MATHEMATICS OF COMPUTATION
Volume 71, Number 239, Pages 1287–1305
S 0025-5718(02)01309-1
Article electronically published on January 11, 2002

SOLVING NORM EQUATIONS IN RELATIVE NUMBER FIELDS USING S-UNITS

DENIS SIMON

ABSTRACT. In this paper, we are interested in solving the so-called norm equation $\mathcal{N}_{L/K}(x) = a$, where L/K is a given arbitrary extension of number fields and a a given algebraic number of K. By considering S-units and relative class groups, we show that if there exists at least one solution (in L, but not necessarily in $\mathbb{Z}_L$), then there exists a solution for which we can describe precisely its prime ideal factorization. In fact, we prove that under some explicit conditions, the S-units that are norms are norms of S-units. This allows us to limit the search for rational solutions to a finite number of tests, and we give the corresponding algorithm. When a is an algebraic integer, we also study the existence of an integral solution, and we can adapt the algorithm to this case.

1. INTRODUCTION

The aim of this paper is to solve explicitly an equation of the type $\mathcal{N}_{L/K}(x) = a$, where L/K is an arbitrary given extension of number fields, and a a given nonzero element of the number field K. We also want to be able to decide if this equation is solvable or not.

By writing a in the form $a = \alpha/b$ with $b \in \mathbb{Z}$ and α integral in K, we see that our equation is equivalent to $\mathcal{N}_{L/K}(x) = b^{d-1}\alpha$, where $d = [L : K]$ is the degree of the extension. Thus without loss of generality we can make the assumption that a is an algebraic integer.

As a first idea we can look for integral solutions when a itself is integral, and this can be done for example by bounding the absolute value of the solutions. This idea, which we will not use, is developped by C. L. Siegel in [12] in the case of Galois extensions, by U. Fincke and M. Pohst in [9] in the case of an absolute extension, or by C. Fieker, A. Jurk and M. Pohst in [8] in the relative case. A more algebraic solution of this problem is given by D. Garbanati in [10] in the case of Abelian extensions, or by C. Fieker for Galois extensions in [7]. Our purpose here is to give an algebraic description of the rational solutions in the general case, and to deduce from this an algorithm. To our knowledge, an algorithm which solves this problem by algebraic considerations in the general case was not known before.

We will first prove some theorems giving a precise description of the prime ideal factorization of the solutions, which give bounds for the primes in the solutions. Secondly, we deduce an algorithm from these theorems that constructs a solution, or proves the nonsolvability of the equation. This algorithm assumes that we have

Received by the editor January 22, 1999 and, in revised form, April 13, 1999.
2000 *Mathematics Subject Classification.* Primary 11D57, 11Y50, 11R29.
Key words and phrases. Relative number fields, norm equation, S-unit, class group.

a good knowledge of the field L. For example we have at our disposal a fundamental system of units of L, and we can solve the "principal ideal problem". We illustrate each proposition by an example. These examples were computed using the algorithms described at the end of this paper, which were implemented on the number theory package PARI/GP.

If we can prove that there is no integral solution, it definitely does not prove that there is no rational solution at all. Let us consider the following example: $L/K = \mathbb{Q}(\sqrt{34})/\mathbb{Q}$, and $a = -1$. The fundamental unit $u = 6\sqrt{34} + 35$ has norm $+1$, hence a cannot be the norm of an integer (in L). However we have $\mathcal{N}_{L/K}((\sqrt{34}+5)/3) = -1$.

The existence of rational solutions to the equation $\mathcal{N}_{L/K}(x) = a$ could make us think that there is no way to reduce this problem to a finite number of tests. Our goal is to show that, on the contrary, this is possible by giving a bound on the denominator or, more precisely, by giving a finite list of prime ideals that can occur in the numerator or in the denominator. Our theorem makes it possible to answer algorithmically the question of existence of a rational solution and at the same time constructs such a solution.

Let S be a finite set of prime ideals of the base field K. We say that an element $a \in K^*$ (resp. $x \in L^*$) is an S-unit if the only primes occuring in the prime ideal decomposition of a (resp. x) are in the set S (resp. above a prime ideal in S). We denote by $\mathbb{U}_{K,S}$ the set of S-units of K and $\mathbb{U}_{L,S}$ those of L. We are looking for solutions x as S-units. It is clear that all primes dividing a may have a contribution in the solutions x, and we will therefore assume that S contains all prime ideals dividing a so that a is an S-unit.

It is clear that the norm of an S-unit of L is an S-unit of K; in other words that $\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) \subset \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$. In view of the previous example, the reverse inclusion is not true (in this case with $S = \emptyset$): an S-unit which is a norm is not always the norm of an S-unit.

The theorem that we shall prove asserts that we have equality as soon as S is large enough, that is as soon as S contains some subset S_0 depending only on the extension L/K. This is to say that in order to solve the equation $\mathcal{N}_{L/K}(x) = a$, it is enough to consider all prime ideals dividing a, together with all exceptional prime ideals of S_0.

Theorem 1.1. *Let L/K be an extension of number fields. There exists a finite set S_0 of prime ideals of K depending only on L/K such that*

$$\text{if } S \supset S_0, \text{ then } \mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

Such an S_0 is given explicitly in terms of some class groups. When S does not contain S_0, it is still possible to give results about the quotient group $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$, which are more precise when the extension is Galois, and even more precise when it is cyclic.

General notation:

If a and b are two integers, (a, b) is the *gcd* of a and b.

If G is a finite group, $|G|$ denotes its order. We say that a finite group G is an n-group if each prime dividing $|G|$ also divides n. If G is abelian, we say that G has *exponent* d if $g^d = 1$ for all $g \in G$, and d is minimal with this property. For a prime p, G_p is the p-Sylow of G.

If G acts on a group A, A^G is the subgroup of elements fixed by G. The notation ${}_{\mathcal{N}}A$ denotes the kernel of a map $\mathcal{N} : A \to B$ (typically a norm map).

2. S-units and S-class groups

In this section we recall the fundamental notions about the S-units of a number field K, without giving the proofs. For more details, see [13].

Let S be a finite set of prime ideals of K. We say that $x \in K$ is an *S-integer* if $v_{\mathfrak{p}}(x) \geqslant 0$ for all $\mathfrak{p} \notin S$. We say that $x \in K^*$ is an *S-unit* if $v_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p} \notin S$. We write $\mathbb{Z}_{K,S}$ for the ring of all S-integers of K, and $\mathbb{U}_{K,S}$ for the multiplicative group of all S-units of K^*. The invertible elements of $\mathbb{Z}_{K,S}$ are exactly the S-units. We denote by $\mathcal{I}_S(K)$ the group of fractionnal ideals of $\mathbb{Z}_{K,S}$ and $\mathcal{P}_S(K)$ the subgroup of principal ideals (we sometimes say S-principal). We call $\langle S \rangle$ the group of ideals I such that $v_{\mathfrak{p}}(I) = 0$ for all $\mathfrak{p} \notin S$, and we say that an ideal I is S-integral if $v_{\mathfrak{p}}(x) \geqslant 0$ for all $\mathfrak{p} \notin S$.

If L/K is an extension of K, and S is still a finite set of prime ideals of the ground field K, we say that $x \in L^*$ is an S-unit if $v_{\mathfrak{P}}(x) = 0$ for all primes $\mathfrak{P}$ except perhaps for those above S. Because there is no possible confusion, we allow the notation $\mathfrak{P} \in S$ instead of $\mathfrak{P}$ above $\mathfrak{p} \in S$. The same kind of definition holds for the S-integers in L. We denote by $\mathbb{U}_{L,S}$ (resp. $\mathbb{Z}_{L,S}$) the set of S-units (resp. S-integers) of L.

Copying the definition of the class group $\mathrm{Cl}(K)$ as the quotient $\mathcal{I}(K)/\mathcal{P}(K)$, we define the *$S$-class group* $\mathrm{Cl}_S(K)$ as the quotient $\mathcal{I}_S(K)/\mathcal{P}_S(K)$.

Proposition 2.1. *The following diagram is exact.*

$$
\begin{array}{ccccccccccc}
 & & & & & & 1 & & 1 & & \\
 & & & & & & \downarrow & & \downarrow & & \\
1 & \to & \mathbb{U}_K & \to & \mathbb{U}_{K,S} & \to & < S > & \to & \mathrm{Cl}(< S >) & \to & 1 \\
 & & & & & & \downarrow & & \downarrow & & \\
1 & \to & \mathbb{U}_K & \to & K^* & \to & \mathcal{I}(K) & \to & \mathrm{Cl}(K) & \to & 1 \\
 & & & & & & \downarrow & & \downarrow & & \\
1 & \to & \mathbb{U}_{K,S} & \to & K^* & \to & \mathcal{I}_S(K) & \to & \mathrm{Cl}_S(K) & \to & 1 \\
 & & & & & & \downarrow & & \downarrow & & \\
 & & & & & & 1 & & 1 & &
\end{array}
$$

This proposition shows in particular that $\mathbb{U}_{K,S}/\mathbb{U}_K$ is a free $\mathbb{Z}$-module of rank equal to the cardinality of S, and that the group $\mathrm{Cl}_S(K)$ is the quotient of the group $\mathrm{Cl}(K)$ by the subgroup generated by S. In particular this group is finite, and its order divides the order of $\mathrm{Cl}(K)$.

