# Computing class groups by induction with generalised norm relations

Fabrice Etienne

# Computing class groups by induction with generalised norm relations

Fabrice Etienne

**Abstract**

We introduce a generalisation of norm relations in the group algebra $\mathbb{Q}[G]$, where $G$ is a finite group. We give some properties of these relations, and use them to obtain relations between the $S$-unit groups of different subfields of the same Galois extension of $\mathbb{Q}$, of Galois group $G$. Then we deduce an algorithm to compute the class groups of some number fields by reducing the problem to fields of lower degree. We compute the class groups of some large number fields.

# Introduction

The problem of computing the class group of number fields is a central problem in number theory, with applications for example in cryptography or in class field theory. Let $K$ be a number field. The most commonly used method to compute the class group or the $S$-units groups of $K$ is Buchmann's algorithm [5]. Its complexity grows quickly with the degree $n$: if we denote by $D(K)$ the discriminant of $K$, the time complexity of this algorithm for fixed $n$ is in $\mathcal{O}(e^{a\sqrt{\ln|D(K)|\ln\ln|D(K)|}})$ where $a$ is a constant, and the implicit constant of the $\mathcal{O}$ depends on $n$ exponentially; note in addition that the discriminant grows at least exponentially with $n$. So it would be beneficial to have an inductive method to reduce these problems to similar ones in number fields of smaller degree and discriminant.

Such inductive methods have already been proposed. Suppose $K/F$ is a Galois extension of number fields, of Galois group $G$. By studying relations between the subgroups of $G$ arising from character theory, we can find corresponding relations between the arithmetic invariants of the intermediate fields. For a subgroup $H < G$, denote by $\mathrm{Ind}_{G/H}(1_H)$ the permutation character of $G$ induced from the trivial representation of $H$. A Brauer relation [4] is a relation of the form

$$\sum_{H<G} a_H \,\mathrm{Ind}_{G/H}(1_H) = 0$$

with $a_H \in \mathbb{Z}$. Brauer proved that when such a relation exists, there is a corresponding relation between arithmetic invariants of the fields $K^H$.

In [2], Biasse, Fieker, Hofmann and Page studied another type of relation called norm relation. Given a subgroup $H < G$, we define its norm element to be the formal sum $N_H = \sum_{h \in H} h$ in $\mathbb{Z}[G]$. If $R$ is a commutative ring, $\mathcal{H}$ a set of subgroups of $G$, a *norm relation* over $R$ with respect to $\mathcal{H}$ is an equality in $R[G]$ of the form

$$1 = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$$

with $a_i, b_i \in R[G]$ and $H_i < G$. In their paper, they derive from such a relation an inductive algorithm to compute the class group or the groups of $S$-units of $K$ by reducing the problem to a similar problem on the subfields $K^H$.

Our goal is to generalize the notion of norm relation in order to be able to use the same kind of method to compute the class group of some number fields $K$ even without a Galois extension $K/F$. If $K$ is a number field, let us denote by $\tilde{K}$ its Galois closure, and let $G$ be its Galois group (i.e. the Galois group of the extension $\tilde{K}/\mathbb{Q}$). Let $H$ be the subgroup of $G$ such that $K = \tilde{K}^H$. Let $R$ be a commutative ring, and $J_1, \cdots, J_l$ some subgroups of $G$. A *generalised norm relation* over $R$ with respect to $H$ and the $J_i$ is an equality in $R[G]$ of the form

$$N_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$$

with $a_i, b_i \in R[G]$. Classical norm relation are a special case of generalised norm relation where $H$ is the trivial group. Given $K$ and subfields $K_i$ of $\tilde{K}$, we say that $K$ admits a generalised norm relation with respect to the $K_i$ if $G$ admits one over $\mathbb{Q}$ with respect to $H$ and $\{J_i\}$, where the $J_i$ are such that $K_i = \tilde{K}^{J_i}$ for all $i$. We impose the condition that the $K_i$ are subfields of the Galois closure $\tilde{K}$, but we prove in theorem 2.11 this causes no loss in generality. The main result of this article is the following:

**Theorem A.** *There exists a polynomial time algorithm that, on input*

- *a number field $K$,*
- *a set $S$ of prime numbers,*
- *subfields $K_i$ of the Galois closure $\tilde{K}$,*
- *for each $i$, a basis of the $S$-unit group of $K_i$,*

*if $K$ admits a generalised norm relation with respect to the $K_i$, outputs a basis of the $S$-unit group of $K$.*

We will describe such an algorithm (algorithm 4.3), as well as another algorithm that is not provably polynomial time, but is often faster than the first one in practice (algorithm 4.6) Using an implementation of such an algorithm in Pari/GP, we compute the class group of some number fields significantly faster than with other methods, including the method using classical norm relations from [2]. In particular, in example 6.2, we compute the class group of a field of degree 105 and discriminant $2^{126} \cdot 29^{90} \cdot 67^{42} \simeq 1.7 \cdot 10^{246}$ in about 5 days (CPU time), whereas without our method, we could not compute it in over 5 months.

One problem we encounter is that there is no known polynomial time algorithm that, given a number field $K$ defined by an irreducible polynomial over $\mathbb{Q}$, computes its its Galois group $G$. We will provide a way to determine whether relations exists without actually having to compute $G$ or $\tilde{K}$. In order to do that, we will need some properties of Hecke algebras [13] and compositums. We will prove that a compositum $\mathcal{C}$ of two number field $K$ and $L$ naturally induces a morphism from $K^\times$ to $L^\times$. This map will be denoted $x \mapsto \mathcal{C} \cdot x$, and is described by the following theorem (see theorem 1.18).

**Theorem B.** *Let $K, L$ be two number fields, let $x$ be an element of $K^\times$ and $\mathcal{C} = (C, \iota_K, \iota_L)$ a compositum of $K$ and $L$. Then $\mathcal{C} \cdot x = N_{C/L}(\iota_K(x))$, where $N_{C/L}$ is the norm of the extension $C/L$.*

We will sometimes refer to this function as the action of the compositum $\mathcal{C}$ on $K^\times$. A similar result also gives a morphism of additive groups $K \to L$ given by the action of the compositum $\mathcal{C}$. We will prove the following characterisation (see theorem 2.20).

**Theorem C.** *Let $K, L_1, \cdots, L_\ell$ be number fields. Let $\alpha$ and $\beta_1, \cdots, \beta_l$ be such that $K = \mathbb{Q}(\alpha)$ and $L_i = \mathbb{Q}(\beta_i)$ for all $i$. Then $K$ admits a generalised norm relation with respect to $L_1, \cdots, L_\ell$, if and only there is a relation of the form*

$$\alpha = \sum_{i=1}^{\ell} \sum_{C \in Compo(K, L_i)} a_{i,C} C \cdot \beta_i$$

*where the coefficients $a_{i,C}$ are in $\mathbb{Q}$.*

To prove theorem A, we will also need some properties of Mackey functors [3]. In particular proposition 3.5, will be useful to find a relation between the $S$-units of the number fields involved in a generalised norm relation. We will prove a bound (theorem 2.15) that is crucial to prove that our algorithm is indeed polynomial.

We will also compare the method to compute class groups using generalised norm relation with the method described in [2] that only uses classical norm relations. We will provide an algorithm to find examples where the method using generalised norm relation is more efficient (algorithm 5.4).

With a systematic research on every group of cardinal up to 700, it appears that we can find many examples where generalised norm relations are useful. We think it is an interesting question to classify norm relation (classical ones as well as generalised ones). We do not have an algorithm that takes a number field and determines whether or not it admits a generalised norm relation in polynomial time, without having to compute the Galois group or the Galois closure. Finding such an algorithm is also an interesting open question.

The article is organised as follows: in section 1, we discuss properties of Hecke algebras and compositum, then in section 2 we recall the definition of classical norm relations, define the generalisation, and prove some properties. In section 3, we recall some properties of Mackey functors that will be useful later to prove the complexity of our algorithms. In section 4, we provide algorithms to check whether given fields admit a generalised norm relation, and to compute the class group and the group of $S$-units of number fields. Then in section 5, we compare these new methods with the methods in [2]. Finally, we give examples in section 6.

**Notations and conventions** When $R$ is a ring and $M$, $N$ are left $R$-modules, we will denote $\mathrm{Hom}_R(M,N)$ the group of $R$-module homomorphisms from $M$ to $N$. In a finite field extension $K/F$, we will denote by $N_{K/F}(x)$ the norm of $x \in K$.

**Acknowledgements** I would like to thank A. Page, who suggested to me to generalise the notion of norm relation, and was here to provide help and advice at every step of the conception of this article. Many thanks also to B. Allombert for his advice regarding the implementation in Pari/GP of the algorithms in section 4, and for his help to compute the $S$-units of some large auxiliary fields.
This research was funded by the University of Bordeaux. It was also supported by the CIAO ANR (ANR-19-CE48-008) and the CHARM ANR (ANR-21-CE94-0003). It took place inside the CANARI team (Cryptographic Analysis and Arithmetic) of the Institute of Mathematics of Bordeaux (IMB).
Experiments presented in this paper were carried out using the PlaFRIM experimental testbed, supported by Inria, CNRS (LABRI and IMB), Université de Bordeaux, Bordeaux INP and Conseil Régional d'Aquitaine

(see https://www.plafrim.fr).

# 1 Hecke algebras and compositums

In this section, $K$ is a number field, $G$ is the Galois group of the Galois closure $\tilde{K}$ of $K$, $H$ and $J$ are subgroups of $G$, respectively fixing the subfields $K$ and $L$. Let $\alpha$ be an element of $\mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$ and $f$ be the minimal polynomial of $\alpha$ in $\mathbb{Q}[X]$. Let $\beta$ be such that $L = \mathbb{Q}(\beta)$ and let $f_L$ be its minimal polynomial.

Our goal in this section is to establish that the set of compositums of $K$ and $L$ acts on the set of fixed points by $H$ of any $G$-module, and to make this action explicit. The action will be described in theorem 1.18. In this section, $R$ denotes a commutative ring and $V$ an $R[G]$-module. To establish this theorem, we will first need some useful isomorphisms involving $R[G]$-modules. First let us write two lemmas, describing some well known isomorphisms. One can find the proofs in [13].

