On Module Lattices with Galois-Symmetries: What You See Is Not What You Get

Keywords: module lattices, number fields, subfields and automorphisms

Abstract. This paper deals with the hardness of finding short vectors in module lattices. Let K be a number field of degree d and $\mathcal{O}_K$ its ring of integers. We show that if a module lattice M of rank n in $(\mathcal{O}_K)^n$ has some Galois-symmetries, namely if it is fixed coordinate-wise (as a set) by a group G of automorphisms of K, then M can actually be seen as a module of rank n over a subfield K' of K (K' is the fixed-field of G), whose degree is $|G|$ times smaller than the degree of K. When one wants to find short vectors in M, this translates into the observation that the module lattice M, which is a priori a lattice of rank $n \cdot d$ can in fact be seen as a lattice of rank only $n \cdot d/|G|$. Hence, finding short vectors in M is easier than what one could have expected by forgetting about the algebraic structure of M. This result is a generalization of a similar result by Boudgoust, Gachon and Pellet-Mary (Crypto'22), which was restricted to ideal lattices (i.e., modules of rank 1).

1 Introduction

Module lattices are Euclidean lattices that enjoy some extra algebraic structure, namely they are $\mathcal{O}_K$-submodules of K^n for some number field K and $\mathcal{O}_K$ its ring of integers. In this introduction, let us focus on a power-of-two cyclotomic field $K = \mathbb{Q}[X]/(X^d + 1)$, with d a power-of-two, and its ring of integers $\mathcal{O}_K = \mathbb{Z}[X]/(X^d + 1)$. A module in K^n is a subset of K^n generated by all $\mathcal{O}_K$-linear combinations of finitely many vectors. In other words, if M is a module, then there exist some finite number r of vectors (not necessarily K-linearly independent) $\mathbf{b}_1, \ldots, \mathbf{b}_r \in K^n$ such that $M = \{\sum_{i=1}^{r} x_i \mathbf{b}_i \,|\, x_i \in \mathcal{O}_K\}$. For simplicity in this introduction, we will only consider modules M such that the K-span of M is equal to K^n (i.e., the module has maximal rank). In this case, the integer n is called the rank of M. In the special case where $n = 1$ and $M \subseteq K$, the module M is usually called an ideal (instead of a module of rank 1).

Module lattices are of interest to cryptography since they are related to famous algorithmic hardness assumptions, such as the NTRU assumption [9] or the Ring and Module LWE assumptions [21,14,4,13]. These hardness assumptions have been successfully used to construct efficient post-quantum primitives, including three of the fours post-quantum primitives standardized by the NIST

in July 2022.[1] The relation between module lattices and the algorithmic problems mentioned above usually goes in two directions. On the one hand, we have reductions from finding short vectors in ideal lattices to solving NTRU and Ring LWE [18,21,14], as well as from finding short vectors in module lattices of rank ≥ 2 to solving NTRU and Module LWE [6,13] (this is restricted to special modules with unusually short vectors in the case of NTRU). On the other hand, NTRU, Ring and Module LWE instances can be transformed into modules of rank ≥ 2 in such a way that finding a short vector in this module can be used to solve the original algorithmic problem.

Given the relations between the problem of finding short vectors (SVP) in module lattices, and the cryptographic assumptions mentioned above, it is important to have a good understanding of module lattices and their geometry. In this article, we will focus on special module lattices, which enjoy some so-called Galois-symmetries. The number field K admits a certain number of field automorphisms (d in our running example, $\leq d$ in general, where d is the degree of K). Given a subgroup G of automorphisms of K, Galois theory tells us that if an element $x \in K$ is fixed by all the automorphisms from G (i.e., $\phi(x) = x$ for all $\phi \in G$), then x actually belongs to a subfield K' of K, of smaller degree $d' = d/|G|$. Here, we will focus on modules that are stabilized, as a set, by a group of automorphisms G. In other words, we consider modules M such that for all $\mathbf{m} \in M$ and all $\phi \in G$, the vector $\phi(\mathbf{m})$ is in M (where ϕ is applied coordinate-wise). The question we want to answer is, given such a module M, can we say (as in the case of an element $x \in K$) that the module M actually "belongs" to a subfield K' of K? Here, we should define what it means for a module M to belongs to a subfield K'. Clearly, we cannot ask that M is an $\mathcal{O}_{K'}$ submodule of $(K')^n$, since M is not even a subset of $(K')^n$. Instead, we will say that M belongs to a subfield K' if it holds that M is the extension to K of an $\mathcal{O}_{K'}$-submodule M' of $(K')^n$, i.e., $M = M' \cdot \mathcal{O}_K$. If we can prove that a module M belongs to a subfield K' in this sense, then it means that one can solve algorithmic problems, such as finding short vectors in M, by actually considering the underlying $\mathcal{O}_{K'}$-module M', which has a smaller dimension than M when seen as a lattice.

This question was already answered in the case of ideal lattices (i.e., modules of rank one) in [17,3].[2] In these works, the authors showed that indeed, if some ideal I in K is stabilized (as a set) by some group G of automorphisms of K,[3] then one can see it as an ideal in a subfield K' of K, of degree $d/|G|$. In the case of module lattices of rank ≥ 2, partial results exist [19], but there is so far no clear answer to this question (the results of [19] are significantly more restrictive than the simple condition "M is stabilized by a group G of automorphisms").

[1] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4
[2] [17] proved it for *prime* ideal lattices, and [3] generalized it to any ideal.
[3] and under some mild assumption on I

Contributions. In this article, we answer the question for modules of any rank, by generalizing the ideas of [17,3]. We prove that if a module M is stabilized as a set by a group G of automorphisms of K, then M can be seen as a module of a smaller field K', which reduces its dimension as a lattice by factor $|G|$. Hence, one can find short vectors in M faster than what would be expected in a non-structured lattice of the same dimension. This results holds under some mild condition on the discriminant ideal of M,[4] which is the same condition that [3] already had for their result on ideals. More formally, we prove the main result below. In this statement, the γ-approximate Hermite Shortest Vector Problem (γ-HSVP) asks, given as input a lattice L of rank n, to output a nonzero vector of L whose euclidean norm is at most $\gamma \cdot \det(L)^{1/n}$.

Main result 1 (Informal formulation, see Corollary 4.3). *There is an algorithm that takes as input a module $M \subset (\mathcal{O}_K)^n$ of rank n (for some $n > 0$) whose discriminant is non-ramified, and a parameter $\gamma \geq 1$, and solves γ-HSVP in M in time*

$$\text{poly}(\textit{input size}) \cdot 2^{O\left(\frac{nd \cdot \log(nd)}{|G| \cdot \log \gamma}\right)},$$

where G is the group of automorphisms of K fixing M as a set.

In addition to this result, we also prove that one can solve the approximate shortest vector problem (γ-SVP) in a module M stabilized by a group of automorphisms, by reducing the problem to a problem of smaller dimension. This reduction does not require any assumption on the discriminant of the module M. Since it applies to modules of any rank, it can also be used for ideals that did not satisfied the mild assumption required in [3]. However, the approximation factor achieved by this algorithm is slightly bigger (by a factor d) than the one achieved by the other reduction. More formally, we prove

Main result 2 (Informal and specialized formulation, see Corollary 3.2). *Let K be a power-of-two cyclotomic number field of degree d.*[5] *There is an algorithm that takes as input a module $M \subset K^n$ of rank n (for some $n > 0$) and a parameter $\gamma \geq 1$, and solves $(d \cdot \gamma)$-SVP in M in time*

$$\text{poly}(\textit{input size}) \cdot 2^{O\left(\frac{nd \cdot \log(nd)}{|G| \cdot \log \gamma}\right)},$$

where G is the group of automorphisms of K fixing M as a set.

This second result is slightly more general and has a simpler proof than the first one. The fact that it achieves an approximation factor slightly worse

[4] The discriminant ideal of a module M is some ideal associated to M, which plays for modules the same role as the determinant would play for standard lattices (it somehow measures the density of the module).

[5] The result also holds for non cyclotomic fields, but in this case the approximation factor has to be increased by a quantity depending on the number field K, which might be larger than d.

than the first one might not be so much of a problem for some cryptanalytic applications. However, we believe that the proof of the first result is more instructive from a theoretical point of view. It really shows that a module M fixed by some automorphisms is an inflated module, generated by a module that lives in a smaller space. This observation could be useful to solve other algorithmic problems, such as the closest vector problem, or the bounded distance decoding problem.

Techniques. The proof of Main result 2 relies on a following simple observation. If K is a field and G is a subgroup of automorphisms of K, then K has a subfield K' consisting of all the elements of K fixed by elements of G. In this situation, we have a map, called the trace map Tr, which sends elements of K into K'. A nice property of this trace map is that, for an element $x \in K$, the euclidean norm of $\mathrm{Tr}(x)$ is not much larger than that of x (it is at most a factor d times larger). Moreover, if M is fixed as a set by the elements of G, then for any vector $\mathbf{m} \in M$, its trace $\mathrm{Tr}(\mathbf{m})$ is still an element of M, which is not the case in general for an arbitrary module M (here, the trace map is applied coordinate-wise to the vector $\mathbf{m}$). The algorithm from Main result 2 is then as follows. Given as input a module M fixed by G, we compute the module $\mathrm{Tr}(M) = \{\mathrm{Tr}(\mathbf{m}) \,|\, \mathbf{m} \in M\} \subset (K')^n$ consisting of the trace of all the elements of M (one can show that this is a module over the smaller ring $\mathcal{O}_{K'}$). This module contains the trace of a shortest nonzero vector of M, so its minimum is not much larger than the one of M. Moreover, since M is fixed by G, then any element of $\mathrm{Tr}(M)$ is also an element of M. Hence, a solution to SVP in $\mathrm{Tr}(M)$ also provides a solution to SVP in M, with a slightly worse approximation factor.

The proof of Main result 1 follows the same high-level framework as the proofs of [17,3]. First, we prove in Proposition 4.1 that if we intersect the module M with the subspace $(K')^n$, and then multiply back by elements of $\mathcal{O}_K$, then we recover the module M. This proposition is actually the core of the proof, and it holds only if M is fixed by G. We provide two proofs of Proposition 4.1 (and a third one in appendix). The first proof is algorithmically inspired by the Hermite Normal Form for module lattices. It requires little mathematical background, but is not very enlightening if one wants to understand why the result holds. The second proof is inspired by the local-global principle from commutative algebra, exploiting the fundamental fact that the module lattices in question are locally-free. This one requires more mathematical background, but is more natural from a mathematical point of view. With this result at hand, we can then show that the normalized volume $\det(M')^{1/(d'n)}$ of $M' := M \cap (K')^n$ (with d' the degree of K') is upper bounded by the normalized volume $\det(M)^{1/dn}$ of M. Hence, by definition of the Hermite shortest vector problem, any solution to HSVP in M' is also a solution to HSVP in M.