3. Relative class groups

If L/K is a relative extension of number fields, there exists at least two canonical morphisms between $\mathrm{Cl}(L)$ and $\mathrm{Cl}(K)$. Indeed, if I_L is an ideal of L, we can take its norm in K. This morphism allows us to define a morphism $\mathcal{N}_{L/K}$ from $\mathrm{Cl}(L)$ to $\mathrm{Cl}(K)$. If I_K is an (integral) ideal of K, we can form the ideal $I_K\mathbb{Z}_L$ of L. This extends to a morphism on fractional ideals, and to a morphism i from $\mathrm{Cl}(K)$ to $\mathrm{Cl}(L)$. These two different morphisms lead to two different definitions of relative class groups for the extension L/K.

3.1. **Definitions.** The map $I_K \mapsto I_K\mathbb{Z}_L$ induces a morphism i from $\mathrm{Cl}(K)$ to $\mathrm{Cl}(L)$, and suggests the following definition.

Definition 3.1. An ideal I_L of L is *pseudo-principal* if there exists $\alpha \in L$ and an ideal I_K of K such that $I_L = \alpha I_K\mathbb{Z}_L$. If $\mathcal{I}$ is the group of fractional ideals of L,

we write $\mathcal{PP}$ for the subgroup of all pseudo-principal ideals. We define the *relative pseudo-class group* by

$$\mathrm{Cl}_i(L/K) = \mathcal{I}/\mathcal{PP}.$$

Remark. It is clear that $\mathcal{PP}$ is a subgroup of $\mathcal{I}$ containing the subgroup of principal ideals of L, and hence that $\mathrm{Cl}_i(L/K)$ is a quotient of $\mathrm{Cl}(L)$. In particular its order is finite. In fact we have $\mathrm{Cl}_i(L/K) = \mathrm{Cl}(L)/i(\mathrm{Cl}(K)) = \mathrm{Coker}(i)$. For example, if $\mathrm{Cl}(K) = 1$, then $\mathrm{Cl}_i(L/K) = \mathrm{Cl}(L)$. We also define the *capitulation group* as $\mathrm{Cl}_i(K) = \mathrm{Ker}(i)$.

The map $I_L \mapsto \mathcal{N}_{L/K}(I_L)$ on ideals induces a morphism $\mathcal{N}_{L/K}$ from $\mathrm{Cl}(L)$ to $\mathrm{Cl}(K)$ and suggests the following definition.

Definition 3.2. The *relative norm class group* $\mathrm{Cl}_{\mathcal{N}}(L/K)$ is the subgroup of $\mathrm{Cl}(L)$ defined by

$$\mathrm{Cl}_{\mathcal{N}}(L/K) = \mathrm{Ker}(\mathcal{N}_{L/K}).$$

Remark. As a subgroup of $\mathrm{Cl}(L)$, $\mathrm{Cl}_{\mathcal{N}}(L/K)$ is necessarily finite. If $\mathrm{Cl}(K) = 1$, then $\mathrm{Cl}_{\mathcal{N}}(L/K) = \mathrm{Cl}(L) = \mathrm{Cl}_i(L/K)$. We also define the group $\mathrm{Cl}_{\mathcal{N}}(K) = \mathrm{Coker}(\mathcal{N}_{L/K}) = \mathrm{Cl}(K)/\mathcal{N}_{L/K}(\mathrm{Cl}(L))$.

As we defined the S-class group in the previous section for an arbitrary set S of prime ideals, we can define the S-relative-pseudo-class-group and the S-relative-norm-class-group by

$$\mathrm{Cl}_{i,S}(L/K) = \mathrm{Cl}_S(L)/i(\mathrm{Cl}_S(K)) = \mathrm{Cl}_i(L/K)/\langle S\rangle,$$

$$\mathrm{Cl}_{\mathcal{N},S}(L/K) = \mathrm{Ker}\left(\mathrm{Cl}_S(L) \overset{\mathcal{N}_{L/K}}{\to} \mathrm{Cl}_S(K)\right) = \mathrm{Cl}_{\mathcal{N}}(L/K)/\langle S\rangle.$$

3.2. **Relations between class groups.** We saw that when $\mathrm{Cl}(K) = 1$, the two relative class groups are equal and coincide with $\mathrm{Cl}(L)$. In the general case they are not equal any more, but we can give some relations between them. We recall here the exact sequences resulting from the definitions:

$$\begin{array}{ccccccccccc} 1 & \to & \mathrm{Cl}_i(K) & \to & \mathrm{Cl}(K) & \overset{i}{\to} & \mathrm{Cl}(L) & \to & \mathrm{Cl}_i(L/K) & \to & 1, \\ 1 & \to & \mathrm{Cl}_{\mathcal{N}}(L/K) & \to & \mathrm{Cl}(L) & \overset{\mathcal{N}_{L/K}}{\to} & \mathrm{Cl}(K) & \to & \mathrm{Cl}_{\mathcal{N}}(K) & \to & 1. \end{array}$$

We denote by $[m]$ the map on a group G consisting in taking the mth power. The previous exact sequences remain exact if we take the p-Sylow of each group. If we denote by $d = [L : K]$ the degree of the extension, we have $\mathcal{N}_{L/K} \circ i = [d]$.

Proposition 3.3. *If $p \nmid h(K)$, then $\mathrm{Cl}(K)_p = \mathrm{Cl}_i(K)_p = \mathrm{Cl}_{\mathcal{N}}(K)_p = 1$ and $\mathrm{Cl}(L)_p \sim \mathrm{Cl}_i(L/K)_p \sim \mathrm{Cl}_{\mathcal{N}}(L/K)_p$. These three groups are generated by the classes of the same ideals.*

If $p \nmid d$, then $\mathrm{Cl}_i(K)_p = \mathrm{Cl}_{\mathcal{N}}(K)_p = 1$ and $\mathrm{Cl}_i(L/K)_p \sim \mathrm{Cl}_{\mathcal{N}}(L/K)_p$. These two groups are generated by the classes of the same ideals.

For a proof of this see [13]. Thus the two notions of relative class groups only differ for the primes dividing $(d, h(K))$. We now give an example that shows that these two groups are not always equal.

Example. Let $K = \mathbb{Q}(y)$ with $y^2 + 30 = 0$. The class group of K is of type $C_2 \times C_2$ generated by the ramified primes $\mathfrak{p}_3$ and $\mathfrak{p}_5$.

Let $L = K(x)$ with $x^2 - y = 0$. In this case, we have $(d, h(K)) = 2$. The class group of L is of type $C_4 \times C_2$ generated by the (totally ramified) primes $\mathfrak{P}_3$ (of order 4) and $\mathfrak{P}_5$ (of order 2). The relations $\mathcal{N}_{L/K}(\mathfrak{P}_3) = \mathfrak{p}_3$ and $\mathcal{N}_{L/K}(\mathfrak{P}_5) = \mathfrak{p}_5$ show that $\mathrm{Cl}_{\mathcal{N}}(L/K) \sim C_2$ is generated by $\mathfrak{P}_3^2$. Moreover, the relations $\mathfrak{p}_3\mathbb{Z}_L = \mathfrak{P}_3^2$ and $\mathfrak{p}_5\mathbb{Z}_L = \mathfrak{P}_5^2$ show that $\mathrm{Cl}_i(L/K) \sim C_2 \times C_2$ is generated by $\mathfrak{P}_3$ and $\mathfrak{P}_5$.

4. Norm equations in Galois extensions

In the case where L/K is a Galois extension, the situation is quite simple and, for this reason, we consider this case first. The results that we obtain are more precise than in [7].

4.1. **Proof of Theorem 1.1 for Galois extensions.** Before proving Theorem 1.1, we study in detail the example of the introduction so that we can have an idea of the general result.

Example. The extension L/K is the real quadratic extension $\mathbb{Q}(\sqrt{34})/\mathbb{Q}$ of discriminant 136. The fundamental unit is $6\sqrt{34} + 35$ of norm $+1$. We have the following relations:

$$\mathcal{N}_{L/K}((\sqrt{34}+5)/3) = -1,$$

$$\mathcal{N}_{L/K}((\sqrt{34}+3)/5) = -1,$$

$$\mathcal{N}_{L/K}((5\sqrt{34}+27)/11) = -1,$$

$$\mathcal{N}_{L/K}((5\sqrt{34}+3)/29) = -1,$$

$$\mathcal{N}_{L/K}((25\sqrt{34}+141)/37) = -1, \ldots.$$

Thus we can find S-units of norm -1 as soon as S contains one of the primes 3, 5, 11, 29, 37, ... But it happens that the field $L = \mathbb{Q}(\sqrt{34})$ has a nontrivial class group of order 2, and can be generated by primes above 3, 5, 11, 29, 37, ... The condition for -1 to be the norm of an S-unit seems in this case to be that S generates the class group of L: this is exactly what we will prove.

We will always denote by S a finite set of prime ideals of the base field K, and by abuse of notation (justified by the definition of S-units given in Section 2), by the same letter S the set of all prime ideals above S for each finite extension of K.