**Lemma 1.1.** *The map*

$$\Phi_1 \colon \mathrm{Hom}_{R[G]}(R[G/H], V) \to V^H, \phi \mapsto \phi(1 \cdot H)$$

*is an isomorphism of $R$-modules, and its inverse is*

$$\Phi_1^{-1} \colon V^H \to \mathrm{Hom}_{R[G]}(R[G/H], V), x \mapsto \begin{cases} \text{The unique morphism } \phi \text{ of} \\ R[G]\text{-modules in } V \text{ such that} \\ \phi(1 \cdot H) = x \end{cases}.$$

**Lemma 1.2.** *There is an isomorphism of $R$-modules*

$$\Phi_2 \colon R[H\backslash G/J] \to R[G/J]^H, \sum_{HgJ \in H\backslash G/J} \alpha_{HgJ} HgJ \mapsto \sum_{gJ \in G/J} \alpha_{HgJ} gJ.$$

*Its inverse is*

$$\Phi_2^{-1} \colon R[G/J]^H \to R[H\backslash G/J], \sum_{gJ \in G/J} \alpha_{gJ} gJ \mapsto \sum_{HgJ \in H\backslash G/J} \alpha_{gJ} HgJ.$$

**Proposition 1.3.** *There is an isomorphism of $R$-modules*

$$\Phi \colon R[H\backslash G/J] \to \mathrm{Hom}_{R[G]}(R[G/H], R[G/J])$$

$$\sum_{HgJ \in H\backslash G/J} \alpha_{HgJ} HgJ \mapsto \begin{cases} \phi \text{ such that} \\ \phi(1 \cdot H) = \sum_{g \in G/J} \alpha_{HgJ} gJ \end{cases}.$$

*Its inverse is*

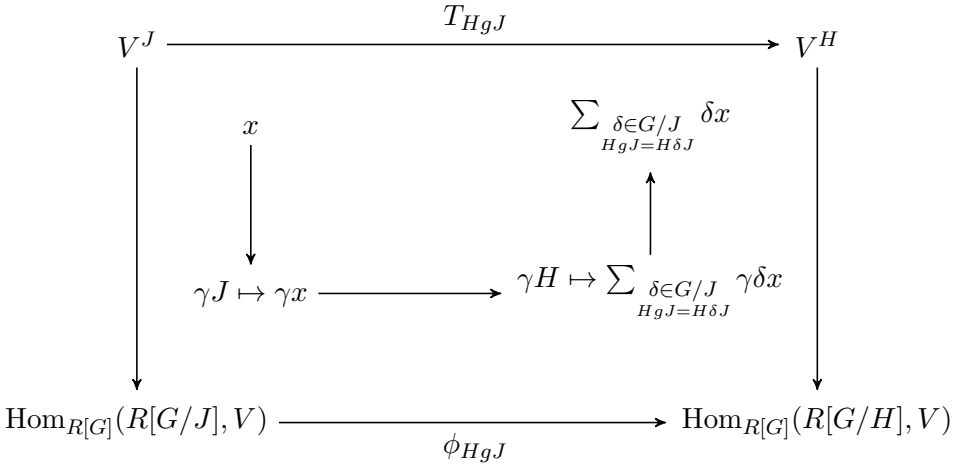
$$\Phi^{-1}\colon \mathrm{Hom}_{R[G]}(R[G/H], R[G/J]) \mapsto R[H\backslash G/J]$$

$$\phi \mapsto \begin{cases} \sum_{HgJ \in H\backslash G/J} \alpha_{gJ} H\delta J \\ \textit{where } \phi(1\cdot H) = \sum_{g\in G/J} \alpha_{gJ} gJ \end{cases} .$$

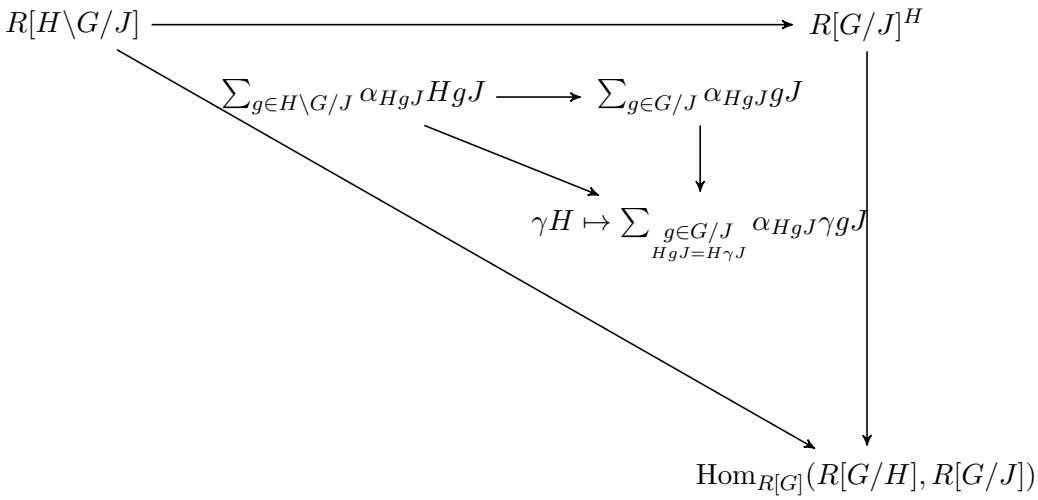
*Proof.* We can then obtain the isomorphism $\Phi$ simply by composing $\Phi_1$ and $\Phi_2$ from the two previous lemmas.

□

**Fact 1.4.** By considering both the isomorphism $\Phi$ in proposition 1.3 and the isomorphism $\Phi_1$ in lemma 1.1, we deduce that given any $R[G]$-module $V$, for every element $HgJ$ of $R[H\backslash G/J]$ we get a morphism $T_{HgJ}$ of $R$-modules from $V^J$ to $V^H$ given by the following diagram:




Where the expression of $\phi_{HgJ}$ is obtained via the following diagram:




**Remark 1.5.** This last proposition gives a natural action of $R[H\backslash G/J]$ that goes from $R[G/H]$ into $R[G/J]$. With the next proposition, we will see that this can also be seen as an action from the set $\mathrm{Hom}(K, \mathbb{C})$ of complex embeddings of $K$ into the set of complex embeddings of $L$.

**Remark 1.6.** The Galois group $G$ acts on the set $\mathrm{Hom}(K, \mathbb{C})$ by $g \cdot \sigma = \sigma \circ g$.

Recall that $\alpha$ is an element of $\mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$, and $f$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$. Let $\sigma \in \mathrm{Hom}(K, \mathbb{C})$ and $g \in G$. The embedding $\sigma$ sends $\alpha$ to a complex root of $f$. Then $g \cdot \sigma$ is the element of $\mathrm{Hom}(K, \mathbb{C})$ that sends $\alpha$ to $g \cdot \sigma(\alpha)$.

**Proposition 1.7.** *We note $E = \mathrm{Hom}(K, \mathbb{C})$ the set of embeddings of $K$ in $\mathbb{C}$, and by $\sigma_g$ the embedding that maps $\alpha$ to $g \cdot \alpha$ for all $g \in G$.*

*There is an isomorphism*

$$\Phi \colon G/H \to E, gH \mapsto \sigma_g.$$

*Its inverse is*

$$\Phi^{-1} \colon S \to G/H, \tau_g \alpha \mapsto gH.$$

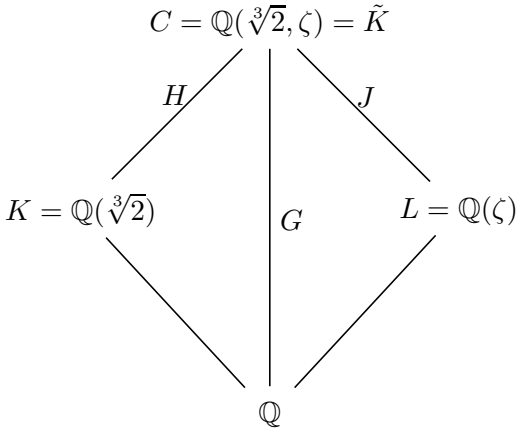
*It is independent from the choice of $g$.*

*Proof.* Let $g_1, g_2 \in G$ such that $g_1 H = g_2 H$, and let $h \in H$ such that $g_2 = g_1 h$. Then, $\sigma_{g_2}$ maps $\alpha$ to $g_1 \cdot (h \cdot \alpha) = g_1 \cdot \alpha$. So $\sigma_{g_2} = \sigma_{g_1}$. □

Now from these actions, we will deduce an action of compositums. First let us recall the following definition.

**Definition 1.8.** Let $K$ and $L$ be number fields. A *compositum* of $K$ and $L$ is a triple $(C, \iota_K, \iota_L)$ where $C/\mathbb{Q}$ is a number field, $\iota_K \colon K \to C$ and $\iota_L \colon L \to C$ are morphisms of $\mathbb{Q}$-algebras, and where $C$ is generated by $\iota_K(K)$ and $\iota_L(L)$ as a ring.

**Example 1.9.** Consider the following diagram, with $\zeta := e^{\frac{2i\pi}{3}}$.




Let $\iota_K \colon K \to C$ be the inclusion, and $\iota_L \colon L \to C$ also the inclusion. It is clear that $C$ is generated by $\iota_K(K)$ and $\iota_L(L)$, so $C$ is a compositum of $K$ and $L$.

Here, we have $C = \tilde{K}$. We will see that up to isomorphism, every compositum of $K$ and $L \subset \tilde{K}$ is included in $\tilde{K}$.

Note that if we take $\iota_{K,2} \colon K \to C$ the inclusion and $\iota_{L,2} \colon K \to C_2, \zeta \mapsto \overline{\zeta}$, then $(C, \iota_{K,2}, \iota_{L,2})$ is another compositum of $K$ and $L$.

**Definition 1.10.** A *morphism of compositums* between two compositums $(C, \iota_K, \iota_L)$ and $(C', \iota'_K, \iota'_L)$ is a field morphism $f \colon C \to C'$, such that $\iota'_K = f \circ \iota_K$ and $\iota'_L = f \circ \iota_L$.

The two following lemma give some properties of compositums.

**Lemma 1.11.** *Up to isomorphism, there is a finite number of compositums of $K$ and $L$, we denote by* $\mathrm{Compos}(K, L)$ *a set of representatives. There is a bijection between this set and the set of quotients of $K \otimes_{\mathbb{Q}} L$. For $f \colon K \otimes_{\mathbb{Q}} L \to C$ surjective, the associated compositum is $(C, \iota_K, \iota_L)$ and $\iota_K = f \circ (\mathrm{id}_K \otimes 1)$, $\iota_L = f \circ (\mathrm{id}_L \otimes 1)$. Every compositum of $K$ and $L$ is isomorphic to a compositum whose underlying field is contained in $\tilde{K}$.*

*Proof.* The second statement is a direct application of the universal property of the tensor product of algebras.

Since $K \otimes_{\mathbb{Q}} L$ is of finite dimension over $\mathbb{Q}$, the set $\mathrm{Compos}(K, L)$ is finite.

Now let us prove the last statement. Denote $K = \mathbb{Q}[X]/p(X)$, with $p(X) \in \mathbb{Q}[X]$ irreducible. Denote $p(X) = \prod_i p_i(X)$ the decomposition of $p(X)$ into a product of irreducible polynomials in $L[X]$. Then $K \otimes_{\mathbb{Q}} L = \prod_i L[X]/(p_i(X))$. What's more, the polynomials $p_i$ are split in $L[X]$, so they are also split in $\tilde{K}[X]$. So for every $i$, we have $L[X]/(p_i(X)) \subset \tilde{K}$, since $\tilde{K}$ contains $L$ and a splitting field of the $p_i$. Hence the conclusion. □

**Lemma 1.12.** *The map*

$$\Psi\colon \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K}) \to \mathrm{Compos}(K, L), \phi \mapsto (\phi(K).L, \phi, \mathrm{incl}_{L/\tilde{K}})$$

*induces a bijection from* $J\backslash \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K})$ *to* $\mathrm{Compos}(K, L)/\sim$. *(Recall that* $J$ *is defined to be the subgroup of* $G$ *that fixes* $L$*)*

*Proof.* Let $\phi \in \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K})$. The composition by $g \in J$ induces an isomorphism $(\phi(K).L, \phi, \mathrm{incl}_{L/\tilde{K}}) \to (g.\phi(K).L, g.\phi, g.\,\mathrm{incl}_{L/\tilde{K}})$. Since $g \in J$, $g$ fixes $L$, so $g.\,\mathrm{incl}_{L/\tilde{K}} = \mathrm{incl}_{L/\tilde{K}}$. So the isomorphism induced by $g$ is of the form $\Psi(\phi) \to \Psi(g \cdot \phi)$. Let us check that the map induced by $\Psi$ is injective. Let $\phi, \phi' \in \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K})$ and let $f\colon \phi(K) \cdot L \to \phi'(K) \cdot L$ an isomorphism of compositums. Then $f \circ \mathrm{incl}_{\tilde{K}/L} = \mathrm{incl}_{\tilde{K}/L}$ and $f$ is the identity over $L$, so $f$ can be extended as an isomorphism $g \in J$. Since $f$ is a morphism of compositums, $g\phi = \phi'$, hence $\phi \sim \phi'$.