Impact. We would like to highlight the fact that the module lattices that are targeted by our algorithms are *very specific* module lattices. For most module lattices, the group G of automorphisms fixing the module will be reduced to

the identity, and in this case our algorithms simply consist in running the BKZ algorithm on the module lattice, forgetting everything about its structure. In particular, the modules that are obtained from random instances of NTRU, Ring or Module LWE are very unlikely to be fixed by any automorphism of K (except the identity). Hence, our algorithms do not enable us to solve instances of NTRU or Ring/Module LWE faster than what was previously known. So far, we were not able to find cryptographic constructions which we could break using our algorithms for modules with Galois-symmetries. Nevertheless, we believe our results may serve as a novel warning sign e.g., for future designers who may wish to introduce such symmetries for the sake of cryptosystem performance. In any case, we believe it is prudent to develop a thorough understanding of the possible effects on security of module lattices caused by symmetries of the underlying number field, and we view our results primarily as a novel stepping stone in that process.

2 Preliminaries

2.1 Lattices

For a lattice L, we write $\lambda_1(L) := \min_{\mathbf{v}\in L\setminus\{0\}} \|\mathbf{v}\|$ its first minimum, and $\lambda_i(L) := \min\{\delta > 0 \mid \exists \text{ linearly independent } \mathbf{v}_1, \ldots, \mathbf{v}_i \in L \text{ s.t. } \forall j \ \|\mathbf{v}_j\| \leq \delta\}$ its successive minima. We let $\det(L) = \sqrt{\det(\mathbf{B}^T\mathbf{B})}$ be its determinant (where $\mathbf{B}$ is any basis of L). Minkowski's first theorem states that $\lambda_1(L) \leq \sqrt{n}\det(L)^{1/n}$ for any rank-n lattice L.

Definition 2.1 (γ-SVP and γ-HSVP). *Let $\gamma \geq 1$. The γ-approximate Shortest Vector Problem (γ-SVP) asks, given as input a basis of a lattice L, to output $\mathbf{v} \in L \setminus \{0\}$ such that $\|\mathbf{v}\| \leq \lambda_1(L)$.*

The γ-approximate Hermite Shortest Vector Problem (γ-HSVP) asks, given as input a basis of a rank n lattice L, to output $\mathbf{v} \in L \setminus \{0\}$ such that $\|\mathbf{v}\| \leq \gamma \cdot \sqrt{n} \cdot \det(L)^{1/n}$.

We note that, by Minskwski's first theorem, γ-HSVP in L reduces to γ-SVP in L for any $\gamma \geq 1$ and lattice L.

When we want to find short vectors in a lattice, we can use the BKZ algorithm, which gives us different trade-offs between run-time and approximation factor. Below, we recall the complexity of provable variants of the BKZ algorithm.

Lemma 2.2 ([8, Theorem 1] and [1, Theorem D.1]). *There is a probabilistic algorithm that takes as input a basis $\mathbf{B}_L \subset \mathbb{Q}^n$ of a rank n lattice L, a parameter $\gamma \in [1, 2^n]$ and solves γ-SVP in L in time* $\mathrm{poly}(n, \mathrm{size}(\mathbf{B}_L)) \cdot 2^{O(n \log n/\log \gamma)}$.

Proof. For approximation factors γ larger than $16n^6$, one can use [8, Theorem 1], and the discussion following the theorem, by picking $\beta = 1+\frac{(n-1)\log(n)}{\log(\gamma)-3\log(n)-\log(4)} \leq 1+\frac{2n\log(n)}{\log(\gamma)}$ (where the upper bound follows from the lower bound on γ). To solve SVP with smaller approximation factors, up to 1, one can use the probabilistic algorithm from [1, Theorem D.1], which runs in time $2^{n+o(n)} = 2^{O(n\log n/\log\gamma)}$ whenever $\gamma \leq 16n^6$, as desired. (This result is also used to estimate the cost of solving 1-SVP in dimension β in [8, Theorem 1]). □

2.2 Number fields

In this article, K and K' will be (mainly) number fields, of respective degree d and d', and $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ will be their respective rings of integers. Moreover, we will always have K' be a subfield of K. We let Δ_K be the absolute value of the discriminant of K. If K/K' are number fields of degree d and d', then it holds that $\Delta_K^{1/d} \geq \Delta_K^{1/d'}$ (see, e.g., [15, Exercice 23]).

We write $\mathrm{Aut}_{K'}(K)$ the set of all field automorphisms of K that fix K' pointwise. If $\phi \in \mathrm{Aut}_{K'}(K)$ and $\mathbf{v} := (v_1, \ldots, v_m) \in K^m$, we define $\phi(\mathbf{v})$ to be the vector $\mathbf{v}$ where we applied ϕ coordinate-wise, i.e., $\phi(\mathbf{v}) = (\phi(v_1), \ldots, \phi(v_m))$. We will often assume that the extension K/K' is Galois, which is equivalent to $|\mathrm{Aut}_{K'}(K)| = d/d'$. The Galois extension we consider will often be obtained by using the following lemma.

Lemma 2.3 ([12, Theorem 1.8, Chap. 6]). *Let K be a number field and H be a subgroup of $\mathrm{Aut}_{\mathbb{Q}}(K)$. Let K^H be the subfield of K fixed by H. Then K/K^H is Galois and has Galois group H.*

When K/K' is Galois with Galois group G, we define the relative trace and relative norm maps, from K to K' by

$$\mathrm{Tr}_{K/K'} : K \to K' \qquad \text{and} \qquad \mathcal{N}_{K/K'} : K \to K'$$
$$x \mapsto \sum_{\phi\in G} \phi(x) \qquad\qquad x \mapsto \prod_{\phi\in G} \phi(x)$$

respectively. When $K' = \mathbb{Q}$ we simply write Tr_K and $\mathcal{N}_K$.

Embedding. We write σ_K the Minkowski's embedding associated to the field K, i.e., the map

$$\sigma_K : K \to \mathbb{C}^d$$
$$x \mapsto (\sigma_1(x), \ldots, \sigma_d(x)),$$

where $\sigma_1, \ldots, \sigma_d$ are the complex embeddings of K. This maps sends $\mathcal{O}_K$ to a rank d lattice in $\mathbb{C}^d$.[6]

[6] Note that this lattice is not full rank, since $\mathbb{C}^d$ has real dimension $2d$, but this will not be a problem here.

We will use the following results on the Minkowski's embedding.

Lemma 2.4. *Let $\mathbf{v} \in K^m$ and $\phi \in \mathrm{Aut}_{\mathbb{Q}}(K)$. Then $\|\sigma_K(\phi(\mathbf{v}))\| = \|\sigma_K(\mathbf{v})\|$.*

Proof. Since ϕ is an automorphism of K, it is invertible and so the map

$$\{\text{Complex embeddings of } K\} \to \{\text{Complex embeddings of } K\}$$
$$\sigma \mapsto \sigma \circ \phi$$

is a bijection. This proves that the vector $\sigma_K(\phi(\mathbf{v}))$ is obtained by permuting the coordinates of $\sigma_K(\mathbf{v})$. In particular, $\|\sigma_K(\phi(\mathbf{v}))\| = \|\sigma_K(\mathbf{v})\|$. □

Lemma 2.5. *Let K/K' of respective degrees d and d', and $\mathbf{v}' \in (K')^m$. Then $\|\sigma_K(\mathbf{v}')\| = \sqrt{d/d'} \cdot \|\sigma_{K'}(\mathbf{v}')\|$.*

Proof. Each complex embedding of K' extends into d/d' complex embeddings of K', hence, $\sigma_K(\mathbf{v}')$ is obtained from $\sigma_{K'}(\mathbf{v}')$ by repeating each coordinate d/d' times. □

Lemma 2.6. *Let K/K' be a Galois extension of Galois group G and respective degrees d and d', and let $\mathbf{v} \in K^m$. Then $\|\sigma_{K'}(\mathrm{Tr}_{K/K'}(\mathbf{v}))\| \leq \sqrt{d/d'} \cdot \|\sigma_K(\mathbf{v})\|$.*

Proof. By definition of the Trace map, we have that

$$\begin{aligned}\|\sigma_K(\mathrm{Tr}_{K/K'}(\mathbf{v}))\| &= \|\sum_{\phi \in G} \sigma_K(\phi(\mathbf{v}))\| \\ &\leq \sum_{\phi \in G} \|\sigma_K(\phi(\mathbf{v}))\| \\ &= d/d' \cdot \|\sigma_K(\mathbf{v})\|\end{aligned}$$

where the last equality comes from Lemma 2.4. We conclude using Lemma 2.5 with $\mathbf{v}' = \mathrm{Tr}_{K/K'}(\mathbf{v}) \in (K')^m$. □

The algorithm we describe in Section 3 uses some quantity $\delta_{K/\mathbb{Q}}$ depending on the number field K, which we define below.

Definition 2.7. *For an extension K/K' of number fields with respective degrees d and d', we define*

$$\delta_{K/K'} = \min\{\delta > 0 \,|\, \exists \alpha_1, \cdots, \alpha_{d/d'} \in \mathcal{O}_K,\ K'\text{-linearly independent with } \|\sigma_K(\alpha_i)\|_\infty \leq \delta,\ \forall i\}.$$

Lemma 2.8. *For any extension of number fields K/K', we have $1 \leq \delta_{K/K'} \leq \delta_{K/\mathbb{Q}} = \lambda_d^\infty(\sigma_K(\mathcal{O}_K))$. Moreover, if K is a cyclotomic field, then $\delta_{K/\mathbb{Q}} = 1$.*

Proof. For any non-zero element $\alpha \in \mathcal{O}_K$, we know that $\|\sigma_K(\alpha)\|\infty \geq 1$ since $|\mathcal{N}_K(\alpha)| \geq 1$ is the product of the absolute values of the coordinates of the vector $\sigma_K(\alpha)$.

In order to prove that $\delta_{K/K'} \leq \delta_{K/\mathbb{Q}}$, let us fix $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ that are $\mathbb{Q}$-linearly independent and with $\|\sigma_K(\alpha_i)\|_\infty \leq \delta_{K/\mathbb{Q}}$. The α_i's generate K as a $\mathbb{Q}$-vector space (since they have rank d, which is the $\mathbb{Q}$-dimension of K), and so in particular they also generate K as a K'-vector space. This means that we can extract from the α_i's a K'-basis of K, that is, a set of d/d' K'-linearly independent vectors. Since this set is a subset of the α_i's, the maximum of their infinity norm is in particular $\leq \max_i \|\alpha_i\|_\infty = \delta_{K/\mathbb{Q}}$.