Lemma 4.1. *Let L/K be a Galois extension, S a finite set of prime ideals of K. Let A be an S-integral ideal of K, and X,Y two S-integral ideals of L. Assume that they satisfy the relation $\mathcal{N}_{L/K}(X) = A \cdot \mathcal{N}_{L/K}(Y)$ and that there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of L (not in S) such that their product divides Y. Then there exist some conjugates $\sigma_1(\mathfrak{p}_1), \ldots, \sigma_k(\mathfrak{p}_k)$ of $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ such that $\prod_{1 \leqslant i \leqslant k} \sigma_i(\mathfrak{p}_i)$ divides X.*

Proof. This is easily proved by induction on k. □

Theorem 4.2. (Galois case) *If L/K is Galois and if S_0 generates the relative class group $\mathrm{Cl}_i(L/K)$, then for all $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$$

$$\text{and } \mathcal{N}_{L/K}(\mathbb{Z}_{L,S}) = \mathcal{N}_{L/K}(L) \cap \mathbb{Z}_{K,S}.$$

Proof. Let $S \supset S_0$. Both inclusions $\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) \subset \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$ and $\mathcal{N}_{L/K}(\mathbb{Z}_{L,S}) \subset \mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S}$ are obvious.

Conversely, let $a \in \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$ (resp. $a \in \mathcal{N}_{L/K}(L^*) \cap \mathbb{Z}_{K,S}$) and $x, y \in \mathbb{Z}_{L,S}$ be such that $\mathcal{N}_{L/K}(x/y) = a$. We can write $\mathcal{N}_{L/K}(x) = a\mathcal{N}_{L/K}(y)$. Let $\prod \mathfrak{p}_i$ be the prime ideal factorization of the principal ideal $y\mathbb{Z}_{L,S}$. According to Lemma 4.1, there exist some conjugates $\sigma_i(\mathfrak{p}_i)$ of the $\mathfrak{p}_i$ such that $\prod \sigma_i(\mathfrak{p}_i)$ divides the principal ideal $x\mathbb{Z}_{L,S}$. Let X be the S-integral ideal of L such that

$$x\mathbb{Z}_{L,S} = \prod \sigma_i(\mathfrak{p}_i) \cdot X.$$

We now use the fact that S_0 generates the relative class group $\mathrm{Cl}_i(L/K)$. Each ideal $\mathfrak{p}_i$ is S_0-pseudo-principal and can be written in the form $\mathfrak{p}_i = \pi_i \cdot \mathfrak{q}_i\mathbb{Z}_{L,S}$, where π_i is an element of L^* and $\mathfrak{q}_i$ an ideal of K. This gives

$$y\mathbb{Z}_{L,S} = \prod \pi_i \prod \mathfrak{q}_i\mathbb{Z}_{L,S},$$

and since $\mathfrak{q}_i\mathbb{Z}_{L,S}$ is fixed by σ_i, we also have

$$x\mathbb{Z}_{L,S} = \prod \sigma_i(\pi_i) \prod \mathfrak{q}_i\mathbb{Z}_{L,S} \cdot X.$$

Now if we set

$$u = \left(x/\prod \sigma_i(\pi_i)\right) / \left(y/\prod \pi_i\right),$$

we have $\mathcal{N}_{L/K}(u) = a$. The previous relations show that

$$u\mathbb{Z}_{L,S} = \frac{X \prod \mathfrak{q}_i\mathbb{Z}_{L,S}}{\prod \mathfrak{q}_i\mathbb{Z}_{L,S}} = X,$$

and hence that u is an S-integer. The second equality of the theorem is then proved. To prove the first one, it remains only to remember that if an S-unit a is the norm of an S-integer u, then u is necessarily an S-unit. □

Corollary 4.3. *Let L/K be a Galois extension such that the group $\mathrm{Cl}_i(L/K)$ is trivial, and a an integer in K, then:*

The equation $\mathcal{N}_{L/K}(x) = a$ has a rational solution if and only if it has an integral solution.

More generally, if S is an arbitrary set of prime ideals whose classes generate $\mathrm{Cl}_i(L/K)$ and if a is an S-integer, then:

The equation $\mathcal{N}_{L/K}(x) = a$ has a rational solution if and only if it has an S-integral solution.

Example. We can illustrate this corollary by the following examples. All the equations $x^2 + y^2 = n$, $x^2 + 2y^2 = n$, $x^2 + xy + y^2 = n$, $x^3 + y^3 + 9z^3 - 3xy^2 - 9xz^2 - 9yz^2 + 9xyz = n$, ... have a rational solution if and only if they have an integral solution (they correspond to norm equations for Galois extensions with class number 1).

4.2. **Structure in the Galois case.** In this subsection, we will use Tate cohomology for the finite group $G = \mathrm{Gal}(L/K)$. For a description of this theory we refer to [11] or to [2]. If A is a G-module, we have for example $\widehat{H}^0(G, A) = A^G/\mathcal{N}(A)$, where A^G is the set of elements fixed by G and $\mathcal{N}(A)$ is the image of the norm map. We also have $\widehat{H}^{-1}(G, A) = {}_{\mathcal{N}}A/I_G A$, where ${}_{\mathcal{N}}A$ is the kernel of the norm map and I_G is the augmentation ideal of $\mathbb{Z}[G]$.

Let S denote a set of primes of K with the only condition that it is finite. We first recall a standard lemma of Noether, which says that any ideal of norm 1 is a product of ideals of the form $I^{\sigma-1}$.

Lemma 4.4. (Noether) *We have* $\widehat{H}^{-1}(G, \mathcal{I}_S(L)) = 1$.

Theorem 4.5. *For all S there exists a surjective map*

$$\frac{\widehat{H}^{-2}(G, \mathrm{Cl}_S(L))}{\mathrm{Im}(\widehat{H}^{-2}(G, \mathcal{I}_S(L)))} \to \frac{\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}}{\mathcal{N}_{L/K}(\mathbb{U}_{L,S})}.$$

If G is cyclic, this map defines an isomorphism

$$\frac{\mathrm{Cl}_S(L)^G}{\mathrm{Cl}_S(\mathcal{I}_S(L)^G)} \sim \frac{\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}}{\mathcal{N}_{L/K}(\mathbb{U}_{L,S})}.$$

Proof. Let denote by Ker the quotient $\left(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}\right) / \mathcal{N}_{L/K}(\mathbb{U}_{L,S})$. We first notice that Ker is the kernel of the natural map

$$\widehat{H}^0(G, \mathbb{U}_{L,S}) \quad \to \quad \widehat{H}^0(G, L^*).$$

The short exact sequences

$$1 \to \mathbb{U}_{L,S} \to L^* \to \mathcal{P}_S(L) \to 1,$$

$$1 \to \mathcal{P}_S(L) \to \mathcal{I}_S(L) \to \mathrm{Cl}_S(L) \to 1$$

lead to the long cohomology exact sequences

$$\widehat{H}^{-1}(G, L^*) \to \widehat{H}^{-1}(G, \mathcal{P}_S(L)) \to \widehat{H}^0(G, \mathbb{U}_{L,S}) \to \widehat{H}^0(G, L^*),$$

$$\widehat{H}^{-2}(G, \mathcal{I}_S(L)) \to \widehat{H}^{-2}(G, \mathrm{Cl}_S(L)) \to \widehat{H}^{-1}(G, \mathcal{P}_S(L)) \to \widehat{H}^{-1}(G, \mathcal{I}_S(L)) = 1.$$

From the first sequence and if G is cyclic, Hilbert's theorem 90 tells us that $\widehat{H}^{-1}(G, L^*) = 1$, so that $\widehat{H}^{-1}(G, \mathcal{P}_S(L)) = \mathrm{Ker}$. In the general case Ker is only a quotient of $\widehat{H}^{-1}(G, \mathcal{P}_S(L))$. From the second one, we can see that $\widehat{H}^{-1}(G, \mathcal{P}_S(L))$ is always isomorphic to the quotient of $\widehat{H}^{-2}(G, \mathrm{Cl}_S(L))$ by $\mathrm{Im}\left(\widehat{H}^{-2}(G, \mathcal{I}_S(L))\right)$. If G is cyclic, we have $\widehat{H}^{-2}(G, *) = \widehat{H}^0(G, *)$ (see [11]) so the last quotient is exactly $\mathrm{Cl}_S(L)^G / \mathrm{Cl}_S(\mathcal{I}_S(L)^G)$. □

The cyclic case of this theorem is a version of the "ambiguous classes formula" given in [3].

If we denote by I_G the augmentation ideal of the ring $\mathbb{Z}[G]$, we can interpret the group $\widehat{H}^{-2}(G, \mathrm{Cl}_S(L))$ as

$$\{\sum_{\sigma \in G} (\sigma - 1) \otimes x_\sigma \in I_G \otimes_{\mathbb{Z}} \mathrm{Cl}_S(L) : \prod_\sigma x_\sigma^{\sigma-1} = 1 \text{ in } \mathrm{Cl}_S(L)\}.$$

This can be seen as a subgroup of $\mathrm{Cl}_S(L)^{|G|-1}$. From this we can consider the quotient of $\widehat{H}^{-2}$ groups in the theorem as a quotient of a subgroup of

$$\left(\mathrm{Cl}_S(L) / \mathrm{Cl}_S(\mathcal{I}_S(L)^G)\right)^{|G|-1},$$

which is itself a quotient of $\mathrm{Cl}_{i,S}(L/K)^{|G|-1}$. This is expressed in the following corollary.