Let us check it is surjective. By lemma 1.11, every compositum in $\mathrm{Compos}(K, L)$ is isomorphic to a compositum where $\iota_L = \mathrm{incl}_{L/\tilde{K}}$. Let $\iota_K\colon K \to \tilde{K}$ be an embedding, then we can always pick $\phi = \iota_K$. □

**Proposition 1.13.** *There is a bijection*

$$\Phi\colon J\backslash G/H \to \mathrm{Compos}(K, L), JgH \mapsto (gK \cdot L, l \mapsto gl \cdot 1_L, \mathrm{incl}_{L/\tilde{K}}).$$

*Its inverse is*

$$\Phi^{-1}\colon \mathrm{Compos}(K, L) \to J\backslash G/H, (C, \iota_K, \iota_L) \mapsto \left\{ \begin{array}{l} JgH \\ \textit{with } g \textit{ such that} \\ \iota_K(\alpha) = g \cdot \alpha \in \tilde{K} \end{array} \right. .$$

*Proof.* The proposition derives from the two lemmas 1.11 and 1.12. □

Thus, using the previous isomorphisms, we obtain an action of $\mathrm{Compos}(K, L)$ on various $R$-modules.

**Proposition 1.14.** *The map*

$$\Phi\colon \mathrm{Compos}(K,L) \to \mathrm{Hom}_{R[G]}(R[G/J], R[G/H])$$

$$(C, \iota_K, \iota_L) \mapsto \begin{cases} \phi \text{ such that} \\ \phi(1 \cdot J) = \sum_{\substack{\gamma H \in G/H \\ J\gamma H = JgH}} \gamma H \\ \text{with } g \text{ such } g \cdot \alpha = \iota_K(\alpha) \end{cases}$$

*is injective.*

*Proof.* This is derived from the proposition 1.13, using the isomorphism of proposition 1.3. □

For all $\alpha'$ a root of $f$, we denote by $\sigma_{\alpha'}$ the embedding of $K$ in $\mathbb{C}$ that sends $\alpha$ to $\alpha'$. Similarly, denote $\tau_{\beta'}$ the embedding of $L$ in $\mathbb{C}$ that sends $\beta$ to $\beta'$.

**Proposition 1.15.** *The map*

$$\Phi\colon \mathrm{Compos}(K,L) \to \quad \mathrm{Hom}_{R[G]}(R[\mathrm{Hom}(L,\mathbb{C})]R[\mathrm{Hom}(K,\mathbb{C})]),$$
$$(C,\iota_K,\iota_L) \mapsto \quad \begin{cases} \phi \text{ such that} \\ \phi(\tau_\beta) = \sum_{\substack{\sigma\in\mathrm{Hom}(K,\mathbb{C}) \\ (C,\iota_K,\iota_L)\sim(C',\sigma,\tau_\beta)}} \sigma \end{cases}$$

*is injective.*

*Proof.* This is derived from proposition 1.14, using the isomorphism of proposition 1.7. □

**Remark 1.16.** Let $(C,\iota_K,\iota_L)$ be a compositum of $K$ and $L$, and let $\phi$ the corresponding element of $\mathrm{Hom}_{R[G]}(R[\mathrm{Hom}(L,\mathbb{C})],R[\mathrm{Hom}(K,\mathbb{C})])$. We can obtain a nicer way to write $\phi(\tau_\beta)$:

$$\phi(\tau_\beta) = \sum_{\substack{\sigma\in\mathrm{Hom}(K,\mathbb{C}) \\ (C,\iota_K,\iota_L)\sim(C',\sigma,\tau_\beta)}} \sigma = \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \sum_{E_\sigma} \sigma$$

where $E_\sigma = \{f \in \mathrm{Hom}(C,\mathbb{C}) | \sigma = f\circ\iota_K \text{ and } \tau_\beta = f\circ\iota_L\}$.

And from that form we can deduce a general expression for $\phi(\tau)$ for every complex embedding $\tau$.

**Proposition 1.17.** *Let $(C,\iota_K,\iota_L)$ be a compositum of $K$ and $L$, and let $\phi$ the corresponding element of* $\mathrm{Hom}_{R[G]}(R[\mathrm{Hom}(L,\mathbb{C})],R[\mathrm{Hom}(K,\mathbb{C})])$. *For all $\tau \in \mathrm{Hom}(L,\mathbb{C})$,*

$$\phi(\tau) = \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \sum_{E_\sigma} \sigma$$

*where $E_\sigma = \{f \in \mathrm{Hom}(C,\mathbb{C}) | \sigma = f\circ\iota_K$ and $\tau_{1_G} = f\circ\iota_L\}$.*

*Proof.* Let $\tau = \gamma\cdot\tau_\beta$ with $\gamma \in G$. (We can always write $\tau$ in that form, because $g$ acts transitively on the elements of $\mathrm{Hom}(L,\mathbb{C})$).

Then,

$$\phi(\tau) = \gamma\cdot\phi(\tau_\beta) = \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \sum_{E_\sigma} \gamma\cdot\sigma$$
$$= \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \sum_{E_{\gamma\cdot\sigma}} \gamma\cdot\sigma$$

because $\gamma\colon \mathrm{Hom}(K,\mathbb{C}) \to \mathrm{Hom}(K,\mathbb{C})$ is a bijection.

$$= \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \sum_{E_\sigma} \sigma$$

because $\gamma\colon \mathrm{Hom}(C,\mathbb{C}) \to \mathrm{Hom}(C,\mathbb{C})$ is a bijection.

□

Similarly, for every $R[G]$-module $V$, a compositum $C$ of $K$ and $L$ induces a map from $V^H$ to $V^J$. (The proof is similar to that of proposition 1.17.)

In the rest of the article, if $x$ is an element of $V^H$, we will denote by $C \cdot x$ the image of $x$ by this map.

**Theorem 1.18.** *Let $x$ be an element of $K^\times$ and let $(C, \iota_K, \iota_L)$ be a compositum of $K$ and $L$. Then $C \cdot x = N_{C/L}(\iota_K(x))$.*

*Proof.* The bijection described in proposition 1.13 allows to identify the compositum $(C, \iota_K, \iota_L)$ with an element $J\backslash g/H$ of $J\backslash G/H$.

First, let us prove that the subfield of $\tilde{K}$ fixed by $H \cap (gJg^{-1}) < G$ is $C$. The subfield fixed by $gJg^{-1}$ is $g(L) = \iota_L(L)$. Denote by $\tilde{C}$ the field fixed by $H \cap (gJg^{-1})$. All elements of $K$ and $\iota_L(L)$ are in $\tilde{C}$ so $C \subset \tilde{C}$. What's more, if we denote by $N$ the subgroup of $G$ fixing $C$, then $N$ is included both in $H$ and in $gJg^{-1}$, so it is included in $H \cap gJg^{-1}$. We get $\tilde{C} \subset C$, so we indeed have $\tilde{K}^{H \cap (gJg^{-1})} = C$.

Now, we know that $C \cdot x = \prod_{\delta \in HgJ/J} \delta x = \prod_{\substack{\delta \in G/J \\ HgJ = H\delta J}} \delta x$ We want to make the change of variables $\delta = hg$. For $h, h' \in H$, we have $hgJ = h'gJ$ if and only if there exists $j \in J$ such that $h = h'(gjg^{-1})$, that is to say if and only if $\overline{h} = \overline{h'}$ in $H/(H \cap (gJg^{-1}))$. This gives $\mathcal{C} \cdot x = \prod_{h \in H/(H \cap (gJg^{-1}))} hgx$. Finally, we obtain

$$\mathcal{C} \cdot x = N_{C/M}(\iota_L(x))$$

as claimed.

□

# 2 Classical and generalised norm relations

In this section we introduce generalised norm relations, which will be the main type of objects that we will study throughout this article. The notion of classical norm relation has been studied by Biasse, Fieker, Hofmann and Page in [2]. They use it to obtain inductive methods to compute the class group or the group of $S$-units of a Galois extension of number fields. The goal of this section is to generalise this notion in order to obtain a similar method applicable to more examples. We will define our generalisation of norm relations in definition 2.4, provide equivalent definitions in proposition 2.7, and prove theorem 2.20 which will be useful for the algorithms in section 4.

**Definition 2.1.** Let $G$ be a finite group and $H$ a subgroup of $G$. We call *norm element* of $H$ the element $N_H = \sum_{h \in H} h \in \mathbb{Z}[G]$.

**Definition 2.2.** Let $G$ be a finite group, $\mathcal{J}$ a set a subgroups of $G$ and $R$ a commutative ring. A *norm relation over $R$ with respect to $\mathcal{J}$* is an equality in $R[G]$ of the form

$$1 = \sum_{i=1}^{l} a_i N_{J_i} b_i$$

where $a_i, b_i \in R[G]$, $J_i \in \mathcal{J}$, and $J_i \neq 1$.

**Example 2.3.** The symmetric group $G = S_3$ admits a norm relation over $\mathbb{Q}$ with respect to $\mathcal{H} = \{\langle (1,2,3)\rangle, \langle (2,3)\rangle\}$.

**Definition 2.4.** Let $G$ be a finite group, $H$ a subgroup of $G$, $\mathcal{J}$ a set a subgroups of $G$ and $R$ a commutative ring. A *generalised norm relation over $R$ with respect to $H$ and $\mathcal{J}$* is an equality in $R[G]$ of the form

$$N_H = \sum_{i=1}^{l} a_i N_{J_i} b_i$$

where $a_i, b_i \in R[G]$, $J_i \in \mathcal{J}$, and $J_i \neq 1$.

**Remark 2.5.** Clearly, with the notations above, a classical norm relation is a generalised norm relation where $H$ is the trivial subgroup.

**Example 2.6.** The alternating group $A_4$ admits a norm relation over $\mathbb{Q}$ with respect to $\mathcal{H} = \{C_2 \times C_2, C_3\}$. It also admits a generalised norm relation with respect to $H = C_2$ and $\mathcal{J} = \{C_2 \times C_2, C_3\}$. Here, we see that the generalised norm relation comes from the regular norm relation.

**Proposition 2.7.** *Let $G$ be a finite group, $H$ a subgroup of $G$, $\mathcal{J} = \{J_1, \cdots, J_\ell\}$ a set of non trivial subgroups of $G$ and $R$ a commutative ring. Then the following assertions are equivalent:*

1. *There exists a surjective morphism of $\mathbb{Q}[G]$-modules*

$$\phi\colon \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]^{n_i} \to \mathbb{Q}[G/H]$$

   *where for all $i$, $n_i \in \mathbb{N}$.*

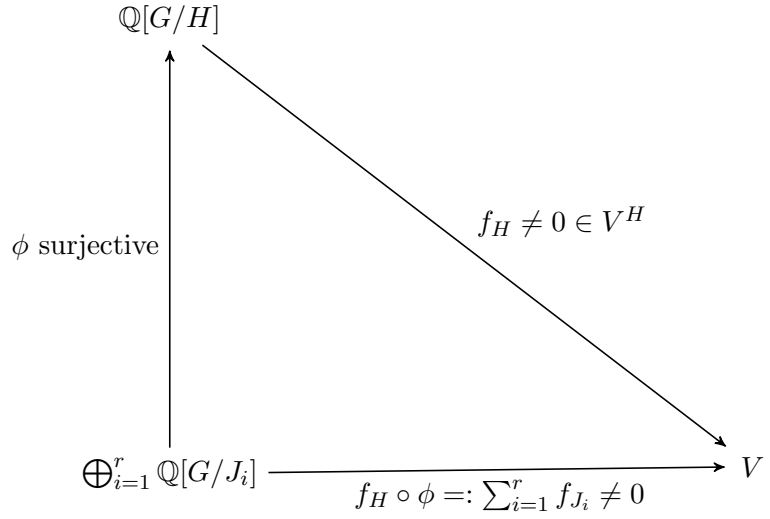
2. *If $e_1, \ldots, e_r$ are the central primitive idempotent elements of $\mathbb{Q}[G]$, then for all $1 \leq i \leq r$, if $e_i N_H \neq 0$, there exists $J \in \mathcal{J}$ such that $e_i N_J \neq 0$.*

3. *For all simple $\mathbb{Q}[G]$-module $V$, if $V^H \neq 0$, there exists $J \in \mathcal{J}$ such that $V^J \neq 0$.*

4. *For all simple $\overline{\mathbb{Q}}[G]$-module $V$, if $V^H \neq 0$, there exists $J \in \mathcal{J}$ such that $V^J \neq 0$.*
5. *For all simple $\mathbb{C}[G]$-module $V$, if $V^H \neq 0$, there exists $J \in \mathcal{J}$ such that $V^J \neq 0$.*
6. *The norm element $N_H$ is in the two sided ideal $\langle N_J : J \in \mathcal{J} \rangle_{\mathbb{Q}[G]}$.*
7. *The group $G$ admits a generalised norm relation over $\mathbb{Q}$ with respect to $H$ and $\mathcal{J}$.*

*Proof.*

- $1 \Rightarrow 3$. We know there is an isomorphism of $R$-modules between $V^H$ and $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/H], V)$. Likewise, for all $i$, $V^{J_i}$ is isomorphic to $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/J_i], V)$. Suppose 1, then we have the following diagram, where $f_H$ is an element of $V^H$ seen as an element of $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/H], V)$, and likewise, the $f_{J_i}$ are elements of $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/J_i], V)$.