In the case of a cyclotomic number field K, if ζ is a primitive d-th root of unity in K; then $\{\alpha^i\}_{0 \leq i \leq d-1}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and satisfies $\|\sigma_K(\alpha^i)\|_\infty = 1$ for all i. □

2.3 Module Lattices from the Algebraic Perspective

The primary object of interest in this article will be finitely generated $\mathcal{O}_K$-modules, included in K^m for some $m > 0$. These objects are a special case of a broader class of objects called finitely generated torsion-free modules over Dedekind domains. In Section 5.2, for the need of the proof, we will need to consider finitely generated torsion-free modules over a Dedekind domain which is not $\mathcal{O}_K$. Since most of the result we will use also hold over any Dedekind domain, we decided to present them in the more general context of Dedekind domain, instead of instantiating the results to ring of integers of a number field.

Below, we start by some introduction to the theory of finitely generated torsion-free module over Dedekind domain, and then we state some useful results over these modules.

More references on the topic can, for instance, be found as follows: Galois theory and theory of free modules over PIDs in [12], algebraic number theory including basic structure of Dedekind modules) in [11], and theory of modules, localization and basic local-global results in [2], Dedekind-modules (including discriminant, structure theorems, HNF and algorithms) in [5]. See also [7] for the latter (minus algorithms).

Some Generalities on Modules. Let R be a commutative ring. An *R-module* is an abelian group M together with a ring morphism sending R to the endomorphism ring of M. In other words, R acts on M as a well-behaved scalar-multiplication. A submodule N is a subgroup of M that is closed under the R-scalar multiplication defined on M. An R-module M is *finitely generated* if there is a finite subset $V \subset M$ such that $R[V] = M$, where $R[V]$ denotes the R-span of V, i.e., the R-module consisting of all finite R-linear combinations over V. The module M is (finite) *free* (over R) if there is such an V that, in

fact, constitutes a *basis*: each $m \in M$ is uniquely expressed as an R-linear combination over the elements of V. Or, equivalently, $M \simeq R^n$ (as R-modules), for some nonnegative integer n. Here, R^n denotes the n-fold cartesian product over R with coordinate-wise addition and -scalar-multiplication. We have $R^n \simeq R^m$ as R-modules if and only if $n = m$. [7] So two such free modules are isomorphic if and only if they have the same dimension.

An R-module M is *torsion-free* if $r \cdot m = 0$ with $r \in R$ and $m \in M$ implies $r = 0$ or $m = 0$. The significance of torsion-freeness in the present context is that it enables arguments involving linear-independence, e.g. each nonzero element is linearly independent.

An R-module is *noetherian* if each of its R-submodules is finitely generated. (This then includes the module itself, of course). When considering R as an R-module in the most natural way (i.e., with scalar multiplication defined by ring multiplication), the ideals of R are precisely the R-submodules of R. The ring R is *noetherian* if each of its ideals is finitely generated as R-module. It is a standard fact that a finitely generated module over a noetherian ring is a noetherian module. Furthermore, an R-module M is *projective* if, for each surjective morphism of R-modules $f : M' \to M$, there is a morphism of R-modules $g : M \to M'$ such that $f \circ g = \mathrm{Id}_M$. The significance of this is that one has the internal direct sum decomposition $M' = \ker f \oplus g(M)$, where $g(M) \simeq M$ since g is injective. It is a standard fact that a free module is projective.

Suppose R is a noetherian domain[8]. Write K for its field of fractions. Let M be a finitely generated torsion-free R-module. It is a standard fact that M is torsion-free if and only if M maps injectively into the K-vector space $M \otimes_R K$, via $m \mapsto m \otimes 1$. If M is torsion-free, then the K-dimension of that space – which is finite – equals the cardinality of any maximal R-linearly independent subset of M. The latter is then called the *R-rank* of M. One take-away of this is that each such module occurs – up to isomomorhism – as R-submodule of some affine vector space K^n (viewing the latter as R-module in the natural way, i.e., by restriction of the scalars). Henceforth, "after clearing denominators," the same conclusion holds when replacing K^n by R^n. It follows from the above characterization that the rank of an R-submodule $M \subset R^n$ is equal to the K-dimension of the vectorspace $M \cdot K \subset K^n$. Here, $M \cdot K$ denotes the K-vector space generated by M, i.e., the space of all finite K-linear combinations taken over M. Also note that if N is an R-submodule of R^n, then it is (trivially)

[7] Only the forward direction needs commenting. Choose a maximal ideal $P \subset R$ (so that R/P is a field) and notice that an isomorphism $R^n \to R^m$ induces an isomorphism of R/P-vectorspaces $R^n \otimes_R R/P \to R^m \otimes_R R/P$, which translates further into an isomorphism $(R/P)^n \to (R/P)^m$. So, by linear algebra, $n = m$. If R is a domain – i.e., there are no zero divisors –, one may tensor-up with the field of fractions K and use the same line of reasoning. But, in this case, the tensor product can also be avoided;"by taking K-linear combinations," one notices that there is a (unique) induced vector space isomorphism $K^n \to K^m$ (and, hence, $n = m$).

[8] R is a domain if it has no zero-divisors. Or, equivalently, it is torsion-free as R-module.

torsion-free (as in the case of K^n) but it is automatically finitely generated since R^n is a noetherian R-module; so there is no need to require separately that it is finitely generated.

In the special case that R is a principal ideal domain (PID), then, by a standard fact, M is free and, hence, its R-rank equals it dimension as a free module. In particular, two such modules M, N are isomorphic if and only if they have the same dimension. It is a standard fact in this case that if M' is an R-submodule then M' is free as well and there is a basis $b_1, \dots b_\ell$ of M and there are nonzero scalars $\lambda_1, \dots, \lambda_d \in R$ (where d is the dimension of M'), such that $\lambda_1 b_1, \dots, \lambda_d b_d$ is a basis of M'.

Finally, it is convenient to say a few words about *rings and modules of fractions*. Now suppose again that R is a commutative ring (with no further restrictions imposed). If $S \subset R$ is a multiplicative subset, i.e., $1 \in S$ and S is closed under multiplication, then one may form the ring $S^{-1} \cdot R$ of all expressions r/s ($r \in R, s \in S$) under the equivalence relation $r/s \equiv r'/s'$ if there is $u \in S$ such that $u(rs' - r's) = 0$. [9] Note that if R is a domain (and $0 \notin S$), then this simplifies to the condition that $rs' = r's$. In this case, we may view R as (canonically) embedded via $r \mapsto r/1$.

In general, an important example is obtained by taking a prime ideal $P \subset R$ and defining the multicative set $S := R - P$. In this case, $S^{-1} \cdot R$ is called the *local ring at* P and is typically denoted as R_P instead. A special case is when R is a domain (so that (0) is a prime ideal) and the field of fractions of R is then obtained by taking $S := R - \{0\}$. If M is an R-module, we may form the $(S^{-1} \cdot R)$-module $S^{-1} \cdot M$ by imposing the equivalence condition on terms of the form m/s instead. In case of localization at a prime ideal P, we will speak of the R_P-module M_P.

It is important to note that the localized ring R_P typically has a simpler structure; it always has a single maximal ideal (with a residue class field associated to it), but, in given cases, further simplifications may be at play (e.g., when it is a PID or even a discrete valuation ring). Therefore, the "localized version" of a problem may be easier to deal with. Pairing this with the "local-global" phenomenon (i.e., the situations where a property P is shown to hold globally if and only if it holds locally everywhere), localization can be a powerful tool. In this respect, it is useful that localization can be expressed by a tensor-product $M \otimes_R R_P$ and that tensoring-up exact sequences (of maps between modules) with R_P preserves exactness. That said, if R is a domain and if M is given as a submodule of R^n (which is the case in this paper), then M_P may be obtained "by taking finite R_P-linear combinations over M", yielding $M_P = R_P \cdot M \subset (R_P)^n$, with M (canonically) embedded into it. This procedure can also be applied to maps.

[9] If $0 \in S$, then $S^{-1} \cdot R$ is necessarily the trivial module $\{0\}$.

Dedekind Modules. A Dedekind domain $\mathcal{O}$ is a domain (that is not a field), satisfying the following further requirements: (i) it is noetherian, (ii) each nonzero prime ideal is maximal, and (iii) it is integrally closed in its field of fractions K. [10] Important examples of Dedekind domains are PIDs and the ring of integers of an algebraic number field. One gets new such ring from a given one by taking a finite, separable [11] extension of the field of fractions. The integral closure [12] in this extension is Dedekind domain as well. Distinguished properties of a Dedekind-ring $\mathcal{O}$ include the facts that there is Dedekind-factorization of ideals, there is a class group $\mathrm{cl}(\mathcal{O})$ (which is finite in the number field case), and for each nonzero prime ideal P of $\mathcal{O}$, the local ring $\mathcal{O}_P$ is a DVR (which is, in particular, a PID). In other words, a Dedekind domain is "locally a DVR."

Let $\mathcal{O}$ be a Dedekind domain. Consider a finitely generated, torsion-free $\mathcal{O}$-module M. [13] A central handle towards structural results about such modules is the fact that they are projective. This is a consequence of the fact that they are locally free, i.e., for each nonzero prime ideal P of $\mathcal{O}$, the localized $\mathcal{O}_P$-module M_P is free (with dimension equal to the $\mathcal{O}$-rank of M), and, therefore, locally projective. Peeling off one single dimension after the other (in each step gluing local information together), this fact quickly leads to the following structural result. Write n for the rank of M and K for the field of fractions of $\mathcal{O}$. Then there are rank-1 submodules $M_1, \ldots, M_n \subset M$ such that we have the internal direct sum decomposition $M = M_1 \oplus \ldots \oplus M_n$. This can be rewritten as follows. For $i = 1, \ldots, n$, there is a nonzero ideal J_i of $\mathcal{O}$, a nonzero element $m_i \in M_i$ and a nonzero scalar $\lambda_i \in K$ such that

$$M = J_1 \cdot (\lambda_1 \otimes m_1) \oplus \ldots \oplus J_n \cdot (\lambda_n \otimes m_n) \subset M \otimes_{\mathcal{O}} K.$$

In particular, the $(1 \otimes m_i)$'s form a K-basis of the n-dimensional K-vector space $M \otimes_{\mathcal{O}} K$, with M naturally embedded via $m \mapsto (1 \otimes m)$. Fixing some identification of the latter space with the affine space K^n, this translates (up to isomorphism) to

$$M = J_1 \cdot (\lambda_1 m_1) \oplus \ldots \oplus J_n \cdot (\lambda_n m_n) \subset K^n,$$

i.e., "M has a *pseudo-basis*." Note that the $\lambda_i m_i$'s form a K-basis of K^n, but that the $\lambda_i m_i$'s may not be contained in M (due to the scalars). Note that this "pseudo-basis theorem" has several extensions. One of those – the so-called Invariant Factor Theorem – deals with the situation-next-in-line where we have an inclusion of modules and want to "line them up" along the same peudo-basis

[10] i.e., $x \in K$ is integral over $\mathcal{O}$ if and only if $x \in \mathcal{O}$.