Corollary 4.6. *Let $r = |G| - 1$. For all S there exists a subgroup $\mathrm{Cl}_{i,S}(L/K)^{r,0}$ of $\mathrm{Cl}_{i,S}(L/K)^r$ and a morphism*

$$\phi : \mathrm{Cl}_{i,S}(L/K)^{r,0} \to (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$$

which is onto.

If u is an S-unit of K, then we have the trivial relation $\mathcal{N}_{L/K}(u) = u^{[L:K]}$, which shows that the group $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$ has an exponent dividing $[L : K]$. This simple remark shows that in Theorem 4.5 (or in Corollary 4.6) it is enough to consider the $[L : K]$-parts of the class groups. For example we have the following corollary.

Corollary 4.7. *Let L/K be a Galois extension and S_0 a finite set of prime ideals of K such that the cardinality of $\mathrm{Cl}_{i,S_0}(L/K)$ is coprime to the degree $[L : K]$ of the extension. Then for all $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S},$$

so that Theorem 1.1 is true with this S_0.

Remark. The assumption that $[L : K]$ is coprime to $|\mathrm{Cl}_{i,S_0}(L)|$ is not enough to prove, as in Theorem 4.2, that all integers that are norms are norms of integers. We illustrate this by an example.

Example. Let $L/K = \mathbb{Q}(\sqrt{229})/\mathbb{Q}$. The group $\mathrm{Cl}(L)$ has order 3 (coprime to 2), and is generated by an ideal $\mathfrak{p}$ above 3. The integer 3 is a norm since

$$\mathcal{N}_{L/K}((16 - \sqrt{229})/3) = 3.$$

But it cannot be the norm of an integer x, otherwise this x would generate one of the two ideals above 3, which are not principal.

We saw in subsection 3.1 that there exist at least two different definitions for the relative class group. The following example shows that Corollary 4.7 is false if we replace $\mathrm{Cl}_i(L/K)$ by $\mathrm{Cl}_{\mathcal{N}}(L/K)$.

Example. Let $K = \mathbb{Q}(y)$ with $y^2 - y - 26 = 0$. The discriminant of K is 105 and its class group has order 2 generated by the prime ideal $\mathfrak{p}_2 = 2\mathbb{Z}_K + (y + 1)\mathbb{Z}_K$ above 2. We consider $L = K(x)$ with $x^2 + (-2y + 1)x - 158 = 0$, so we have $x^4 - 421x^2 + 24964 = 0$. This field L is nothing but $\mathbb{Q}(\sqrt{105}, \sqrt{737})$, with discriminant $105^2 737^2$. In the relative extension L/K, -1 is a norm since

$$\mathcal{N}_{L/K}\left(\frac{(18808y + 87240)x + (-352680y - 1625419)}{((44y - 330)x + (1124y - 4777))^3}\right) = -1.$$

The class group $\mathrm{Cl}(L)$ is of type $C_6 \times C_2$, generated by a prime ideal $\mathfrak{P}_2$ above $\mathfrak{p}_2$ (above 2) of order 6, and a prime ideal $\mathfrak{P}_{59}$ above 59 of order 2. We have

$$\mathcal{N}_{L/K}(\mathfrak{P}_2) = \mathfrak{p}_2 \text{ and } \mathcal{N}_{L/K}(\mathfrak{P}_{59}) = (4y - 21)\mathbb{Z}_K.$$

Hence, the group $\mathrm{Cl}_{\mathcal{N}}(L/K) = \mathrm{Ker}(\mathcal{N}_{L/K})$ has order 6, and its 2-Sylow is generated by $\mathfrak{P}_{59}$. If Corollary 4.7 was true with $\mathrm{Cl}_{\mathcal{N}}(L/K)$ instead of $\mathrm{Cl}_i(L/K)$, then -1 should be the norm of a 59-unit. We now prove that it is not the case.

The fundamental units of L are

$$\begin{aligned} u_1 &= 8y + 37, \\ u_2 &= (17952y - 8976)x + 777239, \\ u_3 &= -18636936x + (18636936y + 243656915), \end{aligned}$$

whose norms are $(8y+37)^2$, 1 and 1, where $8y+37$ is the fundamental unit of K. Therefore, the units cannot have any contribution to the norms. The supplementary fundamental 59-units are given by

$$\begin{aligned} s_1 &= 4x + (26y - 221), \\ s_2 &= 230x + (-230y + 3237), \\ s_3 &= 4y - 21, \\ s_4 &= 59. \end{aligned}$$

We remark that s_3 and s_4 (together with $8y+37$) form a system of fundamental 59-units of K, and for this reason they cannot contribute to the norms. The norms of s_1 and s_2 are $(8y+37)^{-1}(4y-21)^2$ and $-59(4y-21)$. This proves that the only unit which is the norm of a nontrivial 59-unit is $(8y+37)$, but not -1.

5. Norm equations in non-Galois extensions

In this section we consider an extension L/K which is not necessarily Galois. We call $\mathfrak{L}/K$ its Galois closure. We denote by G the Galois group of $\mathfrak{L}/K$, and by H the subgroup of G corresponding to the Galois extension $\mathfrak{L}/L$. We write $d = [L:K]$ and $|H| = [\mathfrak{L}:L]$.

5.1. **Preliminaries.** Before proving Theorem 1.1 in the general case, we prove a proposition relative to this case. With the previous notation, we have

Proposition 5.1. *If S is a finite set of primes in K, then the group*

$$(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$$

has an exponent dividing both d and $|H| \cdot |\operatorname{Cl}_{i,S}(\mathfrak{L}/K)|$.

Proof. Because of the trivial relation $a^d = \mathcal{N}_{L/K}(a)$, the first claim is obvious. For the second one we apply Corollary 4.6 to the Galois extension $\mathfrak{L}/K$. □

Corollary 5.2. *Let L/K be an extension such that d is coprime to $|H|$ and S_0 be a finite set of prime ideals of K. If S_0 is such that $h = |\operatorname{Cl}_{i,S_0}(\mathfrak{L}/K)|$ is coprime to d, then for all $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S},$$

so that Theorem 1.1 is true with this S_0.

This corollary applies for example to Galois extensions ($|H| = 1$, this is exactly Corollary 4.7). In the special case where d is prime, the degree $|H| = [\mathfrak{L}:L]$ must divide $(d-1)!$, so d and $|H|$ are always coprime, and this corollary also applies to this case. For small degrees ($d \leqslant 5$), the only extensions that are not dealt with by this proposition are those with Galois group D_4 (dihedral group of order 8) or S_4 (symmetric group on 4 letters).

We shall now give an example where the group $\operatorname{Cl}(\mathfrak{L})$ (and not only $\operatorname{Cl}(L)$) must be used.

Example. Let $L/K = \mathbb{Q}(x)/\mathbb{Q}$ with $x^4 - x^3 - 27x^2 + 3x + 149 = 0$. This field is of type D_4, and has discriminant $62525 = 5^2 \cdot 41 \cdot 61$. Its class group is trivial, whereas the class group of its Galois closure $\mathfrak{L}$ is of type $C_4 \times C_2$ generated by two prime ideals above 11 (or equivalently 79,151,181,191 ...). All units of L have norm $+1$, and therefore -1 cannot be the norm of a unit. However, we have the relation

$$\mathcal{N}_{L/K}((x^3 - 2x^2 - 14x + 6)/11) = -1,$$

which proves that -1 is the norm of an 11-unit. We have the further relations:

$$\mathcal{N}_{L/K}((28x^3+5x^2-341x+63)/395) = -1,$$

$$\mathcal{N}_{L/K}((29x^3-102x^2-244x+1156)/151) = -1,$$

$$\mathcal{N}_{L/K}((68x^3-135x^2-971x-77)/905) = -1,$$

$$\mathcal{N}_{L/K}((20x^3-32x^2-177x+510)/191) = -1,$$

which prove that -1 is the norm of a 79-unit, a 151-unit, a 181-unit, a 191-unit ... .

5.2. **Proof of Theorem 1.1 for non-Galois extensions.** In the case where the extension is not Galois any more, the conditions on S_0 are more restrictive and the proof is more technical. It uses some ideas found in [1].

We introduce some additional notation.

If C is a subgroup of the Galois group G, $\mathfrak{L}^C$ denotes the subfield of $\mathfrak{L}$ of those elements fixed by the action of C (for example $\mathfrak{L}^H = L$). The group $\mathbb{Z}[G/C]$ is the free abelian group generated by the elements of the quotient G/C, $\mathbb{Z}[G/C]^H$ is the subgroup of $\mathbb{Z}[G/C]$ of the elements fixed by H (for left multiplication), and $\mathbb{Z}[G/C]^{0,H}$ is the subgroup of $\mathbb{Z}[G/C]$ of all elements $\sum a_i\sigma_i C$ fixed by H, and such that $\sum a_i = 0$.

Easy computations in the ring $\mathbb{Z}[G/C]$ lead to the following lemma giving a generalization of Noether's Lemma 4.4 (also true for S-ideals).