  So $\sum_{i=1}^r f_{J_i}$ is non zero, so at least one of the $f_{J_i}$ is non zero, hence the conclusion.

- $2 \Leftrightarrow 3$. Let $V_i$ be the simple $\mathbb{Q}[G]$-module (unique up to isomorphism) such that $e_i V_i \neq 0$ then $\mathbb{Q}[G]/(1 - e_i)$ acts faithfully on $V_i$. So $e_i N_H = 0$ if and only if $N_H \cdot V_i = 0$, so if and only if $(\frac{1}{|H|} N_H) \cdot V_i = 0$ which is equivalent to $V_i^H = 0$.
- $3 \Rightarrow 1$. Suppose 3, then let $V = \mathbb{Q}[G/H]$. Then $V$ is a $\mathbb{Q}[G]$-module, and $V$ can decompose as $V = \bigoplus_k V_k$, where the $V_k$ are simple. For all $k$, let $f_k \colon V \to V_k$ the projection. It can be seen as an element of $V_k^H$ by 1.1. Then there exists a non zero

element of $V_k^{J_i}$ for some $i$, by lemma 3. So we have a nonzero morphism $\bigoplus_{i=1}^{r} \mathbb{Q}[G/J_i] \to V_k$ so it is surjective because $V_k$ is simple. Hence the conclusion by putting together all the $k$.

- $3 \Rightarrow 4$. Suppose 3, let $W$ be a simple $\overline{\mathbb{Q}}[G]$-module. $W$ is isomorphic to a submodule of $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$, with $V$ a simple $\mathbb{Q}[G]$-module. Then we have $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq \bigoplus_{j=1}^{k} W_j$, where the $W_j$ are simple $\overline{\mathbb{Q}}[G]$-modules. So $W$ is isomorphic to one of the $W_j$. What's more, the $W_j$ are pairwise Galois conjugate, so $\dim_{\overline{\mathbb{Q}}} W_j^H = \dim_{\overline{\mathbb{Q}}} W_1^H$ pour tout $j$. So if $W^H$ is non zero, $V^H$ is also non zero. So, by 3, there exists $J \in \mathcal{J}$ such that $V^J$ is non zero. Hence $W^J \neq 0$.
- $4 \Rightarrow 5$. The simple $\mathbb{C}[G]$-modules are exactly the $V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$, where $V$ is a simple $\overline{\mathbb{Q}}[G]$-module. The conclusion follows.
- $5 \Rightarrow 4$. Suppose 5, let $V$ a simple $\overline{\mathbb{Q}}[G]$-module. If $V^H \neq 0$, then $(V \times_{\overline{\mathbb{Q}}} \mathbb{C})^H \neq 0$. So, by 4., there exists $J \in \mathcal{J}$ such that $(V \otimes_{\overline{\mathbb{Q}}} \mathbb{C})^J \neq 0$. Hence $V^J \neq 0$.
- $4 \Rightarrow 3$. Suppose 4, let $V$ a simple $\mathbb{Q}[G]$-module such that $V^H \neq 0$. Consider $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq \bigoplus_{j=1}^{k} W_j$. We know that $W_j^H \neq 0$ for all $j$. So there exists $J \in \mathcal{J}$ such that $W_1^J \neq 0$. So $V^J \neq 0$.
- $3 \Leftrightarrow 6$. Let $I$ be a two-sided ideal of $\mathbb{Q}[G]$. We have $I = \sum_{i=1}^{r} e_i I$. What's more, there is an isomorphic projection of $e_i I$ in a two sided ideal of the algebra $\mathbb{Q}[G]/(1 - e_i)$, which is simple. So $e_i I$ is either zero, or $e_i \mathbb{Q}[G]$. By applying this result to $I = \langle N_J : J \in \mathcal{J} \rangle_{\mathbb{Q}[G]}$, we find the equivalence.
- $6 \Leftrightarrow 7$. This equivalence comes directly from the definition of a generalised norm relation.

□

**Remark 2.8.** It is relatively easy to apply these equivalent definition of generalised norm relations to implement algorithms that take a finite group $G$ and look for $H$ and $\mathcal{J} = \{J_1, \cdots, J_l\}$ such that there is a generalised norm relation.

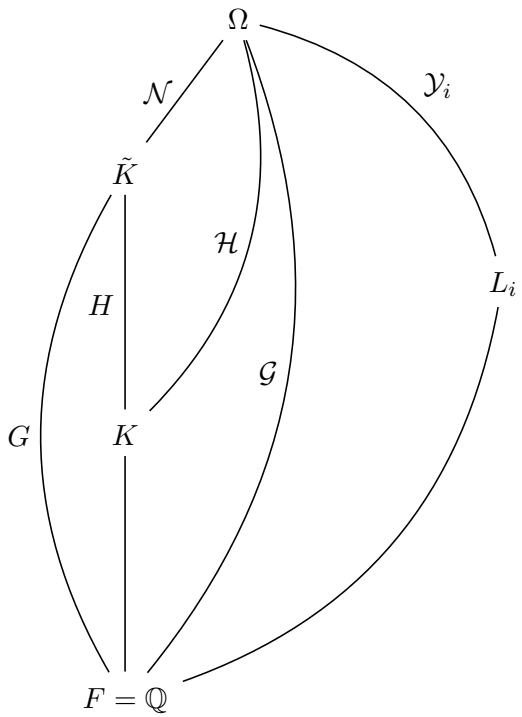
**Definition 2.9.** Let $K, L_1, \cdots, L_\ell$ be number fields. Let $\Omega$ a Galois extension of $\mathbb{Q}$ containing $K$ and all the $L_i$, and let $\mathcal{G}$ its Galois group. We denote by $\mathcal{H}$ the subgroup of $\mathcal{G}$ fixing $K$, and by $\mathcal{Y}_i$ the ones fixing the $L_i$ respectively. Then we say there is a generalised norm relation between $K$ and the $L_i$ if there is a generalised norm relation over $\mathbb{Q}$ with respect to $\mathcal{H}$ and the $\mathcal{Y}_i$.

Now we want to use such a generalised norm relation to find an algorithm that can compute the class group of $K$ given the class class

groups of all the $L_i$. So we will only be interested in generalised norm relations where the degrees of the $L_i$ are lower than the degree of $K$. In other words, the order of all the $\mathcal{Y}_i$ has to be higher than the order of $\mathcal{H}$.

**Example 2.10.** There is a generalised norm relation between the number field $K$ defined by $f(x) = x^6 - 6x^4 + 9x^2 + 23$ and the number fields $L_1, L_2$ respectively defined by $g_1(x) = x^3 - 9x - 27$ and $g_2(x) = x^2 + 207$. Indeed, $K/\mathbb{Q}$ is a Galois extension of Galois group $G = S_3$, and $L_1, L_2$ are the subgroups fixed respectively by $\langle(2,3)\rangle$ and $\langle(1,2,3)\rangle$

**Theorem 2.11.** *Suppose there is a generalised norm relation between a number field $K$ and some $L_i$ that are not necessarily contained in the Galois closure $\tilde{K}$ of $K$. Denote by $\Omega$ a Galois extension of $\mathbb{Q}$ of Galois group $\mathcal{G}$ containing $\tilde{K}$ and all the $L_i$ as in the diagram below.*




*Then there is also a generalized norm relation between $K$ and some $M_i$ that are contained in $\tilde{K}$.*

*Proof.* We have $\mathcal{N} = \bigcap_{g\in\mathcal{G}} g\mathcal{H}g^{-1}$. What's more, $\mathcal{N}$ is normal in $\mathcal{G}$ and $G = \mathcal{G}/\mathcal{N}$ and $H = \mathcal{H}/\mathcal{N}$. Since there is a generalised norm relation between the $L_i$ and $K$, there exist a relation of the form

$N_{\mathcal{H}} = \sum_i a_i N_{\mathcal{Y}_i} b_i \in \mathbb{Q}[G]$. Consider the projection

$$\pi\colon \mathbb{Q}[\mathcal{G}] \to \mathbb{Q}[\mathcal{G}/\mathcal{N}] = \mathbb{Q}[G], \sum_i \lambda_i g_i \mapsto \sum_i \lambda_i \overline{g}_i.$$

This map $\pi$ is a surjective morphism of $\mathbb{Q}$-algebras. Composing the relation by $\pi$ we get

$$\pi(N_{\mathcal{H}}) = |\mathcal{N}| N_H = \sum_i \pi(a_i)\pi(N_{\mathcal{Y}_i})\pi(b_i)$$

and

$$\pi(N_{\mathcal{Y}_i}) = |\mathcal{N} \cap \mathcal{Y}_i| N_{\mathcal{Y}_i/(\mathcal{N}\cap\mathcal{Y}_i)}.$$

So there is a generalised norm relation between $K$ and the $M_i = \Omega^{\mathcal{Y}_i/\mathcal{N}} \in \tilde{K}$. Note that if for some $i$, $\mathcal{Y}_i \subset \mathcal{N}$, then $\tilde{K} \subset L_i$, then the relation was not interesting.

□

The following definition and properties, up to theorem 2.15 aim to provide a bound on a quantity that we call optimal coefficient, which will be useful for the proof of the complexity of algorithm 4.3 in section 4.

**Definition 2.12.** Let $H, J_1, \cdots, J_\ell$ be non trivial subgroups of $G$, and let $\mathcal{J} = \{J_1, \cdots, J_\ell\}$. If there is a norm relation over $\mathbb{Q}$ with respect to $H$ and $\mathcal{J}$, we define the *optimal coefficient* $c(\mathcal{J}, H)$ to be the smallest positive integer such that there exists an injective morphism of $\mathbb{Z}[G]$-module $\psi\colon \mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]^{n_i}$ with $n_i \in \mathbb{N}$ for all $i$, and a surjective morphism of $\mathbb{Z}[G]$-module $\phi\colon \bigoplus_i \mathbb{Z}[G/J_i]^{n_i} \to \mathbb{Z}[G/H]$ such that $\phi \circ \psi = c(\mathcal{J}, H) \cdot \mathrm{id}$.

**Proposition 2.13.** *With the notations of the definition above, $c(\mathcal{J}, H)$ is well defined.*

*Proof.* Since there is a norm relation over $\mathbb{Q}$ with respect to $H$ and $\mathcal{J}$, there is a surjective $\mathbb{Q}[G]$-module morphism $\bigoplus_i \mathbb{Q}[G/J_i]^{n_i} \to \mathbb{Q}[G/H]$.