[11] An extension is separable if, for each element in this extension, its minimal polynomial does not have roots of multiplicity > 1.

[12] The ring consisting of all elements in the extension that are integral over the base ring.

[13] Since $\mathcal{O}$ is, in particular, a noetherian domain, the observations made earlier apply a forteriori.

in some unique way[14], a generalization for a similar result for torsion-free free modules over PIDs.

A further fundamental fact is that, for given ring $\mathcal{O}$, the isomorphism classes are parameterized by the class group $\mathrm{cl}(\mathcal{O})$ and the rank. More precisely, the Steinitz-class of M is the image of the product of the J_i's in this class group (so, in particular, this image does not depend on the decomposition chosen). Then modules M, M' is isomorphic if and only if they have the same rank and their respective Steinitz-classes are equal. Note that, if $\mathcal{O}$ is a PID (so that the class group is trivial), this collapses to the condition that the respective ranks are equal.

Note that each $\mathcal{O}$-submodule of $\mathcal{O}^n$ is torsion-free and finitely generated. Torsion-freeness is trivial. Since $\mathcal{O}$ is, in particular, noetherian and since $\mathcal{O}^n$ is obviously finitely generated over $\mathcal{O}$ (by the unit vectors), $\mathcal{O}^n$ is a noetherian module; so its submodules are finitely generated. In the other direction, a torsion-free, finitely-generated $\mathcal{O}$-module M may be thought of as $\mathcal{O}$-submodule of some $\mathcal{O}^n$. By the structural results above, this already holds with K^n instead of $\mathcal{O}^n$. But by clearing denominators in a finite set of generators, some $\mathcal{O}$-multiple gives an isomorphic copy inside $\mathcal{O}^n$. It is worth noting that this $\mathcal{O}$-scalar can often be chosen in a much smaller ring than $\mathcal{O}$, since this is true for clearing the denominator of just a single fraction in K. For instance, if K is a number field, then, for each $x \in K$, there is a nonzero integer $\mu \in \mathbb{Q}$ such that $\mu x \in \mathcal{O}$. A similar observation holds with $\mathbb{Q}$ replaced by the maximal order of some intermediate number field (if this exists). This observation is sometimes useful.

Setting. From now on, we will consider the following setting. First, we will consider only the case where K and K' are number fields. The ring $\mathcal{O}' \subseteq K'$ is a Dedekind ring such that K' is its field of fractions, and let $\mathcal{O}$ be the integral closure of $\mathcal{O}'$ in K. This implies that $\mathcal{O}$ is also a Dedekind domain. Whenever K/K' is assumed to be Galois, we write $G := \mathrm{Aut}_{K'}(K)$ for its Galois group. Regarding the modules, we will only consider finitely generated $\mathcal{O}$-modules M that are included in K^m for some $m > 0$ (hence are torsion-free).

A typical instantiation of this setting is when $\mathcal{O} = \mathcal{O}_K$ and $\mathcal{O}' = \mathcal{O}_{K'}$ are the rings of integers of K and K' respectively. But the Dedekind rings need not be a ring of integers in some number field. For example, they can be certain "localized" versions of rings of integers, or completions.

Discriminant ideal. Now let M be an $\mathcal{O}$-submodule of K^n of rank n (i.e., M is full rank). Recall that M admits a pseudo-basis $((I_i, \mathbf{b}_i))_{1 \le i \le n}$ where $\mathbf{b}_i \in K^n$ are linearly independent, $I_i \subset K$ are $\mathcal{O}$-fractional ideals and $M = \sum_i I_i \cdot \mathbf{b}_i$. The *discriminant ideal* of M (or just discriminant for short) is the fractional ideal

[14] See the formulation in [16], Theorem 3.32 or see [5].

defined as [15]

$$\operatorname*{disc}_K(M) = \left(\left(\prod_{i=1}^{n} I_i \right) \cdot \det(\mathbf{b}_1, \ldots, \mathbf{b}_n), \right)^2 .$$

This definition does not depend on the pseudo-basis selected. Note that it is straightforward that the discriminant can be rewritten as the square of the fractional ideal generated by all elements of the form $\det(\mathbf{m}'_1, \ldots, \mathbf{m}'_n)$, with the $\mathbf{m}'_i \in \mathbf{b}_i \cdot I_i$. Also note that, if $M \subset \mathcal{O}^n$, then $\operatorname{disc}_K(M)$ is in fact an ideal of $\mathcal{O}$. We also have the following interesting property.

Lemma 2.9. *For a Dedekind domain $\widetilde{\mathcal{O}}$, let $N, M \subset \widetilde{\mathcal{O}}^n$ be $\widetilde{\mathcal{O}}$-submodules of maximal rank n. Suppose $N \subset M$. Then $\operatorname{disc}_K(M) \mid \operatorname{disc}_K(N)$. Moreover, $N = M$ if, and only if, $\operatorname{disc}_K(N) = \operatorname{disc}_K(M)$.*

Hermite normal form. Let $M \subset K^n$ be a rank-n module. Then, there exists a pseudo-basis $((I_i, \mathbf{b}_i))_{1 \le i \le n}$ of M, called the *Hermite Normal form* of M (or HNF for short), such that the matrix $\mathbf{B}$ formed by concatenating the column vectors $\mathbf{b}_i$ is upper triangular with 1's on the diagonal (see [5, Thm. 1.4.6]).

***G*-stable modules.** Let G be a group of automorphisms of K. We define a notion of G-stable modules.

Definition 2.10. *Let K be a number field, G be a group of automorphisms of K and M be an $\mathcal{O}$-module included in K^m for some $m > 0$. We say that M is G-stable if $G(M) := \{\phi(\mathbf{m}) \,|\, \phi \in G, \mathbf{m} \in M\}$ is equal to M.*

If M is a G-stable module of K, we write M^G the set of vectors of M fixed by all automorphisms of G, that it $M^G = \{\mathbf{m} \,|\, \forall \phi \in G\,, \phi(\mathbf{m}) = \mathbf{m}\}$. This is equal to the intersection of M with $(K')^m$, where K' is the subfield of K fixed by G.

Definition 2.11 (Decomposition field of a module). *Let K be a number field and $M \subset K^m$ be a rank-n $\mathcal{O}$-module. We define*

$$H_M := \{\phi \in \operatorname{Aut}_{\mathbb{Q}}(K) \,|\, \phi(M) = M\},$$

and K_M the subfield of K fixed by H_M. We say that K_M is the decomposition field of the module M.

Note that by Lemma 2.3, K/K_M is always Galois.

[15] A more general and coordinate-free definition can be given in terms of a nondegenerate bilinear form, replacing the square of the determinant expression in the definition given here by the determinant of a Gram-matrix.

Trace of a module. If K/K' is Galois and $M \subseteq K^m$ is an $\mathcal{O}$-module, we write $\mathrm{Tr}_{K/K'}(M) := \{\mathrm{Tr}_{K/K'}(\mathbf{m}) \,|\, \mathbf{m} \in M\}$, where, as usual, $\mathrm{Tr}_{K/K'}(\mathbf{m})$ is applied coordinate-wise. This is an $\mathcal{O}'$-module, and, if M is G-stable, then $\mathrm{Tr}_{K/K'}(M) \subseteq M^G = M \cap (K')^m$. One can prove that the rank of $\mathrm{Tr}_{K/K'}(M)$ as an $\mathcal{O}'$-module is equal to the rank of M as an $\mathcal{O}$ module, which in turns imply that the rank of M^G (as an $\mathcal{O}'$-module) is the same as the one of M. [16]

Lemma 2.12. *Suppose K/K' is Galois. Let $M \subset \mathcal{O}^m$ be an $\mathcal{O}$-submodule. Suppose M is G-stable. Consider the $\mathcal{O}'$-submodules $\mathrm{Tr}_{K/K'}(M)$ and $M^G \subset (\mathcal{O}')^m$. Then the $\mathcal{O}'$-rank of $\mathrm{Tr}_{K/K'}(M)$ and M^G equals the $\mathcal{O}$-rank of M.*

Proof. Let n be the $\mathcal{O}$-rank of M. By linear algebra, the K-dimension of $K \cdot M^G$ equals the K'-dimension of M^G. Since the former is *a priori* at most the K-dimension of $K \cdot M$, this implies that the rank of M^G is at most n. Moreover, we have the inclusion $\mathrm{Tr}_{K/K'}(M) \subseteq M^G$ by G-stability of M, hence it suffices to prove that the rank of $\mathrm{Tr}_{K/K'}(M)$ is at least n to conclude the proof. Write $G = \{\phi_1, \ldots, \phi_d\}$. Next, choose an arbitrary K'-basis $\{\alpha_1, \ldots, \alpha_d\}$ of K. Let $\mathbf{m} \in M$ and, for $i = 1, \ldots, d$, define $\mathbf{m}_i = \mathrm{Tr}_{K/K'}(\alpha_i \cdot \mathbf{m}) \in M^G$. Note that

$$\mathrm{Tr}_{K/K'}(\alpha_i \cdot \mathbf{m}) = (\phi_1(\alpha_i), \ldots, \phi_d(\alpha_i)) \cdot (\phi_1(\mathbf{m}), \ldots, \phi_d(\mathbf{m}))^T.$$

Consider the $d \times d$-matrix $A := (\phi_j(\alpha_i))_{i,j}$. This matrix is nonsingular (since the discriminant of a basis is nonzero). So it has an inverse, defined over K. Now observe that

$$(\phi_1(\mathbf{m}), \ldots, \phi_d(\mathbf{m}))^T = A^{-1}(\mathbf{m}_1, \ldots, \mathbf{m}_d)^T.$$

Since some ϕ_i is the identity, m is a finite K-linear combination of elements from $\mathrm{Tr}_{K/K'}(M)$, i.e., the m_j's. Thus the K-dimension of $K \cdot \mathrm{Tr}_{K/K'}(M)$ is at least that of $K \cdot M$; the claim follows. □

Contracting and extending modules. If M is a subset of K^m for some $m > 0$, we define $M \cdot O := \{\sum_{i=1}^{r} x_i \mathbf{v}_i \,|\, r > 0, x_i \in \mathcal{O}, \mathbf{v}_i \in M\}$. The most common application of this notation we will use in this article is when M is an $\mathcal{O}'$-module. We will see below that in this case, $M \cdot \mathcal{O}$ lifts M to an $\mathcal{O}$-module, with some nice properties. We will also use the notation with $m = 1$ and $M = I$ a fractional ideal of $\mathcal{O}'$.