Lemma 5.3. *If $\tau \in \mathbb{Z}[G/C]^{0,H}$, then the map $x \mapsto x^\tau$ maps $\mathfrak{L}^C$ into the kernel of the norm $\mathcal{N}_{L/K}$, denoted by ${}_{\mathcal{N}}L^*$. This also hold for ideals. Conversely, any ideal of L of norm 1 over K is a product (over C and τ) of such ideals.*

Proof. Only the second assertion needs some detail. Let I be an ideal of L whose norm is 1 (or $\mathbb{Z}_{K,S}$ if we are dealing with S-ideals). For each ideal p of K, we choose one ideal $\mathfrak{P}$ of $\mathfrak{L}$ above p. Now if we factor I in $\mathfrak{L}$, this must be of the form $\prod \mathfrak{P}^\tau$, with $\tau \in \mathbb{Z}[G]$. Since $\mathfrak{P}$ is fixed by its decomposition group $C_\mathfrak{P}$, τ is in fact in $\mathbb{Z}[G/C_\mathfrak{P}]$. Since I is an ideal of L, it is fixed by H, and $\tau \in \mathbb{Z}[G/C_\mathfrak{P}]^H$. Now the triviality of the norm of I forces τ to be in $\mathbb{Z}[G/C_\mathfrak{P}]^{0,H}$. □

In the following, C runs over all cyclic subgroups of G. Consider now the group $\prod_C = \prod_C \mathrm{Cl}_{i,S}(\mathfrak{L}^C/K) \otimes \mathbb{Z}[G/C]^{0,H}$, and note that if $\tau \in \mathbb{Z}[G/C]^{0,H}$, then $I^\tau = 1$ for any ideal I of $\mathfrak{L}^C$ fixed by G. This observation allows the construction of a map from $\prod_C$ to $\mathrm{Cl}_S(L)$, defined by the formula $\sum x_\tau \otimes \tau \mapsto \prod \tau(x_\tau)$. By analogy with Theorem 4.5, we write $\widehat{\mathcal{H}}_C^{-2}$ for the kernel of this map. The next proposition is a generalization of Theorem 4.5.

Proposition 5.4. (Non-Galois case) *For all finite sets S containing the primes of K ramified in L, there exists a surjective map*

$$\phi_C : \quad \widehat{\mathcal{H}}_C^{-2} \quad \to \quad (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S}).$$

Proof. Let $\sum I_{C,i} \otimes \tau_{C,i}$ be in $\widehat{\mathcal{H}}^{-2}$. We define ϕ_C as the composite of the maps

$$\sum I_{C,i} \otimes \tau_{C,i} \quad \mapsto \quad \prod (I_{C,i})^{\tau_{C,i}} = x\mathbb{Z}_{L,S} \quad \mapsto \quad \mathcal{N}_{L/K}(x).$$

Using Lemma 5.3, we verify that this is a well-defined map. We have to prove its surjectivity.

Let $a \in \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$, and $x \in L^*$ such that $a = \mathcal{N}_{L/K}(x)$. According to Lemma 5.3, the principal ideal $x\mathbb{Z}_{L,S}$ has the form $\prod I_{C,i}^{\tau_{C,i}}$. Since we are looking only at S-ideals, and S contains the ramified primes of $\mathfrak{L}/K$, the decomposition groups C are all cyclic. Since the ideals $I_{C,i}$ are fixed by C and are unramified, they can be considered either as ideals of $\mathfrak{L}$ or as ideals of $\mathfrak{L}^C$. Taking the classes of $I_{C,i}$ in $\mathrm{Cl}_{i,S}(\mathfrak{L}^C/K)$, we build the element $\sum \bar{I}_{C,i} \otimes \tau_{C,i} \in \widehat{\mathcal{H}}_C^{-2}$.

It is now an easy calculation to verify that the image of this element is exactly a. □

The notation is the same as before, except that D only runs over the cyclic subgroups of G of prime power order. The group $\widehat{\mathcal{H}}_D^{-2}$ is defined similarly to $\widehat{\mathcal{H}}_C^{-2}$.

Theorem 5.5. (Non-Galois case) *For all finite sets S containing the primes of K ramified in L, there exists a surjective map*

$$\phi_D : \quad \widehat{\mathcal{H}}_D^{-2} \quad \to \quad (\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S}).$$

Proof. The definition of ϕ_D is exactly analogous to the definition of ϕ_C in Proposition 5.4. We prove that $\mathrm{Im}\,\phi_D \supset \mathrm{Im}\,\phi_C$ and use the surjectivity of ϕ_C.

Let $a = \phi_C(\sum \bar{I}_{C,\tau} \otimes \tau)$. Consider a cyclic subgroup C of G, of order $|C| = \prod p_i^{a_i}$. Consider also D_i its p_i-Sylow. We have a factorization $C = \prod D_i$. We build the groups $\widehat{D}_i = \prod_{j \neq i} D_j$. Since the p_i are disctinct primes, we can find a relation $\sum d_i |\widehat{D}_i| = 1$. Let now τ be an element of $\mathbb{Z}[G/C]^{0,H}$. We have

$$\tau = \sum d_i |\widehat{D}_i| \tau = \sum d_i \tau \widehat{D}_i,$$

where $\tau_i = \tau \widehat{D}_i$ can be seen as an element of $\mathbb{Z}[G/D_i]^{0,H}$. Since $\phi_C(\sum \bar{I}_{C,\tau} \otimes \tau) = \phi_D(\sum \bar{I}_{C,\tau} \otimes d_i \tau_i)$, our claim is proved. □

From this theorem, it is immediate to derive an explicit version of Theorem 1.1. We now make the assumption that $\mathrm{Cl}_i(\mathfrak{L}/K)$ has order h coprime to the degree $d = [L : K]$. Using successively information about $\mathbb{Z}[G/D]^{0,H}$ and $\mathrm{Cl}_i(\mathfrak{L}^D/K)$, we can reduce the assumptions for Theorem 1.1.

Proposition 5.6. *Let S be a finite set of prime ideals of K containing all ramified primes of L/K, and such that $\mathrm{Cl}_{i,S}(\mathfrak{L}/K)$ has order h coprime to $d = [L : K]$. If D is a cyclic subgroup of G of prime power order such that $H \cap \sigma D \sigma^{-1} = 1$ for all $\sigma \in G$, then $\mathrm{Cl}_{i,S}(\mathfrak{L}^D/K) \otimes \mathbb{Z}[G/D]^{0,H} \subset \widehat{\mathcal{H}}_D^{-2}$ and ϕ_D is trivial on this subgroup.*

Proof. In the above statement we make a little abuse of notation. Indeed, we will not prove this for the map ϕ_D, but for its composite with the map $x \mapsto x^h$. Since h is coprime to d, the map $x \mapsto x^h$ defines an automorphism of the group $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$, so the result remains.

Let $\{\gamma_i\}$ be a system of representatives of G/D. If two elements $\eta \in H$ and $\delta \in D$ are such that $\eta\gamma_i = \gamma_i\delta$ for some γ_i, then $\eta = \gamma_i \delta \gamma_i^{-1}$, but the assumption implies that $\eta = \delta = 1$. This means that we can choose $\{\gamma_i\}$ and $F = \{\phi_j\} \subset G$ such that $\{\gamma_i\}$ is equal to $H \cdot F$.

Let $\tau \in \mathbb{Z}[G/D]^{0,H} = \sum a_i \gamma_i = \sum a_{i,j} \eta_i \phi_j$. Since τ is fixed by multiplication on the left by H, $a_{i,j}$ only depends on j, and we have $\tau = (\sum_H \eta)\,(\sum a_j \phi_j)$. Moreover we have $\sum a_{i,j} = 0 = |H| \sum a_j$, hence $\tau = (\sum_H \eta)\,(\sum a_j(\phi_j - 1))$.

Now let I be an ideal of $\mathfrak{L}^D$. The ideal I^h is S-pseudo-principal in $\mathfrak{L}$, hence we can find $x \in \mathfrak{L}$ such that

$$I^{h\tau} = \mathcal{N}_{\mathfrak{L}/L}((x\mathbb{Z}_{L,S})^{\sum a_j(\phi_j-1)}) = \mathcal{N}_{\mathfrak{L}/L}(x^{\sum a_j(\phi_j-1)})\mathbb{Z}_{L,S},$$

and $\phi_D(I^h \otimes \tau) = \mathcal{N}_{L/K}(\mathcal{N}_{\mathfrak{L}/L}(x^{\sum a_j(\phi_j-1)})) = 1$. □

Corollary 5.7. *Let S_0 be a finite set of prime ideals of K containing all ramified primes of L/K, and such that $\mathrm{Cl}_{i,S_0}(\mathfrak{L}/K)$ has order h coprime to $d = [L : K]$. Assume moreover that for all cyclic subgroups D of G of order p^a with $p \mid (d, |H|)$ such that $D \cap H \neq \{1\}$, we have $\mathrm{Cl}_{i,S_0}(\mathfrak{L}^D/K)_p = 1$.*

With these assumptions, Theorem 1.1 holds.

Proof. Using Proposition 5.1, Theorem 5.5 and Proposition 5.6, we see that it is enough to prove that $\mathrm{Cl}_{i,S_0}(\mathfrak{L}^D/K)_l = 1$ for each prime l dividing $(d, |H|)$ and each cyclic subgroup D of order p^a, with $D \cap H \neq \{1\}$.

Let D and l be such that $p \neq l$. By Proposition 3.3 we know that $\mathrm{Cl}_{i,S_0}(\mathfrak{L}^D/K)_l \subset \mathrm{Cl}_{i,S_0}(\mathfrak{L}/K)_l = 1$. If $p = l$, then by assumption $\mathrm{Cl}_{i,S_0}(\mathfrak{L}^D/K)_l = 1$. □

By a careful examination of the subgroups of G, we can deduce two corollaries of this proposition.