Since $\mathbb{Q}[G]$ is a semi-simple algebra, this means we can write the decomposition in simple modules up to isomorphism $\mathbb{Q}[G/H] = \bigoplus_{j=1}^{n} W_j$ and $\bigoplus_i \mathbb{Q}[G/J_i]^{n_i} = \bigoplus_{j=1}^{n} W_j \oplus \bigoplus_{k=1}^{m} V_k$. Consider $\Phi$ the natural injection $\mathbb{Q}[G/H] \to \bigoplus_i \mathbb{Q}[G/J_i]^{n_i}$, let $c$ be the LCM of the denominators of all coefficients of all the $\Phi(gH)$ for $gH \in G/H$. Then $c \cdot \phi$ induces an injective morphism of $\mathbb{Z}[G]$-module $\mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]^{n_i}$. With the same reasoning, we can construct a surjective morphism of $\mathbb{Z}[G]$-modules $\psi\colon \bigoplus_i \mathbb{Z}[G/J_i]^{n_i} \to \mathbb{Z}[G/H]$. And then $\phi \circ \psi$ is a multiple of $\mathrm{id}_{\mathbb{Z}[G/H]}$. Hence the conclusion.

□

We now prove that the optimal coefficient is also smallest for the divisibility relation.

**Proposition 2.14.** *If $c$ is a positive integer such that there exists $\phi$ and $\psi$ as in definition 2.12 such that $\phi \circ \psi = c \cdot \mathrm{id}_{\mathbb{Z}[G/H]}$, then $c(\mathcal{J}, H) \mid c$.*

*Proof.* Consider the group

$$E = \langle t_2 \circ t_1 | n_i \in \mathbb{N}^\times \forall i, t_1 \in A_{1,n_i}, t_2 \in A_{2,n_i} \rangle_{\mathbb{Z}} \cap \mathbb{Z}\,\mathrm{id}_{\mathbb{Z}[G/H]},$$

where

$$A_{1,n_i} = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \bigoplus_i \mathbb{Z}[G/J_i]^{n_i})$$

and

$$A_{2,n_i} = \mathrm{Hom}_{\mathbb{Z}[G]}(\bigoplus_i \mathbb{Z}[G/J_i]^{n_i}, \mathbb{Z}[G/H]).$$

Then $E$ is a subgroup of $\mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H])$ contained in $\mathbb{Z}\,\mathrm{id}$, so $E$ is of the form $a\mathbb{Z}\,\mathrm{id}$ with $a \in \mathbb{N}$. And by definition, $a = c(\mathcal{J}, H)$. By construction, $c \cdot \mathrm{id}$ is in $E$, hence $c(\mathcal{J}, H) \mid c$.

□

**Theorem 2.15.** *With the notations of Definition 2.12, we have $c(\mathcal{J}, H) \mid |G|^2$.*

*Proof.* Let $p$ be a prime number. Let $\mathcal{O}$ be a maximal order of $\mathbb{Q}_p[G]$ containing $\mathbb{Z}_p[G]$. By [6, 27.1, proposition] we have $\mathcal{O} \subset \frac{1}{|G|}\mathbb{Z}_p[G]$.

Consider $M_H = \mathcal{O} \cdot \mathbb{Z}_p[G/H] \subset \mathbb{Q}_p[G/H]$. Then $M_H$ is an $\mathcal{O}$-module, and we have $\mathbb{Z}_p[G/H] \subset M_H \subset \frac{1}{|G|}\mathbb{Z}_p[G]$. Similarly, for all $i$, we write $M_{J_i} = \mathcal{O} \cdot \mathbb{Z}_p[G/J_i]$.

Let $e_1, \cdots, e_r$ be central primitive idempotents of $\mathbb{Q}_p[G]$ contained in $\mathcal{O}$, which exist since $\mathcal{O}$ is a maximal order. For all $1 \leq i \leq r$, there is a isomorphism $\alpha\colon \mathcal{O}/(1-e_i) \to M_n(\Lambda)$, where $\Lambda = \Lambda_i$ is the maximal order of a division algebra $D$ over $\mathbb{Q}_p$. And $\alpha$ can be extended to $\mathcal{O}$ with the projection $\mathcal{O} \to \mathcal{O}/(1-e_i)$. (see [12]).

We have $M_n(\Lambda) \subset M_n(D)$ and $M_n(D)$ acts on $D^n$, which is the only simple $M_n(D)$-module up to isomorphism.

So $M_H \otimes \mathbb{Q}_p \cong D^{na}$ with $a \in \mathbb{N}^\times$, since $M_H \otimes \mathbb{Q}_p$ is a is a $M_n(D)$-module. Similarly, $\bigoplus_i M_{J_i}^{n_i} \otimes \mathbb{Q}_p \cong D^{nb}$, and thus $M_H \cong \Lambda^{na}$ and $\bigoplus_i M_{J_i}^{n_i} \cong \Lambda^{nb}$.

What's more, we have an surjective morphism of $\mathbb{Q}_p[G]$-modules from $\bigoplus_i M_{J_i}^{n_i} \otimes \mathbb{Q}_p = \bigoplus_i \mathbb{Q}_p[G/J_i]$ to $M_H \otimes \mathbb{Q}_p = \mathbb{Q}_p[G/H]$. Which means that $a \leq b$.

Therefore, we have a natural injection of $\mathcal{O}$-modules $\tilde{\psi}\colon M_H \to \bigoplus_i M_{J_i}^{n_i}$, and a natural surjection $\tilde{\phi}\colon \bigoplus_i M_{J_i}^{n_i} \to M_H$.

Let us denote $\psi = |G|\tilde{\psi}$ and $\phi = |G|\tilde{\phi}$. That way, $\psi$ induces an injective morphism $\mathbb{Z}_p[G/H] \to \bigoplus_i \mathbb{Z}_p[G/J_i]^{n_i}$ and $\phi$ a surjective morphism $\bigoplus_i \mathbb{Z}_p[G/J_i]^{n_i} \to \mathbb{Z}_p[G/H]$. And we have $\phi \circ \psi = |G|^2 \,\mathrm{id}$.

By doing the same reasoning over all $e_i$ and by putting together every prime $p$, we obtain the claimed result.

□

**Remark 2.16.** In the algorithms of section 4, the optimal coefficient $c(\mathcal{J}, H)$ plays a role analogous to that of the optimal denominator $d(\mathcal{H})$ in the case of classical norm relations (see [2, definition 2.15]). Thanks to our new definition, we obtain a $|G|^2$ bound instead of the $|G|^3$ bound in [2, theorem 2.20].

Using the isomorphisms in section 1, we want to find an equivalent definition of generalised norm relations that features only field theory and not group theory. This definition will be useful to design efficient algorithms that will not require the computation of Galois groups or Galois closures.

**Lemma 2.17.** *Let $V$ be a $R[G]$-module and $\phi\colon V \to R[G/H]$ a surjective morphism of $R[G]$-modules. There exists a preimage of $1H$ by $\phi$ that is in $V^H$.*

*Proof.* Since $\phi$ is surjective, there exists $v \in V$ such that $\phi(v) = 1H$. Now consider the element $v' = \frac{1}{|H|}\sum_{h\in H} h \cdot v$.

Then, clearly, $v' \in V^H$, and $\phi(v') = \frac{1}{|H|}\sum_{h\in H} \phi(h\cdot v) = \frac{1}{|H|}\sum_{h\in H} h\cdot \phi(v) = \frac{1}{|H|}\sum_{h\in H} h \cdot 1H = 1H$.

□

**Proposition 2.18.** *We have a generalised norm relation, given by a surjection*

$$\phi\colon \bigoplus_i R[G/J_i] \to R[G/H],$$

*if and only if there is a relation of the form*

$$1H = \sum_i T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H} \sum_k \lambda_{i,k} g_{i,k} J_i,$$

*with $\sum_k \lambda_{i,k} g_{i,k} J_i$ in $(\bigoplus_i R[G/J_i])^H$.*

*Proof.* Suppose there exists $\phi\colon \bigoplus_i R[G/J_i] \to R[G/H]$ surjective. Let us considere $\bigoplus_i \sum_k \lambda_{i,k} g_{i,k} J_i$ a preimage of $1H$. By lemma 2.17, we can suppose $\bigoplus_i \sum_k \lambda_{i,k} g_{i,k} J_i$ is in $(\bigoplus_i R[G/J_i])^H$

Let us write $\phi = \bigoplus_i \phi_i$ with $\phi_i\colon \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$. Then we have

$$1H = \sum_i \phi_i(\sum_k \lambda_{i,k} g_{i,k} J_i).$$

Then, by writing $\phi_i = \sum_h \mu_h T_{J_i \delta_{i,h} H} = T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H}$, we can obtain

$$1H = \sum_i T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H} \sum_k \lambda_{i,k} g_{i,k} J_i$$

□

**Corollary 2.19.** *Let $S$ be set of non-zero prime ideals of $\mathcal{O}_K$. The map*

$$\Phi \colon \bigoplus_{i=1}^{\ell} \bigoplus_{C \in \mathrm{Compos}(K_i, K)} \mathcal{O}_{K_j,S}^{\times} \to \mathcal{O}_{K,S}^{\times}$$

$$\bigoplus_{i=1}^{\ell} \bigoplus_{C \in \mathrm{Compos}(K_i, K)} \mathfrak{a}_{i,C} \mapsto \sum_{i=1}^{\ell} \sum_{C \in \mathrm{Compos}(K_i, K)} C \cdot \mathfrak{a}_{i,C}$$

*has an image of maximal rank.*

**Theorem 2.20.** *If $L_1, \cdots, L_\ell$ are number fields, and $\beta_1, \cdots, \beta_\ell$ such that $L_i = \mathbb{Q}(\beta_i)$, then $K$ admits a* generalised norm relation with respect to $L_1, \cdots, L_\ell$, *if and only if there is a relation of the form*

$$\alpha = \sum_{i=1}^{\ell} \sum_{C \in Compo(K, L_i)} a_{i,C} C \cdot \beta_i$$

*where the coefficients $a_{i,C}$ are in $\mathbb{Q}$.*

*Proof.* This theorem is a rephrasing of proposition 2.18 using the isomorphisms of part 1. □

# 3 Mackey Functors

In this section, we will recall some properties of cohomological Mackey functors. They will be useful mainly to prove the correctness of some algorithms in section 4. The results in this section come from [3] and [13].

The main result in this section will be proposition 3.5, which we will later use to find a relation between the $S$-units of the number fields involved in a generalised norm relation.

First let us recall the definition of a Mackey functor, as in [3].

**Definition 3.1.** Let $G$ be a finite group and $R$ a commutative ring. A *$R$-Mackey functor* $M = (M, c, \mathrm{Res}, \mathrm{Ind})$ on $G$ is a quadruple consisting of

- a family of $R$-modules $M(H)$ where $H \leq G$,

- a family of homomorphisms of $R$-modules $c_{g,H}\colon M(H) \to M({}^gH)$, the *conjugation* maps, where $g \in G$, $H \leq G$ and ${}^gH = gHg^{-1}$,
- a family of homomorphisms of $R$-modules $\mathrm{Res}^H_J\colon M(H) \to M(J)$, the *restriction maps*, where $J \leq H \leq G$, and
- a family of homomorphisms of $R$-modules $\mathrm{Ind}^H_J\colon M(J) \to M(H)$, the *induction* maps, where $J \leq H \leq G$,

such that the following axioms are satified:

- (Triviality) $c_{h,H} = \mathrm{Res}^H_H = \mathrm{Ind}^H_H = \mathrm{id}_{M(H)}$ for all $H \leq G$ and $h \in H$.
- (Transitivity) $c_{g'g,H} = c_{g',{}^gH} \circ c_{g,H}$, $\mathrm{Res}^J_L \circ \mathrm{Res}^H_J = \mathrm{Res}^H_L$ and $\mathrm{Ind}^H_J \circ \mathrm{Ind}^J_L = \mathrm{Ind}^H_L$ for all $L \leq J \leq H \leq G$ and $g, g' \in G$.
- ($G$-equivariance) $c_{g,J} \circ \mathrm{Res}^H_J = \mathrm{Res}^{{}^gH}_{{}^gJ} \circ c_{g,H}$ and $c_{g,J} \circ \mathrm{Ind}^H_J = \mathrm{Ind}^{{}^gH}_{{}^gJ} \circ c_{g,J}$ for all $J \leq H \leq G$ and $g \in G$.
- (Mackey formula) For all $H \leq G$, $U, J \leq H$, one has

$$\mathrm{Res}^H_U \circ \mathrm{Ind}^H_J = \sum_{h \in U\backslash H/J} \mathrm{Ind}^U_{U\cap {}^hJ} \circ \mathrm{Res}^{{}^hJ}_{U\cap {}^hJ} \circ c_{h,J}$$

  where $h \in H$ runs through a set of representatives for the double cosets $U\backslash H/K$.