The lemma below show some properties on the lift of a module M', and provides a description of a pseudo-basis for the lifted module, given a pseudo-basis of M'.

Lemma 2.13. *Let K/K' be number fields. Let $M' \subset (K')^m$ be an $\mathcal{O}'$-module of rank n. Let $((I'_i, \mathbf{b}'_i))_{1 \le i \le n}$ be a pseudo-basis of M' (with $\mathbf{b}'_i \in (K')^m$ and I'_i fractional $\mathcal{O}'$-ideals). Then $M' \cdot \mathcal{O}$ is an $\mathcal{O}$-module of rank n in K^m and $((\mathbf{b}'_i, I'_i \mathcal{O}_K))_{1 \le i \le n}$ is a pseudo-basis of it.*

[16] This is an adaptation from Lemma 5.8.1 and its proof in [20].

Proof. This follows from the definition of $M' \cdot \mathcal{O}$ and $I'_i \cdot \mathcal{O}$ (see above). □

Corollary 2.14. *Let K/K' be number fields and $M' \subset (K')^m$ be an $\mathcal{O}'$-module of rank n (for some $m \geq n > 0$). Then $\mathrm{disc}_K(M' \cdot \mathcal{O}) = \mathrm{disc}_{K'}(M') \cdot \mathcal{O}$.*

Proof. This follows from Lemma 2.13 and the definition of the discriminant. □

One can also provide a description of a pseudo-basis of the intersection of a module with a subfield, given a pseudo-basis of a module, with special properties.

Lemma 2.15. *Let K/K' be number fields. Let $M \subset K^m$ be a rank-n $\mathcal{O}$-module (for some $m \geq n > 0$). Assume that M admits a pseudo-basis $\{(\mathbf{b}'_i, I_i)\}_{1 \leq i \leq n}$ with the vectors $\mathbf{b}'_i \in (K')^m$ (instead of in K^m), and the $I_i \subset K$ fractional $\mathcal{O}$-ideals (as usual). Then, $M \cap (K')^m$ is a rank-n $\mathcal{O}'$ module and $\{(\mathbf{b}'_i, I_i \cap K')\}_{1 \leq i \leq n}$ is a pseudo-basis of it.*

Proof. Let M' be the rank-n $\mathcal{O}'$ module generated by the pseudo-basis $\{(\mathbf{b}'_i, I_i \cap K')\}_{1 \leq i \leq n}$. We want to prove that $M \cap (K')^m = M'$. The inclusion $M' \subseteq M \cap (K')^m$ follows from the definition. In the other direction, let $\mathbf{v} \in M \cap (K')^m$. Since $\mathbf{v} \in M$, there exist $x_i \in I_i$ for $1 \leq i \leq n$ such that $\mathbf{v} = \sum_i x_i \mathbf{b}'_i$. Recall that the vectors $\mathbf{b}'_i$ are K-linearly independent, and so also K'-linearly independent. This implies that there exists a matrix $\mathbf{M} \in (K')^{n \times m}$ such that $\mathbf{M} \cdot \mathbf{B}' = I_n$, where $\mathbf{B}'$ is the matrix whose columns are the vectors $\mathbf{b}'_i$ and I_n is the identity matrix. Then, $\mathbf{M} \cdot \mathbf{v}$ is the vector $(x_1, \cdots, x_n)^T$. But both $\mathbf{M}$ and $\mathbf{v}$ have their coordinates in K', so all the x_i's are in K'. In other words, $x_i \in I_i \cap K'$, which implies that $\mathbf{v} \in M'$ as desired. □

Contracting and extending ideals. For most of the results presented in this article, we will need to assume that some ideal is unramified in the extension K/K'. The notion of ramified ideal is defined below, with some related properties.

Proposition 2.16 (Ramification Theory of Galois-Extensions). *Suppose K/K' is Galois. Let P' be a prime of $\mathcal{O}'$. Then the set of primes $P_1, \ldots, P_r$ of $\mathcal{O}$ lying above [17] P' is finite and nonempty and the Galois-group G permutes these. Moreover, there is the ideal-factorization $\mathcal{O} \cdot P' = P_1^e \cdot \ldots \cdot P_r^e$, for a positive integer e, the* ramification exponent*.*

The prime P' is said to ramify *in $\mathcal{O}$ if $e > 1$. In this case, each of the P_i 's is said to be* ramified *in $\mathcal{O}$. If $e = 1$ then P' is said* unramified *in $\mathcal{O}$ and each P_i is* unramified *in $\mathcal{O}$. If no prime of $\mathcal{O}'$ ramifies in $\mathcal{O}$, then $\mathcal{O}/\mathcal{O}'$ is* unramified*. The $\mathcal{O}'/P'$-vector spaces $\mathcal{O}/P_i$ have the same finite dimension (*residual degree*) f. Finally, there is the* fundamental identity *that $efr = [K : K']$.*

[17] These are the primes of $\mathcal{O}$ containing P'. It holds that $P_i \cap \mathcal{O}' = P'$. In particular, if P', P'' are two distinct primes of $\mathcal{O}'$ then the respective sets of primes over each are disjoint.

For an integral ideal $I \subseteq \mathcal{O}$ not necessarily prime, we say that I is non-ramified in K/K' if none of its prime factors ramifies in K/K'. For a module $M \subseteq \mathcal{O}^n$ of rank n, we say that M is non-ramified in K/K' if its discriminant ideal $\mathrm{disc}_K(M)$ in non-ramified.

We note that if a prime ideal P ramifies in K/K', then, a fortiori, P ramifies in $K/\mathbb{Q}$. Hence, if an ideal I or a module M is non-ramified in K/K', then it is also non-ramified in K/K' for any subfield K' of K.

The following lemma is a generalization of [3, Lemma 3.3] to the context of general Dedekind ring $\mathcal{O}$ (the result from [3] was restricted to ideals in the ring $\mathcal{O} = \mathcal{O}_K$). The proof of the lemma is similar to the one from [3, Lemma 3.3] and is postponed to Appendix A.

Lemma 2.17. *Suppose K/K' is Galois. Let I be an ideal of $\mathcal{O}$. Suppose that I is not divisible by any ramified prime of $\mathcal{O}$. Then I is G-stable if, and only if, $I = I^G \cdot \mathcal{O}$. In other words, I is G-stable if, and only if, it equals the extension of its contraction.*

Module lattices. In this subsection, we assume that the rings $\mathcal{O} = \mathcal{O}_K$ is the rings of integers of K. In this case, $\sigma_K(\mathcal{O}_K) \subseteq \mathbb{C}^d$ is a rank-d lattice, with $\det(\sigma_K(\mathcal{O}_K)) = \Delta_K^{1/2}$. A similar result holds for modules of rank n in K^n, as stated in the lemma below.

Lemma 2.18. *Let K be a number field of degree d. Let $M \subset K^n$ be a rank n $\mathcal{O}_K$-module. Then $\sigma_K(M) \subset \mathbb{C}^{nd}$ is a rank-(nd) lattice with volume $\det(\sigma_K(M)) = \mathcal{N}_K(\mathrm{disc}_K(M))^{1/2} \cdot \Delta_K^{n/2}$.*

2.4 Computational considerations

In all this article, we always assume that the algorithms are given a representation of the automorphisms of K which allows for efficient evaluation (polynomial in the size of the element of K on which we want to evaluate the automorphism).

Lemma 2.19. *Let K be a number field. There is an algorithm $\mathcal{A}$ that takes as input a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and a pseudo-basis of a rank-n $\mathcal{O}_K$-module $M \subset K^m$ (for some $m \neq n > 0$), and outputs a $\mathbb{Z}$-basis of the lattice $\sigma_{K_M}\big(M \cap (K_M)^m\big)$, where K_M is the decomposition field of M (cf Definition 2.11). Algorithm $\mathcal{A}$ runs in polynomial time in its input size.*

The proof of this lemma is very similar to the proof of Theorem 3.1 in [3], which did it in the ideal case. We provide the proof for modules below, for completeness.

Proof. The algorithm does the following. First, it computes the subgroup H_M of $\mathrm{Aut}_{\mathbb{Q}}(K)$ that stabilize M. To do so, the algorithm computes, from the pseudo-basis of M and the $\mathbb{Z}$-basis $\mathbf{B}_K$ of $\mathcal{O}_K$, a $\mathbb{Z}$-basis $\{\mathbf{m}_1, \ldots, \mathbf{m}_{nd}\}$ of M. To test if an automorphism ϕ of K stabilizes M, it then suffices to check that $\phi(\mathbf{m}_i) \in M$ for all i's. If this is the case, then for any $\mathbf{m} = \sum x_i \mathbf{m}_i$ in M ($x_i \in \mathbb{Z}$), it holds that $\phi(\mathbf{m}) = \sum x_i \phi(\mathbf{m}_i)$ since ϕ is $\mathbb{Q}$-linear, and so we have $\phi(M) \subseteq M$. We can then test equality by performing the same test with ϕ^{-1}. Since we assumed that we can efficiently evaluate all the automorphisms of K, this first computation can be performed in polynomial time.

Once we have H_M, we can compute a basis of K_M by linear algebra (see more details in [3, proof of theorem 3.1]). Observe then that $\sigma_K(M \cap (K_M)^m)$ is the intersection of the lattice $\sigma_K(M)$ with the subspace $\sigma_K((K_M)^m)$, and we have a basis of both the lattice and the subspace (a $\mathbb{Z}$-basis of $\sigma_K(M)$ can be efficiently computed from the pseudo-basis of M and the $\mathbb{Z}$-basis of $\mathcal{O}_K$). Computing a basis over $\mathbb{Z}$ of the intersection can then be performed in polynomial time using, e.g., [3, Lemma A.1]. To obtain a basis of $\sigma_{K'}(M \cap (K_M)^m)$, it then suffices to discard the redundant coordinates. □

3 Solving approximate-SVP via the trace map

In this section, we prove the following theorem.

Theorem 3.1. *Let K/K' be a Galois extension of number fields of respective degrees d and d', $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ be their respective rings of integers, and G be the Galois group. Let $m \geq n > 0$ and $M \subset K^m$ be an $\mathcal{O}_K$-module of rank n which is G-stable (see Definition 2.10). Then,*

$$\mathrm{Tr}_{K/K'}(M) \subseteq M \cap (K')^m$$

is an $\mathcal{O}_{K'}$ module of rank n and

$$\lambda_1\big(\sigma_{K'}(\mathrm{Tr}_{K/K'}(M))\big) \leq \sqrt{d/d'} \cdot \delta_{K/K'} \cdot \lambda_1\big(\sigma_K(M)\big),$$

where $\delta_{K/K'}$ is as in Definition 2.7.