Corollary 5.8. (D_4-extensions) *Let L/K be an extension of degree 4 of type D_4. If S_0 contains all ramified primes of L/K and if S_0 is such that $\mathrm{Cl}_{i,S_0}(\mathfrak{L}/K)$ and $\mathrm{Cl}_{i,S_0}(L/K)$ have odd order, then for all $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$$

so that Theorem 1.1 is true with S_0.

Corollary 5.9. (S_4-extensions) *Let L/K be an extension of degree 4 of type S_4. Let $\mathfrak{L}^{C_2}$ be one of the three conjugate cyclic subfields of $\mathfrak{L}$ of index 2 and containing L. If S_0 contains all ramified primes of L/K and if S_0 is such that $\mathrm{Cl}_{i,S_0}(\mathfrak{L}/K)$ and $\mathrm{Cl}_{i,S_0}(\mathfrak{L}^{C_2}/K)$ have odd order, then for all $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}$$

so that Theorem 1.1 is true with this S_0.

We shall give here an example which shows the necessity of the condition on the ramified primes.

Example. Let $L/K = \mathbb{Q}(x)/\mathbb{Q}$ with $x^4 - x^3 - 8x^2 + 9x + 3 = 0$. This field of discriminant $25857 = 3^2 \cdot 13^2 \cdot 17$ is of type D_4, and its class group is trivial. Its Galois closure $\mathfrak{L}$ has also a trivial class group. The fundamental units have norm $+1$. If we forget the condition on ramified primes in Corollary 5.8, it should imply that the equation $\mathcal{N}_{L/K}(x) = -1$ has no solution. However, we find

$$\mathcal{N}_{L/K}((x^3 + 2x^2 - 8x + 3)/6) = -1.$$

This number factors in the form $\mathfrak{p}_1\mathfrak{p}_2^{-1}$ with $\mathfrak{p}_1^2\mathfrak{p}_2^2 = 3$, so it is a 3-unit, and 3 is ramified because 3 divides the discriminant of the field L.

We remark that in this example, it is not enough to consider the discriminant of $\mathfrak{L}/L$ but really the discriminant of L/K (or equivalently the discriminant of $\mathfrak{L}/K$). Indeed only primes above 17 ramify in the extension $\mathfrak{L}/L$, whereas 3,13 and 17 ramify in L/K.

We can prove that this solution is unique up to the multiplication by an element of norm 1. This example is therefore of a completely different nature than the other ones where the solutions (up to elements of norm 1) were usually in infinite number, parametrized by all ideals with given class in some class group.

5.3. **The special case of extensions of $\mathbb{Q}$.** In Theorem 1.1 and in most of the other results we claim the existence of a set S_0 such that the groups $\mathcal{N}_{L/K}(\mathbb{U}_{L,S_0})$ and $\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S_0}$ are equal, and such that equality also holds for all larger S. There exists some cases, where equality holds for some S_0 but not for all S containing this S_0. We give here a criterion for this to be true, and an example where it is false.

Proposition 5.10. *If $\mathcal{N}_{L/K}(\mathbb{U}_{L,S_0}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S_0}$ and if $\mathrm{Cl}_{\mathcal{N},S_0}(L)$ has order h coprime to $d = [L:K]$, then for all $S \supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

Proof. Let $S \supset S_0$ satisfy the conditions and $a = \mathcal{N}_{L/K}(x) \in \mathbb{U}_{K,S}$. We can factor the principal ideal $x\mathbb{Z}_{L,S_0}$ in L:

$$x\mathbb{Z}_{L,S_0} = \prod_{\mathfrak{p}_i \in S} \mathfrak{p}_i^{a_i} \cdot \prod_{\mathfrak{p}_i' \notin S} \mathfrak{p}_i'^{\,a_i'} = I \cdot I'.$$

Since $\mathcal{N}_{L/K}(I') = 1$, the definition of h makes the ideal $I'^{\,h}$ S_0-principal. We then have $I'^{\,h} = z'\mathbb{Z}_{L,S_0}$. But $\mathcal{N}_{L/K}(z')$ is an S_0-unit, hence there exists $y \in \mathbb{U}_{L,S_0}$ with $\mathcal{N}_{L/K}(z') = \mathcal{N}_{L/K}(y)$. Now let $z = x^h/z'$: this is an S-unit. The relations

$$a^h = \mathcal{N}_{L/K}(x^h) = \mathcal{N}_{L/K}(zz') = \mathcal{N}_{L/K}(zy)$$

hold, and this proves that a^h is the norm of an S-unit. □

This allows us to consider the special case of extensions of $\mathbb{Q}$ with odd degree, or the totally complex ones, because in these two cases the units that are norms are well known.

Corollary 5.11. *Let $L/\mathbb{Q}$ be an extension of degree d. Assume either that d is odd or $L/\mathbb{Q}$ is totally complex. If the order h of $\mathrm{Cl}(L)$ is coprime to d, then for all S*

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S}.$$

We now give an example in which the equality holds for $S_0 = \emptyset$ but does not hold for some larger S.

Example. Let $L/K = \mathbb{Q}(x)/\mathbb{Q}$, with $x^3 - x^2 - 41x + 93 = 0$. This totally real extension of degree 3 has discriminant $28212 = 2^2 \cdot 3 \cdot 2351$ and has Galois group S_3 (so it is a non-Galois extension). It is clear that $\mathcal{N}_{L/\mathbb{Q}}(\mathbb{U}_L) = \mathbb{U}_{\mathbb{Q}}$. Consider now $S = \{3\}$. We have

$$\mathcal{N}_{L/\mathbb{Q}}((-3x^2 + 7x + 31)/31) = 3.$$

This proves that 3 is a norm, but the solution has 31 in the denominator. We shall prove that there is no 3-unit of norm 3. Suppose on the contrary that 3 is the norm of a 3-unit s. We have $3\mathbb{Z}_L = \mathfrak{p}_1^2\mathfrak{p}_2$ with $\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{p}_1) = 3$ and $\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{p}_2) = 3$, so we can write

$$s\mathbb{Z}_L = \mathfrak{p}_1^{v_1}\mathfrak{p}_2^{v_2}$$

with $v_1+v_2=1$. But the class group of L is cyclic of order 3, generated by $\mathfrak{p}_1$, and the principality of the ideal $s\mathbb{Z}_L$ forces the relation $v_1+v_2\equiv 0 \mod 3$. These two relations cannot hold together, which proves that 3 cannot be the norm of a 3-unit.

5.4. **Existence of integral solutions.** In this subsection, we are interested in finding integral solutions x when the parameter a is an algebraic integer. We will look for a generalization of Theorem 4.2 on the integers and the S-integers.

Remark. If we want the integers that are norms to be norms of integers, this should first be true for units; such results are given by Corollary 5.2 or 5.7. It is also necessary that all integral ideals that are norms be norms of integral ideals. The condition for this is weaker than the one for integers and is the object of the following lemma.

Lemma 5.12. *Let L/K be an extension (not necessarily Galois) of degree 3, 4 or 6, I_K an ideal of K, and $I_K=\prod \mathfrak{p}^{v_\mathfrak{p}}$ its prime ideal factorization in K. Suppose that I_K is the norm of an ideal I_L of L, then for all prime ideals $\mathfrak{p}$ of K there exists a prime ideal $\mathfrak{P}$ of L above $\mathfrak{p}$ whose residual index $f_{\mathfrak{P}/\mathfrak{p}}$ divides $v_\mathfrak{p}$. In other terms, any integral ideal which is a norm is the norm of an integral ideal.*

Proof. It is enough to observe that in any partition $d=\sum e_i f_i$ the *gcd* of all the f_i is always one of the f_i. □

Theorem 5.13. *Let L/K be an extension (not necessarily Galois) of degree 3, 4 or 6 and S_0 satisfying $\mathcal{N}_{L/K}(\mathbb{U}_{L,S_0})=\mathcal{N}_{L/K}(L^*)\cap\mathbb{U}_{K,S_0}$. If S_0 also generates the group $\mathrm{Cl}_\mathcal{N}(L/K)$, then for all $S\supset S_0$*

$$\mathcal{N}_{L/K}(\mathbb{Z}_{L,S})=\mathcal{N}_{L/K}(L)\cap\mathbb{Z}_{K,S}.$$

Proof. The inclusion $\mathcal{N}_{L/K}(\mathbb{Z}_{L,S})\subset\mathcal{N}_{L/K}(L^*)\cap\mathbb{Z}_{K,S}$ is trivial. For the reverse inclusion, let $a=\mathcal{N}_{L/K}(x)\in\mathbb{Z}_{K,S}$. Lemma 5.12 asserts the existence of an S-integral ideal I with norm $a\mathbb{Z}_{K,S_0}$. Since the group $\mathrm{Cl}_{\mathcal{N},S_0}(L)$ is trivial, we have $x^{-1}I=x_0\mathbb{Z}_{L,S_0}$. But the norm of x_0 is an S_0-unit, hence is also the norm of an S_0-unit y. We have the relations

$$a=\mathcal{N}_{L/K}(x)=\mathcal{N}_{L/K}(xx_0y^{-1}).$$

Since xx_0 is an S-integer and y is an S_0-unit, the result is proved. □

Remarks. 1. Note that the condition of this theorem is really on the group $\mathrm{Cl}_\mathcal{N}(L/K)$ and not on $\mathrm{Cl}_i(L/K)$ as for the other results.