**Definition 3.2.** A $R$-Mackey functor $M$ on $G$ is called *cohomological* if the axiom

$$\mathrm{Ind}^H_J \circ \mathrm{Res}^H_J = [H : J]\,\mathrm{id}_{M(H)}, \text{ for all } J \leq H \leq G$$

holds.

**Theorem 3.3.** *Let $R$ be a commutative ring and $G$ a group. The association $H \mapsto R[G/H]$ forms a cohomological Mackey functor with the following operations:*

- $\mathrm{Ind}^H_K\colon R[G/K] \to R[G/H], gH \mapsto gK$
- $\mathrm{Res}^H_K\colon R[G/H] \to R[G/K], gH \mapsto \sum_{h\in H/K} ghK$
- $c_{g,H}\colon R[G/H] \to R[G/{}^gH], xH \mapsto xg^{-1}\ {}^gH$

*Proof.* See [13, example 4.1], with $D$ the trivial group. □

**Theorem 3.4.** *Let $M$ be a cohomological Mackey functor. If $H, K$ are subgroups of $G$ and $g$ an element of $G$, let us define the operator*

$$T_{HgK}\colon M(K) \to M(H), x \mapsto \mathrm{Ind}^H_{{}^gK\cap H} \circ \mathrm{Res}^{{}^gK}_{{}^gK\cap H} \circ c_{g,K}(x).$$

*Then, all operators of this form follow the rules of compositions of $R[H\backslash G/K]$ comming from the isomorphism of proposition 1.3.*

*Proof.* See [13, theorem 4.1]. □

**Proposition 3.5.** *Let $R$ be a ring, $G$ a group, $H < G$ a subgroup and $\{J_i\}$ a set of subgroups. If we have $\phi\colon \bigoplus_{i=1}^m R[G/J_i] \to R[G/H]$ a morphism of $R[G]$-modules and $\psi\colon R[G/H] \to \bigoplus_{i=1}^m R[G/J_i]$ a morphism of $R[G]$-modules, such that $\phi \circ \psi = d \cdot \mathrm{id}_{R[G/H]}$, then for every cohomological Mackey functor $M$, there exists $\phi_M\colon \bigoplus_{i=1}^m M(J_i) \to M(H)$ and $\psi_M\colon M(H) \to \bigoplus_{i=1}^m M(J_i)$ such that $\phi_M \circ \psi_M = d \cdot \mathrm{id}_{M(H)}$.*

*Proof.* See [3, corollary 1.4]. □

**Remark 3.6.** We can describe more precisely the form of $\phi_M$ and $\psi_M$. They are obtained by decomposing $\phi$ and $\psi$ into sums of morphisms respectively $R[G/J_i] \to R[G/H]$ and $R[G/H] \to R[G/J_i]$, expressing these morphisms as elements of $H\backslash G/J_i$ or $J_i\backslash G/H$ and then applying theorem 3.4.

**Remark 3.7.** This previous proposition, along with proposition 2.13, give a induction relation between $M(H)$ and the $M(J_i)$ for every cohomological Mackey functor $M$. We will use it in section 4 with $M(H) = \mathcal{O}^\times_{\tilde{K}^H,S}$ and $M(J_i) = \mathcal{O}^\times_{\tilde{K}^{J_i},S}$, but it could also be useful to compute other Mackey functors.

# 4 Algorithms

In this section, we will present algorithms to resolve some problems around the notion of generalised norm relation.

We will suppose the Galois group and the Galois closure of the fields we will use are not known a priori.

Note that if we know the Galois group of a field, it is easy to make an algorithm that determines all the generalised norm relation. We implemented such an algorithm and it has been useful to find examples of generalised norm relations. There is also a method to calculate the group of $S$ units of $\tilde{K}^H$ using the $S$-units of the $\tilde{K}^{J_i}$ if $\tilde{K}$ is a Galois extension of $\mathbb{Q}$ of Galois group $G$ and $G$ admits a generalised norm relation over $\mathbb{Q}$ with respect to $H$ and $\mathcal{J} = \{J_1, \cdots, J_\ell\}$.

Here, we will describe algorithms relying only on field theory, and without having to compute any Galois group which we do not know how to compute in polynomial time.

The main algorithm in this section is algorithm 4.3, which computes a $\mathbb{Z}$-basis of the $S$-units of a number field $K$, given some fields $K_j$ such that $K$ admits a generalised norm relation with respect to the $K_j$. Its complexity is polynomial in the size of the input, including a $\mathbb{Z}$-basis of the $S$-units of the $K_j$ (see theorem 4.4).

**Algorithm 4.1.** input: A number field $K = \tilde{K}^H$ and a family $(K_i = \tilde{K}^{J_i})$ of number fields given by $f$, the minimal polynomial of $\alpha$ with $K = \mathbb{Q}(\alpha)$, and $f_i$ the minimal polynomials of the $\beta_i$, with $K_i = \mathbb{Q}(\beta_i)$.

output: A boolean indicating whether there is a generalised norm relation, and if so, a formula of the form

$$1H = \sum_i T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H} \sum_k \lambda_{i,k} g_{i,k} J_i$$

in $\mathbb{Z}[G/H]$

- For all $i$, list all compositums of $K$ and $K_i$.
  If $f_i = p_1 \cdots p_r \in K[X]$, Then, the compositums are the $K[X]/(p_j)$, with $\iota_K$ the inclusion, and $\iota_{L_i} : \beta_i \mapsto X$.
- For all $i$, and for all $\sigma \in \mathrm{Hom}(L_i, \mathbb{C})$ and for every compositum $\mathcal{C}$, compute $\mathcal{C} \cdot \sigma \in \mathbb{Q}[\mathrm{Hom}(K, \mathbb{C})]$.
- By linear algebra in $\mathbb{Q}[G/H] = \mathbb{Q}[\mathrm{Hom}(K, \mathbb{C})]$, find a linear combination of these element that amounts to $1H$ (if such a combination exists).

**Theorem 4.2.** *This algorithm is correct and its complexity is polynomial in the size of the input.*

*Proof.* The correctness of the algorithm follows from theorem 2.20.

For the complexity, we have to check that every step of the algorithm works in polynomial time.

- Listing all the compositums boils down to a problem of factorisation of polynomials in $K[X]$, which is polynomial thanks to the LLL algorithm (see [9]). The number of compositums to list is at most $\sum_{j=1}^{\ell} \deg(K_j)$.
- Given a complex embedding $\sigma$ of a field $K_j$, and a compositum $\mathcal{C}$ of $K$ and $K_j$, computing $\mathcal{C} \cdot \sigma$ is in $\mathcal{O}(\deg(K_j) \times \deg(K))$. And the number of times such a computation occurs is at most $\sum_j \deg(K_j) \times |\mathrm{Compos}(K, K_j)|$. What's more, the size of $\mathcal{C} \cdot \sigma$ is polynomial in the size of the input.

□

**Algorithm 4.3.** input: A number field $K$ and a set of number fields $\{K_j\}$, each given by an irreducible polynomial in $\mathbb{Q}[X]$ and such that $K$ admits a generalised norm relation with respect to the $K_j$, a set $S$ of prime numbers, and for each $j$ a $\mathbb{Z}$-basis $B_j$ of $\mathcal{O}^\times_{K_j,S}$.

output: A $\mathbb{Z}$-basis of $\mathcal{O}^\times_{K,S}$.

1. Compute $\pi_1, \cdots, \pi_k$ all the prime divisors of $(n!)^2$ where $n$ is the degree of $K$ (ie all the primes lesser than $n$). Let $r_i = v_p((n!)^2)$.
2. For all $j$, compute all the compositums of $K$ and $K_j$ (up to isomorphism).
3. Compute the set $B$ of images of every element of the $B_j$ by every compositum of $K$ and $K_j$.
4. Compute the subgroup $V \subset \mathcal{O}_{K,S}^{\times}$ generated by $B$.
5. For every $i$:
   - $V_i \leftarrow V$
   - $V_i \leftarrow \langle V_i, (\alpha_1)^{\frac{1}{p_i}}, \cdots, (\alpha_m)^{\frac{1}{p_i}} \rangle$ where $(\overline{\alpha_i})$ is a basis of $(V_i \cap (K^{\times})^{p_i})/V_i^{p_i}$. (See [2, corollary 4.13])
   - Reduce the basis of $V_i$ as in [10, lemma 7.1].
6. $V \leftarrow V_1 \cdots V_k$
7. Return a basis of $V$.

**Theorem 4.4.** *Assume the generalized Riemann Hypothesis (GRH). Then this algorithm is correct and its complexity is polynomial in the size of the input.*

*Proof.* First, let us prove the correctness. Let $G$ be the Galois group of $K$, let $H$ the subgroup fixing $K$ and for every $i$, let $J_i$ the subgroup fixing $K_i$. Since there is a generalised norm relation, we know that there exists an integer $c$, a surjective morphism of $\mathbb{Z}[G]$-module $\phi\colon \bigoplus_i \mathbb{Z}[G/J_i] \to \mathbb{Z}[G/H]$ and an injective morphism of $\mathbb{Z}[G]$-modules $\psi\colon \mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]$, such that $\phi \circ \psi = \mathrm{id}$ (by proposition 2.13).

Therefore, by proposition 3.5, for any cohomological Mackey functor $M$, there is a surjective morphism $\phi_M\colon \bigoplus_{i=1}^m M(J_i) \to M(H)$. Consider $M(H) = \mathcal{O}_{\tilde{K}^H,S}$ and $M(J_i) = \mathcal{O}_{\tilde{K}^{J_i},S}$. Since we know by remark 3.6 that $\phi_M$ can be expressed as a sum of elements of $J_i \backslash G/H$, and since, by proposition 1.13, these can be seen as elements of $\mathrm{Compos}(K_i, K)$, this proves the correctness.

Then let us prove the complexity. Let $\Sigma$ denote the total size of the input. To compute all the $\pi_i$ in step 1, we can use a sieve method, which is polynomial in $n$ where $n$ is the degree of $K$. Therefore, step 1 takes polynomial time.

As seen before, for every $j$, computing all the compositums of $K$ and $K_j$ takes polynomial time. What's more, the number and the size of the compositums obtained are also polynomial. So step 2 is also polynomial.

The size of the image of an element $x \in K_j$ by a compositum $\mathcal{C}$ is also polynomial, since the map induced by $\mathcal{C}$ is the composition of the injection $K_j \to C$ and the norm $C \to K$. So step 3 is polynomial.

For step 4 as well as step 7, one can deduce a basis from a generating set of the groups involved in polynomial time. The algorithms of [7] provide a basis of the relations between the generators, and the Hermite normal form [8] allows us to obtain a basis of the group in polynomial time.

The saturation in step 5 is performed as many times as the number of primes dividing $(n!)^2$, counted with multiplicity, according to theorem 2.15. That number is polynomial in $n$, since the number of different primes in the decomposition of $(n!)^2$ is at most $n$, and for every prime $p$, $v_p(n!) \leq \frac{\log(n!)}{\log(2)} = \mathcal{O}(n \log(n))$.

□

**Remark 4.5.** The paper [1] gives a polynomial method to approximate $\kappa_K$, the residue of the Dedekind zeta function $\zeta_K(s)$ at $s = 1$ of a number field $K$, from the discriminant $\Delta_K$ and the norm of prime ideals of $K$.