This theorem leads to Corollary 3.2.

Corollary 3.2. *Let K be a number field of degree d and $\mathcal{O}_K$ be its ring of integers. There is an algorithm that takes as input a $\mathbb{Z}$-basis $\mathbf{B}_K$ of $\mathcal{O}_K$, a pseudo-basis $\mathbf{B}_M$ of an $\mathcal{O}_K$-module $M \subset K^m$ of rank n (for some $m \geq n > 0$) and a parameter $\gamma \geq 1$, and solves γ'-SVP in $\sigma_K(M)$ for $\gamma' = d_M \cdot \delta_{K/\mathbb{Q}} \cdot \gamma$ in time*

$$\mathrm{poly}(\textit{input size}) \cdot 2^{O\left(\frac{nd \cdot \log(nd)}{d_M \cdot \log \gamma}\right)},$$

where $d_M = |\{\phi \in \mathrm{Aut}_{\mathbb{Q}}(K) \mid \phi(M) = M\}|$ is the number of automorphisms of K fixing M as a set.

Note that Theorem 3.1 and Corollary 3.2 can be applied to ideals (as rank-1 $\mathcal{O}_K$-modules) without additional restriction such as not being ramified, contrary to previous results such as in [3,19].

Proof (Proof of Corollary 3.2). Let H_M be the set of automorphisms fixing M as a set and $K' = K_M$ its decomposition field (see Definition 2.11). Then, K/K' is Galois, and has Galois group $G = H_M$. By definition of H_M, the module M is G-stable.

By Lemma 2.12, we have that $M^G = M \cap (K')^m$ is a rank-n $\mathcal{O}_{K'}$-module. Moreover, by Theorem 3.1, we have $\mathrm{Tr}_{K/K'}(M) \subseteq M^G$, and so $\lambda_1\big(\sigma_{K'}(M^G)\big) \leq \sqrt{d/d'} \cdot \delta_{K/K'} \cdot \lambda_1(\sigma_K(M))$.

The algorithm from the corollary then goes as follows: it first computes a $\mathbb{Z}$-basis of the lattice $L = \sigma_{K'}(M^G)$ of rank $d'n$, using Lemma 2.19. This can be done in polynomial time. Then, the algorithm runs the BKZ algorithm from Lemma 2.2 with parameter γ and returns the vector $\mathbf{s} \in M^G$ output by BKZ. This requires time $\mathrm{poly}(\text{input size}) \cdot 2^{O((nd')\log(nd')/\log(\gamma))}$, where d' is the degree of K', i.e., $d' = d/d_M$.

The running time of the algorithm follows from the explanations given above: everything is polynomial in the input size, except the BKZ call. Regarding correctness, we know from Lemma 2.2 and the discussion above, that $\mathbf{s}$ is non-zero and satisfies

$$\|\sigma_{K'}(\mathbf{s})\| \leq \gamma \cdot \lambda_1\big(\sigma_{K'}(M^G)\big) \leq \sqrt{d/d'} \cdot \delta_{K/K'} \cdot \gamma \cdot \lambda_1\big(\sigma_K(M)\big).$$

We conclude from the definition of $\gamma' = d/d' \cdot \delta_{K/K'} \cdot \gamma$ and using Lemma 2.5 that $\|\sigma_K(\mathbf{s})\| \leq \gamma' \cdot \lambda_1\big(\sigma_K(M)\big)$. □

Proof (Proof of Theorem 3.1). The fact that $\mathrm{Tr}_{K/K'}(M) \subseteq M$ follows from the G-stability of M and the definition of the trace. The fact that $\mathrm{Tr}_{K/K'}(M)$ is an $\mathcal{O}_{K'}$-module of rank n follows from Lemma 2.12.

Let $\mathbf{v} \in M$ be a non-zero vector of M reaching the minimal euclidean norm, i.e., $\|\sigma_K(\mathbf{v})\| = \lambda_1(\sigma_K(M))$. Let $\alpha_1, \cdots, \alpha_{d/d'}$ be a set of K'-linearly independent vectors in $\mathcal{O}_K$ with $\|\sigma_K(\alpha_i)\|_\infty \leq \delta_{K/K'}$ for all i (such vectors exist by definition of $\delta_{K/K'}$). Define $\mathbf{w}_i = \alpha_i \cdot \mathbf{v}$ for $i = 1$ to d/d'.

Note that at least one of the $\mathbf{w}_i$ satisfies $\mathrm{Tr}_{K/K'}(\mathbf{w}_i) \neq 0$. Indeed, if we had $\mathrm{Tr}_{K/K'}(\mathbf{w}_i) = 0$ for all i's, then we would have $\mathrm{Tr}_{K/K'}(x \cdot \mathbf{v}) = 0$ for all $x \in K$ (since the α_i's form a K'-basis of K and $\mathrm{Tr}_{K/K'}$ is K'-linear), which implies $\mathbf{v} = 0$ by non-degeneracy of the trace map (applied to each coordinate). This is impossible by definition of $\mathbf{v}$.

Let us then fix i such that $\mathrm{Tr}_{K/K'}(\mathbf{w}_i) \neq 0$. Since $\alpha_i \in \mathcal{O}_K$, we have $\mathbf{w}_i \in M$ and so $\mathrm{Tr}_{K/K'}(\mathbf{w}_i) \in \mathrm{Tr}_{K/K'}(M) \setminus \{0\}$. It only remains to upper bound its euclidean norm. By definition of $\mathbf{w}_i$, we have that $\|\sigma_K(\mathbf{w}_i)\| \leq \|\sigma_K(\alpha_i)\|_\infty \cdot \|\sigma_K(\mathbf{v})\| \leq \delta_{K/K'} \cdot \lambda_1(\sigma_K(M))$. By Lemma 2.6, this, in turns, implies that $\|\sigma_{K'}(\mathrm{Tr}_{K/K'}(\mathbf{w}_i))\| \leq \sqrt{d/d'} \cdot \delta_{K/K'} \cdot \lambda_1(\sigma_K(M))$, as required. □

4 Solving Hermite SVP without loss in the approximation factor

In the previous section, we have seen that if a module M is stabilized by a certain number of field automorphisms, then one can reduce the problem of solving SVP in M to the problem of solving SVP in $M \cap (K_M)^m$, which is a module in a field of smaller degree than M. One drawback of this reduction however is that it does not preserve the approximation factor. As a consequence, this provides an algorithm for SVP in M only for approximation factors larger than some lower bound $d_M \cdot \lambda_d^\infty(\sigma_K(\mathcal{O}_K))$ (where d_M is the dimension of K over K_M: the more we gain in dimension, the larger the loss in the approximation factor).

In this section, we present a more evolved analysis that shows that if M is G-stable, if it has maximal rank n in K^n and if its discriminant satisfies some condition,[18] then one can reduce the problem of solving HSVP in M into solving HSVP in $M \cap (K_M)^m$, without any loss on the approximation factor. This result is the analogous of the results from [3, Section 3] for modules instead of ideals.

The core of our proof is captured by the following proposition, which is the analogous of [3, Lemma 3.3] for modules instead of ideals.

Proposition 4.1. *Let K/K' be a Galois extension of number fields, with Galois group G, and let $\mathcal{O}_K$ be the ring of integers of K. Let $M \subseteq (\mathcal{O}_K)^n$ be a rank n module (for some $n > 0$) whose discriminant $\mathrm{disc}_K(M)$ is not divisible by a ramified prime. Then, M is G-stable if, and only if, $M^G \cdot \mathcal{O}_K = M$.*

The proof of this proposition will be the focus of the next section (where we will give two different proofs). In this section, we simply explain how to obtain our main result from it. Namely, we prove the following theorem (which is the generalization to modules of [3, Theorem 3.2]).

Theorem 4.2. *Let K be a number field and $M \subseteq (\mathcal{O}_K)^n$ be a rank n module (for some $n > 0$) whose discriminant $\mathrm{disc}_K(M)$ is not divisible by any ramified prime ideal of $\mathcal{O}_K$. Let K_M be the decomposition field of M (see Definition 2.11), and $d_M = [K : K_M]$. Let $\gamma \geq 1$.*

Then any $\mathbf{v} \in M \cap (K_M)^n$, which is a solution to γ-HSVP in $\sigma_{K_M}(M \cap (K_M)^n)$ (via σ_{K_M}) is also a solution to γ-HSVP in $\sigma_K(M)$ (via σ_K).

Note that in our statement above, we have no loss in the approximation factor γ, whereas [3, Theorem 3.3] had a loss $\sqrt{d_M}$. This is due to the fact that our definition of Hermite-SVP differs from the one in [3]: we chose to compare the length of our short vector with $\sqrt{n} \cdot \det(L)^{1/n}$ (where L is a lattice of rank n), when [3] chose to compare it with $\det(L)^{1/n}$. The Gaussian heuristic claims that, up to a constant factor, the length of a shortest vector of a lattice is expected

[18] Note that these two last conditions were not needed in the previous section.

to be roughly equal to $\sqrt{n} \cdot \det(L)^{1/n}$, which is why we changed our definition of Hermite-SVP compared to [3].

The proof of this Theorem is very similar to the proofs of [17, Theorem 4] and [3, Theorem 3.2].

Proof. Let us write d the degree of K, $K' = K_M$, d' the degree of K', G the Galois group of K/K' and $M^G = M \cap (K')^n$. Let $\mathbf{v} \in M^G$ be a solution to γ-HSVP in $\sigma_{K'}(M^G)$, i.e., $\|\sigma_{K'}(\mathbf{v})\| \leq \gamma \cdot \sqrt{nd'} \cdot \det(\sigma_{K'}(M^G))^{1/(nd')}$. The vector $\mathbf{v}$ is non-zero by definition, and belongs to M since $M^G \subseteq M$. Moreover, by Lemma 2.5, we know that $\|\sigma_K(\mathbf{v})\| = \sqrt{d/d'} \cdot \|\sigma_{K'}(\mathbf{v})\|$, which, together with the assumption on $\mathbf{v}$, implies that

$$\|\sigma_K(\mathbf{v})\| \leq \gamma \cdot \sqrt{nd} \cdot \det(\sigma_{K'}(M^G))^{1/(nd')}.$$

To conclude the proofs, it hence suffices to prove that $\det(\sigma_{K'}(M^G))^{1/(nd')} \leq \det(\sigma_K(M))^{1/(nd)}$.

