper*, pages 63–363. Springer Berlin Heidelberg, Berlin, Heidelberg, 1932.

[31] G. J. Janusz. *Algebraic Number Fields*. Graduate Studies in Mathematics. American Mathematical Society, 2nd edition, 2005.

[32] B. Korbee. Thesis code. `https://github.com/m1tix/ThesisCode`, 2023.

[33] P. Koymans and N. Rome. A note on the Hasse norm principle, 2023, 2301.10136.

[34] A. Macedo. The Hasse norm principle for A_n-extensions. *Journal of Number Theory*, 211:500–512, 2020.

[35] A. Macedo and R. Newton. Explicit methods for the Hasse norm principle and applications to A_n and S_n extensions. *Mathematical Proceedings of the Cambridge Philosophical Society*, 172(3):489–529, 2022.

[36] J. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[37] H. Minkowski. Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Coefficienten in einander rational transformirt werden können. *Journal für die reine und angewandte Mathematik*, 1890(106):5–26, 1890.

[38] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer, 1999.

[39] Y. Oki. The Hasse norm principle for some non-Galois extensions of square-free degree, 2023, 2307.12550.

[40] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge University Press, 1989.

[41] J. J. Rotman. *An Introduction to Homological Algebra*. Universitext. Springer, New York, NY, second edition, 2009.

[42] W. M. Schmidt. Linearformen mit algebraischen Koeffizienten. II. *Mathematische Annalen*, 191(1):1–20, 1971.

[43] J.-P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer, Berlin, Germany, fourth edition, 1996.

[44] D. Simon. Solving norm equations in relative number fields using S-units. *Mathematics of Computations*, 71(239):1287–1305, 2002.

[45] N. P. Smart. *The Algorithmic Resolution of Diophantine Equations*. Number 41 in London Mathematical Society Student Texts. Cambridge University Press, New York, 1998.

[46] P. Stevenhagen. Number Rings, 2019. Available online at: `https://websites.math.leidenuniv.nl/algebra/ant.pdf`, last accessed on 08.02.2023.

[47] P. Stevenhagen. Local Fields, 2021. Available online at: `https://www.math.leidenuniv.nl/~psh/vg.pdf` , last accessed on 08.02.2023.

[48] The Sage Developers. *SageMath, the Sage Mathematics Software System*, 2023. DOI 10.5281/zenodo.6259615.

[49] P. Vojta. *Integral points on varieties*. PhD thesis, Harvard University, 1983.

[50] V. E. Voskresenskii. Maximal tori without effect in semisimple algebraic groups. *Mathematical notes of the Academy of Sciences of the USSR*, 44:651–655, 1988.

[51] C. A. Weibel. History of Homological algebra. Available online at: `https://www.mat.uniroma2.it/~schoof/historyweibel.pdf`, last accessed on 27.08.2023.