We now present an alternative to Algorithm 4.3, which is more efficient in practice but not provably polynomial-time.

**Algorithm 4.6.** input: A number field $K = \tilde{K}^H$ and a family $(K_i = \tilde{K}^{J_i})$ of number fields, such that $K$ admits a generalised norm relation with respect to $K_1, \cdots K_\ell$. We know $f$, the minimal polynomial of $\alpha$ with $K = \mathbb{Q}(\alpha)$, and $f_i$ the minimal polynomials of the $\beta_i$, with $L_i = \mathbb{Q}(\beta_i)$.

output: The structure of the class group of $K$

1. For every $K_j$, compute every compositums of $K$ and $K_j$.
2. Compute $HR_K = h_K \operatorname{Reg}_K$ using the approximation method in [1]. An approximation up to a factor 1.5 is enough.
3. Initialize $T$ a set of prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) = 1 \mod d$, where $d = \deg(K)^2$.

   *The primes in $T$ will be used to detect $d$-th powers.*
4. Initialize $S_\mathbb{Q}$ a set of prime numbers, and compute the set $S$ of prime ideals of $K$ above the primes in $S_\mathbb{Q}$.

   *We hope that $S$ will generate the class group.*
5. For all $K_j$, let $S_j$ be the set of prime ideals of $K_j$ above all primes $p$ in $S_\mathbb{Q}$, and compute a set $U_j$ of generators of the group of $S_j$ units of $K_j$.
6. For each $j$, for each $\mathfrak{p}$ in $S_j$, compute the vector $V_{j,\mathfrak{p}}$ of valuations of every element of $U_j$ at $\mathfrak{p}$.

7. Compute the matrix of a map $\Phi$, that sends all the ideals above all the primes in $S_j$ to their image by every compositum. Apply this matrix to every $V_{j,\mathfrak{p}}$, then concatenate all the vectors to obtain a matrix $M$.
8. Apply the action of every compositum to every generator of the $U_j$ then compute the discrete logarithms in $\mathbb{F}_{\mathfrak{p}}$ of for every $p$ in $T$. Concatenate all the vectors of discrete logarithms to obtain a matrix $N$.
9. Concatenate the matrix $M$ and $N$ and compute the kernel $R$ modulo $d$ of this matrix.

   *We hope to obtain a basis of the $d$-saturation of the images in $K$ of the $S_j$-units of the $K_j$ by the actions of every compositum.*
10. Compute the Smith normal form of the concatenation of $M$ and a basis of $R$.

    *If $T$ and $S$ are large enough, that should give us the structure of* $\mathrm{Cl}(K)$.
11. Compute the regulator of the group of units of $K$ obtained by the $d$-saturation of images of the units of the $K_j$ by the actions of every compositum. Multiply it with the class number to obtain a new $HR$ product, that we will denote by $H\tilde{R}_K$. If the approximation for $HR_K$ is up to a factor 1.5, then the regulator should be calculated with precision up to a factor $\frac{4}{3}$.
12. Check if the $HR$ product corresponds to the one in step 3. If not, increase the size of $T$ and $S_{\mathbb{Q}}$ and go back to step 5.

**Theorem 4.7.** *If this algorithm terminates, then it is correct.*

*Proof.* By the remark 3.7, we know the algorithm finds indeed all the $S$-units in $K$. Then, if the verification of the $HR$ product is correct, it means the $S$-units are enough to generate the class group. The crucial observation is that the approximation errors due to the choice of $T$ and $S$ cannot compensate. If $T$ is not large enough and the algorithm incorrectly assumes an element to be a $d$-th power, then $H\tilde{R}_K$ a divisor of its expected value. The same will happen if $S$ is not large enough to generate the class group. □

**Remark 4.8.** Suppose we have a number field $K = \tilde{K}^H$ and a family $(K_i = \tilde{K}^{J_i})$ of number fields, such that $K$ admits a generalised norm relation with respect to $K_1, \ldots, K_\ell$. If we want to compute the class group of $K$ using algorithm 4.6, we could expect the most expensive step to be the computation of the $S_j$ units in all the $K_j$, since it is the only step whose computation is not polynomial in the size of the input.

However, in practice, when we try to apply this method to reasonable size examples, the most expensive step is often the computation of the images of the ideals in the $S_j$ by the compositums.

# 5 Comparison with classical norm relations

In this section, we will discuss the relevance of studying generalised norm relation instead of classical norm relation. A generalised norm relation of a group $G$ with respect to $H < G$ and a set of subgroup $\mathcal{J}$ can come directly from a classical norm relation in $G$ (see fact 5.1) or in a quotient of $G$ (see proposition 5.2). But we will see that it is not always the case, and that in some examples, the methods in section 4 indeed allows to compute the class groups more efficiently than classical norm relations.

**Fact 5.1.** If there is a classical relation $1 = \sum_{i=1}^{l} a_i N_{J_i} b_i$ for some finite group $G$ and some set $\mathcal{J}$ of subgroups of $G$, then for any subgroup $H$, we can construct a generalised norm relation with respect to $H$ and $\mathcal{J}$, simply by multiplying both sides of the classical relation by $N_H$.

**Proposition 5.2.** *Let $G$ be a finite group, $H, J_1, \cdots, J_l$ subgroups of $G$. Let $N$ be a normal subgroup of $G$ contained in $H$. Denote by $\pi$ the projection from $G$ to $G/N$. Then $G$ admits a generalised norm relation with respect to $H$ and $J_1, \cdots, J_\ell$ if and only if $G/N$ admits a generalised norm relation with respect to $\pi(H)$ and $\pi(J_1), \cdots, \pi(J_\ell)$.*

*Proof.* Suppose $G$ admits a generalised norm relation over $\mathbb{Q}$ with respect to $H$ and $J_1, \cdots, J_\ell$, of the form $N_H = \sum_{i=1}^{l} a_i N_{J_i} b_i$.

Let $\Pi\colon \mathbb{Q}[G] \to \mathbb{Q}[G/N], \sum_i \lambda_i g_i \mapsto \sum_i \lambda_i \pi(g_i)$. Then $\Pi$ is a surjective morphism of $\mathbb{Q}[G]$-modules. And we have $\Pi(N_H) = |N| N_{H/N}$, and $\Pi(N_{Ji}) = |N \cap J_i| N_{J_i/(N\cap J_i)}$. Then, if we compose the relation by $\Pi$, we get a generalised norm relation of $G/N$ with respect to $\pi(H)$ and $\pi(J_1), \cdots, \pi(J_\ell)$.

Now suppose $G/N$ admits a generalised norm relation with respect to $\pi(H)$ and $\pi(J_1), \cdots, \pi(J_\ell)$. So there is a surjective morphism $\phi\colon \bigoplus_{i=1}^{l} \mathbb{Q}[\pi(G)/\pi(J_i)] \to \mathbb{Q}[\pi(G)/\pi(H)]$.

So $\phi \circ \Pi$ is a surjective morphism from $\bigoplus_{i=1}^{l} \mathbb{Q}[G/J_i]$ to $\mathbb{Q}[\pi(G)/\pi(H)]$. And since $N \subset H \subset G$, we have $\pi(G)/\pi(H) \simeq G/H$. Hence a surjective morphism from $\bigoplus_{i=1}^{l} \mathbb{Q}[G/J_i]$ to $\mathbb{Q}[G/H]$.

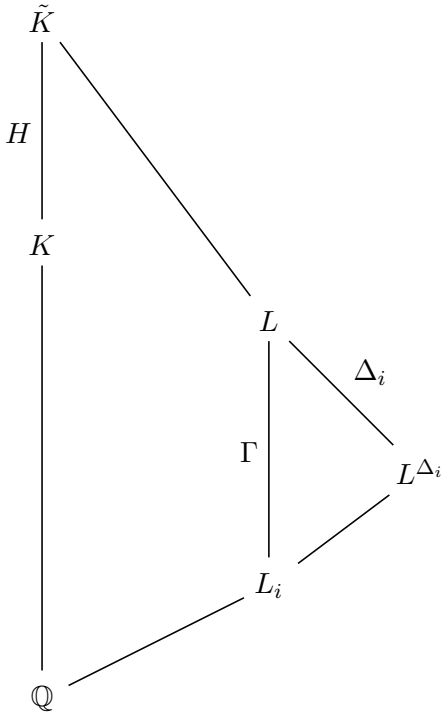
□

It is important to note however that some generalised norm relation do not come from a regular norm relation in a subgroup or in a quotient.

**Example 5.3.** For example, the symmetric group $S_4$ admits a norm relation over $\mathbb{Q}$ with respect to $H = C_2 \times C_2$, and $\mathcal{J} = \{D_8, S_3\}$. This generalised norm relation does not come from a regular norm relation because we can check that $S_4$ does not have a norm relation with respect to $\mathcal{J}$. It does not come from a quotient either because the largest normal subgroup of $S_4$ contained in $H$ is trivial.

Classical norm relations can be useful to compute class groups of number fields even when they are not Galois extensions of $\mathbb{Q}$.

Indeed, let $K$ be a non Galois extension of $\mathbb{Q}$. Denote by $\tilde{K}$ its Galois closure, $G$ its Galois group and $H < G$ such that $K = \tilde{K}^H$. Suppose there is a subfield $L$ of $\tilde{K}$ and a subfield $M$ of $L$ such that $L/M$ is a Galois extension of Galois group $\Gamma$. Suppose also that there exists a classical norm relation in $\mathbb{Q}[\Gamma]$ involving some subgroups $\Delta_i$, as in the figure below.




In this case, if we write the norm relation in $\mathbb{Q}[\Gamma]$ as $1 = \sum_i a_i N_{\Delta_i} b_i$, then we have a generalised norm relation $N_H = \sum_i a_i N_{\Delta_i}(b_i \cdot N_H)$ in $\mathbb{Q}[G]$ that we can use to compute the class group of $K$.

This is equivalent to saying that a subquotient of $G$ admits a classical norm relation, as in proposition 5.2. In the particular case where $L = \tilde{K}$, then the generalised norm relation comes from a classical norm relation in a subgroup of $G$, as in remark 5.1.

We saw already with example 5.3 that not all generalised norm relation of a group $G$ comes from a subgroup or a quotient of $G$. The following algorithm is useful to find examples where generalised norm relation allow to compute class groups more efficiently than classical norm relations in any subgroups or quotients.

**Algorithm 5.4.** input: A group $G$, that is the Galois group of $\tilde{K}/\mathbb{Q}$

output: For all subgroup $H$ of $G$, the maximum of the degree of the subfields of $\tilde{K}$ one needs to compute the class group of, in order to compute the class group of $\tilde{K}^H$ using the best classical norm relations in quotients of $G$.

- $L_J \leftarrow$ All subgroups of $G$ up to conjugation
- $M \leftarrow$ List of the $\frac{|G|}{|J|}$ for all $J$ in $L_J$. *The entries of $M$ represent the degrees of the $\tilde{K}^J$. The goal will be to explore all classical norm relations in all quotients of $G$ and update the entries of $M$ to represent the maximum degree of the fields one has to study in order to compute the class group of $\tilde{K}^J$.*
- $M_2 \leftarrow$ An empty list
- WHILE $M_2 \neq M$
  - $M_2 \leftarrow M$
  - FOR $i$ from 1 to $\#L_J$
    - $H \leftarrow L_J[i]$
    - FOR $j$ from $i+1$ to $\#L_J$
      - $J \leftarrow L_J[j]$
      - Check if $H$ is conjugate to a normal subgroup of $J$. If not, go directly to the next $J$.
      - Look for a classical norm relation in $J/H$ that minimizes the entries of $M$ corresponding to the subgroups involved.
      - If such a relation is found, update the entries of $M$ accordingly. The entry corresponding to $\tilde{K}^H$ but also those corresponding to its subfields or all the fields isomorphic to those.