2. When the degree is different from 3, 4 or 6, then Lemma 5.12 is not always true and neither is Theorem 5.13. In degree 5 we can consider the following example.

Example. $L/K=\mathbb{Q}(x)/\mathbb{Q}$ with $x^5+3x-2=0$. The number 7 is a norm because

$$\mathcal{N}_{L/K}((90x^4+8x^3+34x^2+24x+281)/7)=7.$$

The prime 7 splits into two prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ with residual index 3 and 2. If 7 is the norm of an integer z, then z has valuation v_1 and v_2 at $\mathfrak{P}_1$ and $\mathfrak{P}_2$, with the relation $3v_1+2v_2=1$, which implies that v_1 or v_2 is negative, and hence that z cannot be an integer. We can also remark that there are infinitely many primes with this property, and this shows that there is no finite set S satisfying Theorem 5.13.

There exist a great deal of extensions of degree different from 3, 4 or 6, which satisfy Lemma 5.12. This is certainly the case for all Galois extensions, but also for all extensions of type D_p (dihedral group of order $2p$ with p an odd prime). It would be interesting to give a characterization of such extensions in terms of the groups $G = \mathrm{Gal}(\mathfrak{L}/K)$ and $H = \mathrm{Gal}(\mathfrak{L}/L)$.

6. Norm equations: The algorithm

The algorithms we now describe were implemented in the PARI package for number theory, which already contains a large quantity of algorithms that we can use. For example we assume that the fields K and L are completely known, in the sense that we know their discriminants, integral basis, class groups, fundamental units, and the corresponding discrete logarithms (for a description of these algorithms see [4]).

For a proof of the algorithms of this section, see [13].

6.1. **Algorithms for S-units.** We give here the algorithm that computes a system of fundamental S-units (modulo the units of K) together with the group $\mathrm{Cl}_S(K)$.

Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$, $d_1, \dots, d_r$ be the elementary divisors of the group $\mathrm{Cl}(K)$, and $\mathfrak{g}_1, \dots, \mathfrak{g}_r$ the corresponding generators. We use the notation $(A|B)$ for the concatenation of the two matrices A and B. If V is a vector with k entries and U a $k \times l$ matrix, $W = V^U$ is the vector with l entries defined by $W_j = \prod_i V_i^{U_{i,j}}$. Note that $(V^A)^B = V^{AB}$.

Algorithm 6.1. (Computation of $\mathrm{Cl}_S(K)$ and of a fundamental system of generators for $\mathbb{U}_{K,S}/\mathbb{U}_K$)

1. *Let*
$$M = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \end{pmatrix}$$
and $V = (\beta_1, \dots, \beta_r)$ *such that* $\mathfrak{g}_i^{d_i} = \beta_i \mathbb{Z}_K$, *with* $\beta_i \in K^*$.
2. *Let* $M' = -(e_{i,j})$ *and* $V' = (\alpha_1, \dots \alpha_s)$ *such that* $e_{i,j} \in \mathbb{Z}$, $\alpha_j \in K^*$ *and*
$$\mathfrak{p}_j = \left(\prod_i \mathfrak{g}_i^{e_{i,j}} \right) \alpha_j.$$
3. *Compute a unimodular matrix* $U = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ *such that* $(M|M')U = (0|H)$ *is in HNF (Hermite Normal Form).*
4. *Compute* $(W|W') = (V|V')^U$.

Results.
$$\mathrm{Cl}_S(K) = \prod_i (\mathbb{Z}/H_{i,i}\mathbb{Z})\mathfrak{g}_i,$$
and W *is a fundamental system of generators for* $\mathbb{U}_{K,S}/\mathbb{U}_K$.

Remarks. 1. If we really want the elementary divisors of $\mathrm{Cl}_S(K)$, we have to take the SNF (Smith Normal Form) of H, and not only its HNF. This amounts to left multiplication by an invertible matrix, which corresponds to a change of basis on the $\mathfrak{g}_i$.

2. The matrix C of step 3 contains the valuations of the fundamental S-units at the $\mathfrak{p}_i$ of S. Its determinant is not zero. This matrix is only defined up to

the multiplication on the right by some unimodular matrix. Hence, we can choose the system of fundamental units with additional properties. For example, we can obtain integral S-units if we take the HNF of C. We can obtain "small" S-units if we LLL-reduce C. In this case, small means with small valuations on the prime ideals. Note that the multiplication on the left of C by a permutation matrix is equivalent to a change of order of the $\mathfrak{p}_i$ in S.

Corollary 6.2. *There exists a system of fundamental S-units which is formed by integral elements of K.*

If we keep the matrix C of Algorithm 6.1, it is easy to express any S-unit as a product of the fundamental S-units. It is also simple to solve the "principal ideal problem" in $\mathrm{Cl}_S(K)$ if we keep the matrices H and D, and the vectors W and W'.

We have the two following algorithms.

Algorithm 6.3. (Discrete logarithm in $\mathbb{U}_{K,S}/\mathbb{U}_K$)
Input: $u \in \mathbb{U}_{K,S}$.
1. *Compute* $F = (F_i)$ *such that* $u\mathbb{Z}_K = \prod \mathfrak{p}_i^{F_i}$.
2. $Z = C^{-1}F$ *has integral coefficients.*
Result: We have $u = \prod W_i^{Z_i} \cdot u'$ *where* $u' \in \mathbb{U}_K$.

Algorithm 6.4. (Principal ideal algorithm in $\mathrm{Cl}_S(K)$)
Input: I *ideal of* K.
1. *Compute* $F = (F_i)$ *and* α *such that* $I = \prod \mathfrak{g}_i^{F_i} \cdot \alpha$ *(this is the principal ideal algorithm in* $\mathrm{Cl}(K)$*).*
2. *Reduce* F *modulo* H*:* $F' = F - HZ$.

Result: We have

$$I = \left(\prod \mathfrak{g}_i^{F'_i}\right)\left(\prod \mathfrak{p}_i^{(-DZ)_i}\right)\left(\prod W_i^{Z_i} \cdot \alpha\right).$$

6.2. **How to compute relative class groups.** We will not give a direct method to compute these two relative class groups, because it is far beyond our task. For the relative quadratic case, H. Cohen, F. Diaz y Diaz and M. Olivier in [5] give an explicit algorithm for this, which can be extended to the general relative case. It is preferable to use this relative algorithm when possible.

What we indicate here is the use of the definitions. Indeed $\mathrm{Cl}_i(L/K)$ is a quotient of $\mathrm{Cl}(L)$, and [6] explains how to compute it from the knowledge of $\mathrm{Cl}(L)$, $\mathrm{Cl}(K)$, and the map i. The same paper explains how to compute $\mathrm{Cl}_{\mathcal{N}}(L/K)$ as the kernel of the norm map from $\mathrm{Cl}(L)$ to $\mathrm{Cl}(K)$.

6.3. **General norms.** The previous sections gave conditions on S which ensure that all S-units that are norms are norms of S-units. The general strategy of the algorithm that finds a solution of our equation $\mathcal{N}_{L/K}(x) = a$ is to say that a is an S-unit for a suitable set S. The remaining part of the algorithm consists of "discrete logarithms" in the S-unit group, and linear algebra over $\mathbb{Z}$.

The algorithm can be briefly described as follows.

Algorithm 6.5. (Find a solution to the equation $\mathcal{N}_{L/K}(x) = a$ in L)
Input: K, L *and* $a \in K^*$.
1. *Determine the set* S *using Algorithm 6.8.*
2. *Find an* S*-unit* x *such that* $\mathcal{N}_{L/K}(x) = a$ *using Algorithm 6.9.*

Result: If step 2 gives some x, then it is a solution; otherwise the equation has no solution in L.

In the following subsections we decribe this in more detail. Note that if we want integral solutions (or S-integral solutions), then we can use Algorithm 6.10 directly.

6.4. **Determine the sets S_0 and S.** If we want to find an integral solution to the equation $\mathcal{N}_{L/K}(x) = a$ where a is an integer of K, then any prime ideal that divides a solution x also divides a, and hence for the set S it is enough to consider all primes dividing a; that is, we can take $S_0 = \emptyset$. If we want a rational solution, we have to add to the set of primes above a, a set S_0 of exceptional primes satisfying Theorem 1.1, that is $S = S_0 \cup \{\mathfrak{p} \mid a\}$. Such an S_0 is described in the previous subsections.

We note that this set S_0 only depends on the relative extension L/K and not at all on the value of a in the equation $\mathcal{N}_{L/K}(x) = a$. It can be computed only once if we need to solve several norm equations in the same extension. For this reason it is preferable to write separate algorithms.

Algorithm 6.6. (Compute the set S_0 for Galois extensions L/K)

1. *Compute the relative class group* $\mathrm{Cl}_i(L/K)$, *and let* $\mathfrak{g}_i$ *be generators of the* $[L : K]$*-part of this group.*
2. *Compute all prime factors of the ideals* $\mathcal{N}_{L/K}(\mathfrak{g}_i)$.