To prove this, we rely on the fact K/K' is Galois (see Lemma 2.3), that M is G-stable by choice of G, and that the discriminant of M does not contain any ramified prime factors in $K/\mathbb{Q}$ and so, a fortiori, does not contain any ramified prime factors in K/K'. Hence, we can apply Proposition 4.1, and we know that $M = M^G \cdot \mathcal{O}_K$.

By Corollary 2.14, we know that $\mathrm{disc}_{K'}(M^G) \cdot \mathcal{O}_K = \mathrm{disc}_K(M^G \cdot \mathcal{O}_K) = \mathrm{disc}_K(M)$, which implies that $\mathcal{N}_K(\mathrm{disc}_K(M)) = \mathcal{N}_K(\mathrm{disc}_{K'}(M^G) \cdot \mathcal{O}_K) = \mathcal{N}_{K'}(\mathrm{disc}_{K'}(M^G))^{d/d'}$. By Lemma 2.18, we have that

$$\begin{aligned}
\det(\sigma_K(M))^{1/(nd)} &= \left(\mathcal{N}_K(\mathrm{disc}_K(M)) \cdot \Delta_K^{n/2}\right)^{1/(nd)} \\
&= \left(\mathcal{N}_{K'}(\mathrm{disc}_{K'}(M^G))^{d/d'} \cdot \Delta_K^{n/2}\right)^{1/(nd)} \\
&= \left(\mathcal{N}_{K'}(\mathrm{disc}_{K'}(M^G)) \cdot \Delta_{K'}^{n/2}\right)^{1/(nd')} \cdot \frac{\Delta_K^{1/(2d)}}{\Delta_{K'}^{1/(2d')}} \\
&\geq \det(\sigma_{K'}(M^G))^{1/(nd')},
\end{aligned}$$

where we used in the last inequality the fact that $\Delta_K^{1/d} \geq \Delta_{K'}^{1/d'}$ (see preliminaries). □

From this Theorem, we finally obtain Corollary 4.3 below (this is the generalization to modules of [3, Theorem 3.1]).

Corollary 4.3. *There is an algorithm that takes as input a $\mathbb{Z}$-basis $\mathbf{B}_K$ of $\mathcal{O}_K$, a pseudo-basis $\mathbf{B}_M$ of an $\mathcal{O}_K$-module $M \subset (\mathcal{O}_K)^n$ of rank n (for some $n > 0$) whose discriminant is non-ramified, and a parameter $\gamma \geq 1$, and solves γ-HSVP in $\sigma_K(M)$ in time*

$$\mathrm{poly}(\textit{input size}) \cdot 2^{O\left(\frac{nd \cdot \log(nd)}{d_M \cdot \log \gamma}\right)},$$

where $d_M = |\{\phi \in \mathrm{Aut}_{\mathbb{Q}}(K) \mid \phi(M) = M\}|$ is the number of automorphisms of K fixing M as a set.

Proof. The algorithm is the same as the one from Corollary 3.2. It computes a pseudo-basis of $M \cap (K_M)^n$ and a $\mathbb{Z}$-basis of $\mathcal{O}_{K_M}$ (where K_M is the decomposition field of M), using Lemma 2.19. Then it solves HSVP in $M \cap (K_M)^n$ with approximation factor γ using the algorithm from Lemma 2.2 on the lattice $\sigma_{K_M}(M \cap (K_M)^n)$ The running time of the algorithm follows from Lemmas 2.19 and 2.2. The correctness follows from Lemma 2.2, from the fact that a solution to γ-SVP in any lattice L is also a solution to γ-HSVP in L, and from Theorem 4.2. □

5 Contracting then extending a module

In this section, we prove the core result of our article, namely Proposition 4.1, which we recall below.

Proposition (Proposition 4.1). *Let K/K' be a Galois extension of number fields, with Galois group G, and let $\mathcal{O}_K$ be the ring of integers of K. Let $M \subseteq (\mathcal{O}_K)^n$ be a rank n module (for some $n > 0$) whose discriminant $\mathrm{disc}_K(M)$ is not divisible by any prime ideal that ramifies in K/K'. Then, M is G-stable if and only if $M^G \cdot \mathcal{O}_K = M$.*

We propose two proofs of this proposition, one using the HNF basis of the module, and one using localization. The proof using the HNF basis requires only simple mathematical objects (or, at least, objects that have been frequently used in cryptography over the past few years), but may not be very enlightening from a mathematical point of view. The proof using localization on the other hand is very natural from a mathematical point of view, but requires some mathematical notions that are less commonly seen in a cryptographic context. We recall the necessary mathematical notions in Section 5.2, before the proof. Additionally, we also provide a third proof of a more general result, which implies Proposition 4.1, using yet another approach (in this third proof, we use projectivity of the modules). We postpone this proof to Appendix B.

Before going to the proofs, let us observe that one direction of the equivalence stated in Proposition 4.1 can be obtained easily, hence, only one direction needs to be proven in the next subsections.

Lemma 5.1. *Keep the notations from Proposition 4.1. If $M^G \cdot \mathcal{O}_K = M$ then M is G-stable.*

Proof. Define $M' = M^G$. This is an $\mathcal{O}_{K'}$-module in $(K')^n$. Let $\mathbf{m} = \sum_i x_i \mathbf{m}'_i$ be a vector of M, where $x_i \in \mathcal{O}_K$ and $\mathbf{m}'_i \in M'$. Let $\phi \in G$. Then $\phi(\mathbf{m}) = \sum_i \phi(x_i)\mathbf{m}'_i \in M$, where we used the fact that ϕ is the identity on K' and $M' \subset (K')^n$. This implies that $\phi(M) \subseteq M$ for all $\phi \in G$, and so M is G-stable as desired. □

5.1 Proof using the HNF

We start by proving the following lemma.

Lemma 5.2. *Consider K/K' a Galois extension of number fields with Galois group G, together with $M \subseteq (\mathcal{O}_K)^n$ an $\mathcal{O}_K$-module of rank n. If M is G-stable and $\mathrm{Tr}_{K/K'}(\mathcal{O}_K) \cdot \mathcal{O}_K$ is coprime with the discriminant $\mathrm{disc}_K(M)$, then there exists a pseudo-basis $((I_k, \mathbf{b}_k))_{1 \leq k \leq n}$ of M such that $\mathbf{b}_k \in (K')^n$, $\det_K(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{O}_{K'}$, and $I_k \subseteq \mathcal{O}_K$ is G-stable.*

Proof. Consider the Hermite Normal Form of M (see preliminaries), i.e., a pseudo-basis $((I_k, \mathbf{b}_k))_{k \in [\![1,n]\!]}$ such that the matrix $\mathrm{Mat}_K(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ formed by concatenating the column vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is of the form

$$\begin{bmatrix} 1 & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ 0 & & \ddots & * \\ & \ddots & & \\ 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Then it is easy to see that $M \subseteq (\mathcal{O}_K)^n$ implies that for each $k \in [\![1, n]\!]$ the ideal I_k is integral. Let us show that it is also G-stable.

Fix $k \in [\![1, r]\!]$, $\phi \in G$ and $x \in I_k$. Then $\phi(x\mathbf{b}_k) \in M$ since M is stable under the action of G thus we get $\phi(x\mathbf{b}_k) = \sum_{i=1}^{n} x_i b_i$ with $x_i \in I_i$ for any $i \in [\![1, n]\!]$. Considering the triangular shape of the matrix $\mathrm{Mat}_K(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, one can conclude that $\forall i > k, x_i = 0$. Moreover if one focuses on the k-th coefficient of $\phi(x\mathbf{b}_k)$, one has $\phi(x) = x_k \in I_k$. This is true for any $\phi \in G$ and any $x \in I_k$, thus I_k is G-stable, and this holds for any $k \in [\![1, n]\!]$.

Before moving on, let us observe that since $\mathrm{Mat}_K(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is triangular with 1's on the diagonal, and by definition of the discriminant of M, it holds that $\mathrm{disc}_K(M) = \prod_{k=1}^{n} I_k^2$. In particular, since $\mathrm{disc}_K(M)$ is coprime with $\mathrm{Tr}_{K/K'}(\mathcal{O}_K) \cdot \mathcal{O}_K$ by assumption, then we also have that I_k is coprime with $\mathrm{Tr}_{K/K'}(\mathcal{O}_K)\mathcal{O}_K$ for all k's. This implies that for each k, there exist some elements $\alpha_k \in \mathcal{O}_K$ and $\beta_k \in I_k$ such that $\mathrm{Tr}_{K/K'}(\alpha_k) = 1 + \beta_k$.[19] We will use these elements later in the proof.

Next, we prove that one can always choose $\mathbf{b}_k$ to be a vector with coefficients in K', for any $k \in [\![1, n]\!]$. Let us prove this property by induction on k. It is clearly true for $k = 1$ (since $1 \in K'$). Assume it to be true for a given $k \geqslant 1$. For the time being, let us write z_i the non-zero coefficients of $\mathbf{b}_{k+1}$ for $i \leqslant k$. Our goal is to prove that each z_i can be replace by $y_{i,k+1} \in K'$. Let us proceed by decreasing induction on $i \leqslant k$. For a given $x \in I_{k+1}$ and $\phi \in G$, the vector

[19] Here we actually use the coprimality of $\mathrm{Tr}_{K/K'}(\mathcal{O}_K)$ with $I_k \cap \mathcal{O}_{K'}$, which is implied by the coprimality of $\mathrm{Tr}_{K/K'}(\mathcal{O}_K)\mathcal{O}_K$ and I_k.