**Example 5.5.** Let $G = C_3 \times PSL_3(2)$, and $H = S_3 < G$, suppose we have $\tilde{K}$ a Galois extension of $\mathbb{Q}$ of Galois group $G$. Then $K = \tilde{K}^H$ is a field of degree 84. To compute the class group of $K$, we can verify that

there are no classical norm relations in any quotients or subgroups of $G$ that allows us to recursively reduce the problem to fields of degree less than 84. However, there exists a generalised norm relation that allows us to reduce the problem to four fields of respective degree 24, 21, 8 and 3.

**Remark 5.6.** We can do a systematic research by enumerating all groups $G$ up to isomorphism, all subgroups $H < G$, and check every time if there is a generalised norm relation that is more efficient than any classical norm relation in any quotient or subgroups. For $|G| < 250$, we find 101 such examples of pairs $(G, H)$.

**Remark 5.7.** As explained in [2, theorem 2.11], the groups that do not admit classical norm relations are the ones with with a fixed point free unitary representation. We could not find any generalised norm relations in these groups either, except the ones coming from classical norm relations in quotients. We do not know if this is true in general or if counterexamples are simply larger.

In the rest of this section, we will see that if we have an example of a useful generalised norm relation for a finite group $G$, we can build infinitely many other examples, simply by taking the same relation in $C_p \times G$, for any prime $p$ that does not divide $|G|$.

**Definition 5.8.** Let $G$ be a group that admits a generalised norm relation with respect to $H < G$ and a set a subgroups $\mathcal{J} = \{J_1 \cdots J_\ell\}$. we say that the relation is *optimal* if it is the relation that maximizes the quotient $\frac{|J_i|}{|H|}$, where $J_i$ is the smallest group in $\mathcal{J}$.

**Remark 5.9.** With the notations of the previous definition, if $\tilde{K}/\mathbb{Q}$ is a Galois extension of Galois group $G$, then the quotient $\frac{|J_i|}{|H|}$ is the quotient of the degree of $\tilde{K}^H$ by the degree of $\tilde{K}^{J_i}$.

**Proposition 5.10.** *Let $G$ be a group that admits a generalised norm relation with respect to $H < G$ and a set a subgroups $\mathcal{J} = \{J_1 \cdots J_\ell\}$. Suppose this generalised norm relation is optimal. Let $p$ be a prime number that does not divide $|G|$. Then $C_p \times G$ admits an optimal generalised norm relation with respect to $1 \times H$ and $\mathcal{J}_2 = \{1 \times J_1, \cdots, 1 \times J_\ell\}$.*

*Proof.* Let $G' = C_p \times G$. Let $\rho'$ be an irreducible representation of $G'$. Then $\rho' = \xi \otimes \rho$, whis $\chi$ a character of $C_p$ and $\rho$ an irreducible representation of $G$.

**Lemma 5.11.** *For all subgroup $K'$ of $G'$, either $K'$ is of the form $1 \times K$ with $K < G$, or it is of the form $C_p \times K$ with $K < G$.*

*Proof.* Suppose $K'$ contains an element $i \times g \in G' = C_p \times G$ with $i \neq 1$. Let $n$ be the order of $g$ in $G$. Then, since $\gcd(n, p) = 1$, the subgroup $K'$ contains all the $(kn)i \times 1_G$ with $k$ in $\mathbb{N}$. So $C_p \times 1_G$ is contained in $G'$. So it is easy to check that the projection of $K'$ on $G$ is indeed a subgroup of $G$.

□

Let $K$ a subgroup of $G$. Then $(\rho')^{1\times K} = \rho^K$ and $(\rho')^{C_p\times K} = \chi^{C_p} \otimes \rho^K$. So $(\rho')^{C_p\times K} \neq 0$ if and only if $\chi$ is trivial and $\rho^K \neq 0$.

Since $G$ admits a generalised norm relation with respect to $H$ and $\mathcal{J}$, then for every irreducible representation $\rho$ of $G$, if $\rho^H \neq 0$, there exists $J \in \mathcal{J}$ such that $\rho^J \neq 0$. Let $\rho' = \chi \otimes \rho$ be an irreducible representation of $G'$. Then it is easy to check that if $(\rho')^{1\times H} \neq 0$, there exists $J \in \mathcal{J}$ such that $(\rho')^{1\times J} \neq 0$. So $G'$ admits a generalised norm relation with respect to $1 \times H$ and $\{1 \times J_1, \cdots, 1 \times J_\ell\}$.

Now let us prove that this relation is optimal. Suppose $G$ has a better generalised norm relation with respect to $\tilde{H}' < G'$ and $\{\tilde{J_1}', \ldots, \tilde{J_m}'\}$. Let $\tilde{H}, \tilde{J}_1, \cdots, \tilde{J}_m < G$ the projections of $\tilde{H}'$ and of the $\tilde{J_i}'$ onto $G$. Then, using the same method as before, it is easy to check that $G$ admits a generalised norm relation with respect to $\tilde{H}$ and the $\tilde{J}_i$, and that this norm relation is better than the first one, which is a contradiction.

□

# 6 Examples

**Example 6.1.** The group $G = S_5$ admits a generalised norm relation with respect to $H = S_3 < G$ and $\mathcal{J} = \{A_4, D_{12}, C_5 : C_4\}$. We can check that this relation does not come from a classical norm relation quotient. There are non conjugate copies of $S_3$ in $S_5$. For $H$ we have to take the one with no fixed points.

If we choose a Galois extension $\tilde{K}/\mathbb{Q}$ of Galois group $G$, then $K = \tilde{K}^H$ is of degree 20, and we can compute its class group inductively, by reducing the problem to three fields of respective degree 10, 10 and 6.

By choosing $\tilde{K}$ such that $K$ has a big discriminant, we can obtain examples where the recursive method is more efficient to compute the class group of $K$ than the preexisting methods. For example, consider the polynomial $p(x) = x^5 + 91x^4 + 7x^3 - 11x^2 - x + 1$ and define $\tilde{K}$ to be the splitting field of $p(x)$. Then $\tilde{K}$ has Galois group $S_5$, and $K = \tilde{K}^{S_3}$ is a number field of degree 20 and of discriminant $2^{28} \cdot 383^{10} \cdot 4723^{10} \cdot 23831^{10} \simeq 6 \cdot 10^{114}$. On Pari/GP [11], the function to compute $\mathrm{Cl}(K)$ was not able to finish in three days, whereas with the method of generalised norm relations, implemented also in Pari/GP,

we obtained the result in less than nine hours (CPU time). The result is $\mathrm{Cl}(K) = C_4 \times C_2^4$.

**Example 6.2.** The group $G = A_5$ admits a a generalised norm relation with respect to $H = C_2 \times C_2 < G$ and $\mathcal{J} = \{A_4, D_{10}\}$. We can check that this relation does not come from a classical norm relation quotient.

If we choose a Galois extension $\tilde{K}/\mathbb{Q}$ of Galois group $G$, then $K = \tilde{K}^H$ is of degree 15, and we can compute its class group inductively, by reducing the problem to two fields of respective degree 6 and 5. However, the method with classical norm relations also applies here, but with that method, the largest field we would need to consider is of degree 12.

To create a bigger example, since $7 \nmid |A_5|$, we can consider the generalised norm relation of $G' = C_7 \times A_5$ with respect to $H = C_2 \times C_2 < G$ and $\mathcal{J} = \{A_4, D_{10}\}$. That way, we can compute the class group of a field of degree 105 by reducing the problem to two fields of respective degree 42 and 35, whereas with classical norm relations, we would have reduced the problem to a field of degree 84.

For example, consider the polynomial $f(x) = x^6 - 2x^5 + 3x^4 - 4x^3 + 2x^2 - 2x - 1$. Define $\tilde{L}$ to be the splitting field of $f(x)$. Then $\tilde{L}$ has Galois group $A_5$. The splitting field $\tilde{M}$ of the polynomial $g(x) = x^4 + x^3 + 4x^2 + 20x + 23$ has Galois group $C_7$. Up to isomorphism, there is only one compositum $\tilde{K}$ of $\tilde{L}$ and $\tilde{M}$. What's more, $\tilde{K}/\mathbb{Q}$ is Galois and its Galois group is $G = C_7 \times A_5$. Denote by $K$ the subfield of $\tilde{K}$ fixed by $H = C_2 \times C_2$, which is a field of degree 105 and of discriminant $2^{126} \cdot 29^{90} \cdot 67^{42} \simeq 1.7 \cdot 10^{246}$. With the method involving only classical norm relation, we can compute $\mathrm{Cl}(K)$, but we have to compute the class group of some subfields, the largest of which is $F = \tilde{K}^{C_5}$, of degree 84 and of discriminant $2^{126} \cdot 29^{72} \cdot 67^{42} \simeq 8 \cdot 10^{219}$. On Pari/GP, the function to compute $\mathrm{Cl}(F)$ was not able to finish in over 5 months, whereas with our implementation of the method of generalised norm relations, we computed $\mathrm{Cl}(K)$ in about 5 days (CPU time). The result is $\mathrm{Cl}(K) = 1$.

# References

[1] Karim Belabas and Eduardo Friedman. "Computing the residue of the Dedekind zeta function". In: *Math. Comp.* 84.291 (2015), pp. 357–369. ISSN: 0025-5718,1088-6842. DOI: 10.1090/S0025-5718-2014-02843-3. URL: https://doi.org/10.1090/S0025-5718

[2] Jean-François Biasse et al. “Norm relations and computational problems in number fields”. English. In: *J. Lond. Math. Soc., II. Ser.* 105.4 (2022), pp. 2373–2414. ISSN: 0024-6107. DOI: 10.1112/jlms.12563.

[3] Robert Boltje. “Class group relations from Burnside ring idempotents”. English. In: *J. Number Theory* 66.2 (1997), pp. 291–305. ISSN: 0022-314X. DOI: 10.1006/jnth.1997.2165.

[4] Richard Brauer. “Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers”. German. In: *Math. Nachr.* 4 (1951), pp. 158–174. ISSN: 0025-584X. DOI: 10.1002/mana.3210040116.

[5] Johannes Buchmann. *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*. English. Sémin. Théor. Nombres, Paris/Fr. 1988-89, Prog. Math. 91, 27-41 (1990). 1990.

[6] Charles W. Curtis and Irving Reiner. *Methods of representation theory with applications to finite groups and orders. Volume 1.* English. Paperback edition. New York etc.: John Wiley &— Sons, 1990. ISBN: 0-471-52367-4.

[7] GE. “Algorithms related to multiplicative representations of algebraic numbers, PhD thesis”. In: *University of California, Berkeley* (1993).

[8] James L. Hafner and Kevin S. McCurley. “Asymptotically fast triangularization of matrices over rings”. English. In: *Discrete algorithms. Proceedings of the 1st annual ACM-SIAM symposium, held January 22-24, 1990 in San Francisco, CA (USA).* Philadelphia, PA (USA): SIAM, 1990, pp. 194–200. ISBN: 0-89871-251-3.

[9] A. K. Lenstra, H. W. jun. Lenstra, and László Lovász. “Factoring polynomials with rational coefficients”. English. In: *Math. Ann.* 261 (1982), pp. 515–534. ISSN: 0025-5831. DOI: 10.1007/BF01457454. URL: https://eudml.org/doc/182903.

[10] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems. A cryptographic perspective.* English. Vol. 671. Kluwer Int. Ser. Eng. Comput. Sci. Boston, MA: Kluwer Academic Publishers, 2002. ISBN: 0-7923-7688-9.

[11] *PARI/GP version 2.15.4*. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2023.

[12] I. Reiner. *Maximal orders*. English. Reprint of the 1975 original. Vol. 28. Lond. Math. Soc. Monogr., New Ser. Oxford: Oxford University Press, 2003. ISBN: 0-19-852673-3.

[13] Tomoyuki Yoshida. "On G-functors. II: Hecke operators and G-functors". English. In: *J. Math. Soc. Japan* 35 (1983), pp. 179–190. ISSN: 0025-5645. DOI: 10.2969/jmsj/03510179.