Algorithm 6.7. (Compute the set S_0 for non-Galois extensions L/K)

1. *Determine the field* $\mathfrak{L}$ *and let* $\mathfrak{h}_i$ *be generators of the* $[L : K]$*-part of* $\mathrm{Cl}_i(\mathfrak{L}/K)$.
2. *Determine* $G = \mathrm{Gal}(\mathfrak{L}/K)$, $H = \mathrm{Gal}(\mathfrak{L}/L)$ *and all cyclic subgroups* D *of* G *of order* p^a *with* $p \mid ([L : K], [\mathfrak{L} : L])$ *and* $D \cap H \neq \{1\}$.
3. *Compute the relative class groups* $\mathrm{Cl}_i(\mathfrak{L}^D/K)$, *and let* $\mathfrak{g}_i$ *be generators of the* p*-part of these groups.*
4. *Compute all prime factors* $\mathfrak{p}_j$ *of the ideals in* K *under* $\mathfrak{h}_i$ *or* $\mathfrak{g}_i$.

Algorithm 6.8. (Compute the set S for the equation $\mathcal{N}_{L/K}(x) = a$)

1. *Determine the set* S_0 *using Algorithm 6.6 or 6.7.*
2. *Factor* a *into prime ideals* $\mathfrak{p}_i$ *of* K, *and set* $S = S_0 \cup \{\mathfrak{p}_i \mid a\}$.

Remark. Both Algorithms 6.6 and 6.7 can be simplified if we are able to find generators $\mathfrak{g}_i$ and $\mathfrak{h}_i$, which are prime ideals, and this is in theory always possible.

6.5. **Looking for solutions as S-units.** In this paragraph, we give an algorithm which solves the norm equation $\mathcal{N}_{L/K}(x) = a$ when a is an S-unit, and when we require the solution x to be also an S-unit for a given S. As soon as we have written x and a as a product of S-units, the problem reduces to a linear system. The algorithm is as follows.

Algorithm 6.9. (Find a solution to $\mathcal{N}_{L/K}(x) = a$ in $\mathbb{U}_{L,S}$)

1. *Using Algorithm 6.1 compute a fundamental system* $\{s_0, \ldots, s_n\}$ *of* S*-units of* K, *and* $\{\sigma_0, \ldots, \sigma_m\}$ *of* L, *where* s_0 *and* σ_0 *are the torsion units of order* w_K *and* w_L, *with* $w_K \mid w_L$.
2. *Using Algorithm 6.3, compute* a_i *and* $b_{i,j}$ *such that*

$$a = \prod s_i^{a_i} \text{ and } \mathcal{N}_{L/K}(\sigma_j) = \prod s_i^{b_{i,j}}.$$

3. *Solve the linear system*

$$\text{for all } i > 0,\ \sum_{j>0} b_{i,j}x_j = a_i,$$

$$\sum_{j\geqslant 0} b_{0,j}x_j \equiv a_0 \mod w_K.$$

Result: The equation $\mathcal{N}_{L/K}(x) = a$ has a solution with x an S-unit if and only if the linear system above has a solution in $\mathbb{Z}$. A solution is given by

$$\mathcal{N}_{L/K}(\prod \sigma_j^{x_j}) = a.$$

Remark. In step 2, a_0 is only defined mod w_K. Since the norm of a torsion unit is again a torsion unit, we have $b_{i,0} = 0$ for all $i > 0$. In step 3 the linear congruence $b_1x_1 + \cdots + b_nx_n \equiv a_0 \mod w_K$ with n variables is equivalent to the linear equation over $\mathbb{Z}$ with $n+1$ variables $b_1x_1 + \cdots + b_nx_n + w_Kx_0 = 0$.

6.6. **Looking for S-integral solutions.** Suppose now that we want to solve $\mathcal{N}_{L/K}(x) = a$ where a is an S-integer, and that we also want x to be S-integral for a given S. The algorithm uses the fact that the prime factors of x are above the prime factors of a, except perhaps some prime ideals in S.

If we write x and a as products of prime ideals, the equation $\mathcal{N}_{L/K}(x\mathbb{Z}_{L,S}) = a\mathbb{Z}_{K,S}$ reduces to a linear system (step 2 of Algorithm 6.10). The fact that $x\mathbb{Z}_{L,S}$ is a principal ideal gives a new linear system which must be solved simultaneously with the first one (step 2 of Algorithm 6.10). The integrality of the desired solution x implies that all the solutions of the system must be nonnegative. The number of such solutions is finite (step 3 of Algorithm 6.10). For each solution of this system we deduce an equality of the form $\mathcal{N}_{L/K}(b) = a \cdot u$, where u is an S-unit, and b an S-integer. It remains only to write the S-unit u as the norm of an S-unit to obtain a solution of our problem (step 4 of Algorithm 6.10).

The algorithm is the following.

Algorithm 6.10. (Find a solution to $\mathcal{N}_{L/K}(x) = a$ in $\mathbb{Z}_{L,S}$)

1. *Factorization: Compute the prime ideals $\mathfrak{p}_i$ (not in S) and the integers a_i such that $a\mathbb{Z}_{K,S} = \prod \mathfrak{p}_i^{a_i}$. Compute also the prime ideals $\mathfrak{P}_{i,j}$ of L and the integers $e_{i,j}$ and $f_{i,j}$ such that*

$$\mathfrak{p}_i = \prod \mathfrak{P}_{i,j}^{e_{i,j}} \text{ and } \mathcal{N}_{L/K}(\mathfrak{P}_{i,j}) = \mathfrak{p}_i^{f_{i,j}}.$$

2. *Compute $m_{i,j,k}$: Using Algorithm 6.1, compute a system of generators $\{g_k\}$ of the class group $\mathrm{Cl}_S(L)$, and d_k the corresponding orders. Using Algorithm 6.4, compute the components $m_{i,j,k}$ of the ideals $\mathfrak{P}_{i,j}$ on the generators g_k.*
3. *Solve a linear system: Find all the tuples of integers $(b_{i,j})$ satisfying the conditions*

$$\text{for all } i,\ \sum_j f_{i,j}b_{i,j} = a_i,$$

$$\text{for all } k,\ \sum_{i,j} m_{i,j,k}b_{i,j} \equiv 0 \mod d_k,$$

$$0 \leqslant b_{i,j} \leqslant a_i.$$

4. *Kill the spurious S-units: For each tuple $(b_{i,j})$ find an algebraic S-integer b of L such that $b\mathbb{Z}_{L,S} = \prod \mathfrak{P}_{i,j}^{b_{i,j}}$, and let u be the S-unit such that $\mathcal{N}_{L/K}(b) = a \cdot u$. Using Algorithm 6.9, try to find an S-unit v such that $u = \mathcal{N}_{L/K}(v)$.*

Result: If step 3 or step 4 has no solution, then the equation has no solution in S-integers. Otherwise the S-integer bv^{-1} is a solution.

Remark. It is easy to adapt this algorithm to obtain all the solutions up to S-units. If we are only interested in the equation $\mathcal{N}_{L/K}(x) = a \cdot u$, then it is also possible to adapt the algorithm.

References

1. H.J. Bartels: *Über Normen algebraischer Zahlen*, Math. Ann., **251** (1980) 191-212. MR **81k:**12010
2. K. Brown: *Cohomology of groups*, Graduate Texts in Math., Vol. 87, Springer-Verlag (1982). MR **83k:**20002
3. C. Chevalley: *Sur la théorie du corps de classe dans les corps finis et les corps locaux*, J. Fac. Sci Tokyo, **2** (1933) 365-475.
4. H. Cohen: *A course in computational algebraic number theory*, Graduate Texts in Math., Vol. 138, Springer-Verlag (1993). MR **94i:**11105
5. H. Cohen, F. Diaz y Diaz, M. Olivier: *Computation of relative quadratic class groups*, ANTS III, Springer LN in Computer Science, 1423 (J. Buhler Ed. 1998), p 433-440. MR **2000j:**11165
6. H. Cohen, F. Diaz y Diaz, M. Olivier: *Algorithms for finite abelian groups*, submitted to J. Symb. Comp.
7. C. Fieker : *Ueber Relative Normgleichungen in Algebraischen Zahlkörpern*, Dissertation, Technische Univertität Berlin (1997);
8. C. Fieker, A. Jurk, M. Pohst: *On solving relative norm equations in algebraic number fields*, Math. Comp., **66** (1997) 399-410. MR **97c:**11118
9. U. Fincke, M. Pohst: *A procedure for determining algebraic integers of given norm*, Proceedings EUROCAL 83, Springer LN in Computer Science, **162** (1983) 194-202. MR **86k:**11078
10. D. Garbanati: *An algorithm for finding an algebraic number whose norm is a given rational number*, J. Reine Angew. Math., **316** (1980) 1-13. MR **81k:**12004
11. J.-P. Serre: *Corps Locaux*, Hermann, 2ème éd. (1968). MR **50:**7096
12. C.L. Siegel: *Normen algebraischer Zahlen*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. II **1973**, 197-215. MR **49:**7237
13. D. Simon: *Équations dans les Corps de Nombres et Discriminants Minimaux*, thèse, Université de Bordeaux I (1998).

Université Bordeaux I, Laboratoire A2X, 351 Cours de la Libération, 33405 Talence, France

E-mail address: desimon@math.u-bordeaux.fr