$\phi(x\mathbf{b}_{k+1})$ belongs to M so as before one can write :

$$\phi(x\mathbf{b}_{k+1}) = \sum_{i=1}^{k} x_i \mathbf{b}_i + \phi(x)\mathbf{b}_{k+1}, \tag{1}$$

and the k-th coordinate gives $\phi(xz_k) = x_k + \phi(x)z_k$, which leads to $\phi(x)(z_k - \phi(z_k)) = -x_k \in I_k$. This is true for any $x \in I_{k+1}$ hence we have $\phi(I_{k+1}) \cdot (z_k - \phi(z_k)) \subseteq I_k$. Since I_{k+1} is G-stable, this is equivalent to $I_{k+1} \cdot (z_k - \phi(z_k)) \subseteq I_k$, i.e., $(z_k - \phi(z_k)) \in I_k \cdot I_{k+1}^{-1}$. Let α_k be as above, i.e., $\mathrm{Tr}_{K/K'}(\alpha_k) = 1 + \beta_k$ for some $\beta_k \in I_k$. Since $I_k \cdot I_{k+1}^{-1}$ is an ideal and $\phi(\alpha_k) \in \mathcal{O}_K$ (because $\alpha_k \in \mathcal{O}_K$, it holds that $\phi(\alpha_k) \cdot (z_k - \phi(z_k)) \in I_k \cdot I_{k+1}^{-1}$. Summing over all $\phi \in G$ gives

$$\mathrm{Tr}_{K/K'}(\alpha_k) \cdot z_k - \mathrm{Tr}_{K/K'}(\alpha_k \cdot z_k) \in I_k \cdot I_{k+1}^{-1}.$$

Recall that $\mathrm{Tr}_{K/K'}(\alpha_k) = 1 + \beta_k$ with $\beta_k \in I_k$. Observe also that $z_k \in I_{k+1}^{-1}$ since $\mathbf{b}_{k+1} \cdot I_{k+1} \subset (\mathcal{O}_K)^n$ (recall that M is integral). Hence, $\beta_k \cdot z_k \in I_k \cdot I_{k+1}^{-1}$ and the equation above can be rewritten

$$z_k - \mathrm{Tr}_{K/K'}(\alpha_k \cdot z_k) \in I_k \cdot I_{k+1}^{-1}.$$

Therefore, we can replace $\mathbf{b}_{k+1}$ by $\mathbf{b}'_{k+1} := \mathbf{b}_{k+1} + (\mathrm{Tr}_{K/K'}(\alpha_k z_k) - z_k) \cdot \mathbf{b}_k$ (which is still a pseudo-basis of M), which ensure that the new coefficient z'_k of $\mathbf{b}'_k$ is equal to $\mathrm{Tr}_{K/K'}(\alpha_k z_k) \in K'$.

Let us now write $y_{k,k+1}$ this element. Now fix $2 \leqslant i \leqslant k$ and assume the following: $\forall j \geqslant i, z_j = y_{j,k+1} \in K'$. We will prove that we can replace z_{i-1} by an element of K'. Consider again $x \in I_{k+1}$ and $\phi \in G$. We will use Equation (1) again. For now, assume the following:

$$\forall j \in [\![i, k]\!], x_j = 0. \tag{$*$}$$

We can now consider the $(i-1)$-th coordinate in Equation (1) which gives $\phi(x)\phi(z_{i-1}) = x_{i-1} + \phi(x)z_{i-1}$, using ($*$). We see that we are in the same situation as before, replacing k by $i-1$. Thus, the same steps lead to $z_{i-1} - \mathrm{Tr}_{K/K'}(\alpha_{i-1}z_{i-1}) \in I_{i-1}I_{k+1}^{-1}$, thus one can replace z_{i-1} by $y_{i-1,k+1} := \mathrm{Tr}_{K/K'}(\alpha_{i-1}z_{i-1})$. This ends our proof by induction.

We are left with proving ($*$). We will again show this by induction. The k-th coordinate of Equation (1) gives $\phi(xy_{k,k+1}) = \phi(x)y_{k,k+1} = x_k + \phi(x)y_{k,k+1}$, using the fact that $\phi(y_{k,k+1}) = y_{k,k+1}$. Thus, we have $x_k = 0$. Now assume that $x_k = x_{k-1} = \cdots = x_j = 0$ for some fixed $j \in [\![i, k]\!]$. The $(j-1)$-th coordinate in Equation (1) gives $\phi(x)\phi(y_{j-1,k+1}) = \phi(x)y_{j-1,k+1} = \sum_{l=j-1}^{k} x_l y_{j-1,l} + \phi(x)y_{k+1,l}$. By induction hypothesis we have $\phi(x)y_{j-1,k+1} = x_{j-1} + \phi(x)y_{k+1,l}$, so $x_{j-1} = 0$.

Summing up, we have proven that the vectors $\mathbf{b}_k$ of the HNF basis can always be chosen to live in $(K')^n$. It remains to prove that $\det(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{O}_{K'}$. This follows from the fact that the matrix $\mathrm{Mat}_K(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is triangular with 1's on the diagonal, so its determinant is $1 \in \mathcal{O}_{K'}$. □

Proof (Proof of Proposition 4.1). We know that $\mathrm{Tr}_{K/K'}(\mathcal{O}_K) \cdot \mathcal{O}_K$ is divided only by ramified prime ideals. Hence, if the discriminant of M is non-ramified, then it should be coprime with $\mathrm{Tr}_{K/K'}(\mathcal{O}_K) \cdot \mathcal{O}_K$. Applying Lemma 5.2, we know that there exists a pseudo-basis $((\mathbf{b}_k, I_k))_{1 \le k \le n}$ of M where the vectors $\mathbf{b}_k$ live in $(K')^n$, the ideals $I_k \subseteq \mathcal{O}_K$ are integral and are G-stable, and $\det(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is in $\mathcal{O}_{K'}$. We first remark since $\det(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{O}_K$ and the ideals I_k are integral, then each ideal I_k divides the discriminant of M (by definition of the discriminant), and so is unramified by assumption.

Using Lemmas 2.15 and 2.13 from preliminaries, we then see that $((\mathbf{b}_k, I_k^G \cdot \mathcal{O}_K))_{1 \le k \le n}$ is a pseudo-basis of $M^G \cdot \mathcal{O}_K$. Since the ideals I_k are G-stable, integral and unramified, we know from Lemma 2.17 that $I_k^G \cdot \mathcal{O}_K = I_k$ for all k. This implies that $M^G \cdot \mathcal{O}_K = M$ as desired. □

5.2 Proof using the localization

Localization. Perhaps the most basic fact about the kind of modules we consider [20] is that these are *locally-free*, i.e., after localizing to a prime, they become finite free over a PID; a well-understood class which is perhaps the "simplest" after vector spaces. Therefore, it is only natural to study our problem from this perspective. An important consequence of this local-freeness is *projectivity*; this enables direct sum decompositions and we will exploit this as well. We elaborate below.

Let R be a commutative domain and let P be a prime ideal of R. Define the multiplicative set $S := R - P$. The local ring at P, denoted R_P, is the ring of fractions $S^{-1} \cdot R$. The ring R is naturally embedded into R_P (via $r \mapsto r/1$) and the latter is, in turn, naturally embedded into the field K of fractions of R. Note that K is the special case with $P = (0)$. If I is an ideal of R, then its image I_P (which equals $I \cdot R_P$) in R_P is the unit-ideal (i.e., all of R_P) if and only if $I \cap S \neq \emptyset$ ("I meets S"). In particular, the prime ideals of R_P are precisely the images of the prime ideals of R contained in P (which include P itself, of course). Thus, R_P has a single maximal ideal, namely $P \cdot R_P$.

In the rest of this section, we let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers of a number field K (recall that this is a Dedekind domain). Since its prime ideals P are maximal, $\mathcal{O}_P$ has $P \cdot \mathcal{O}_P$ as its single prime ideal. Moreover, $\mathcal{O}_P$ inherits the Dedekind property. So when considering a nonzero ideal I of $\mathcal{O}$ and its Dedekind factorization, taking the image means "stripping off" the contributions of all primes other than P, while leaving P (and its exponent) intact. Since $\mathcal{O}_P$ is actually a DVR (thus, in particular, a PID), the image of P^k thus becomes a principal ideal $(t)^k$ where t is a prime element of $\mathcal{O}_P$. Because of this "preservation property" this often opens the way to "separation of concerns" by focusing on one prime at a time. Since $\mathcal{O}_P$ has a simpler structure, a problem often becomes easier in the process.

[20] finitely generated, torsion-free, over $\mathcal{O}_K$

We now describe a *variation* that is particularly useful to us. Let P' be a nonzero prime ideal of $\mathcal{O}'$ (where $\mathcal{O}' = \mathcal{O}_{K'}$ is the ring of integers of a subfield K' of K). Then define the multiplicative set $S' := \mathcal{O}' - P'$, and the ring $\mathcal{O}_{P'} := (S')^{-1} \cdot \mathcal{O}$, which is naturally embedded in K. So this is a variation in the sense that we "localize $\mathcal{O}$ to a prime of $\mathcal{O}'$." That said, $\mathcal{O}'_{P'}$ – as defined previously – is naturally a subring of $\mathcal{O}_{P'}$. But more is true. First, $\mathcal{O}_{P'}$ only has finitely many primes, namely the images of the primes of $\mathcal{O}$ *above* P'. Since Dedekind domains with only finitely many prime ideals are PIDs, $\mathcal{O}_{P'}$ is a PID (thus, in particular, a Dedekind domain). The image in $\mathcal{O}_{P'}$ of a nonzero ideal I of $\mathcal{O}$ is then obtained by stripping off the contributions in I of primes of $\mathcal{O}$ that are *not* above P', and to leave the rest (including exponents) intact. Again, such image becomes principal in $\mathcal{O}_{P'}$. Second, $\mathcal{O}_{P'}$ is the integral closure of $\mathcal{O}'_{P'}$ in K. Note $\mathcal{O}_{P'} \cap K' = \mathcal{O}'_{P'}$. Moreover, if K/K' is Galois, then $\mathcal{O}_{P'}$ is G-stable since $S \subset \mathcal{O}'$ (so we may view $(\mathcal{O}_{P'})^n$ as an $\mathcal{O}'_{P'}[G]$-module). Finally, we note again that the residue class field of $\mathcal{O}'_{P'}$ (i.e., the field obtained by modding out the maximal ideal) is isomorphic to $\mathcal{O}'/P'$. In summary, given $\mathcal{O}/\mathcal{O}'$ as defined in our setting, then its local version $\mathcal{O}_{P'}/\mathcal{O}'_{P'}$ also fits with our setting and so we may pass to it whenever convenient.

Finally, if P is a prime of $\mathcal{O}$, $S = S(P) = \mathcal{O} - P$, and $M \subset \mathcal{O}^n$ is an $\mathcal{O}$-submodule, then $M_P := S^{-1} \cdot M \subset \mathcal{O}_P^n$ is just $M \cdot \mathcal{O}_P$, i.e., it contains all finite $\mathcal{O}_P$-linear combinations of elements from M. We sometimes call this *extension by* $\mathcal{O}_P$ of an $\mathcal{O}$-module. Note that, by clearing denominators, each element is indeed of the form m/s with $m \in M$ and $s \in S(P)$, so this is consistent with the definition from Section 2.3. Rank clearly does not change in the process (since $\mathcal{O}_P$ has the same quotient field as $\mathcal{O}$). If M has maximal rank, then M_P is free of maximal rank over the PID (DVR) $\mathcal{O}_P$. Moreover, by inspection of the discriminant definition, $\mathrm{disc}_K(M_P) = \mathrm{disc}_K(M)_P$, i.e., *localization and taking discriminant commute*. Similarly for the version where P' is a prime of $\mathcal{O}'$ and we consider extension by $\mathcal{O}_{P'}$ instead.

Remark 5.3 (Notation). Whenever applicable, the discriminant of an $\mathcal{O}$-module $M \subset \mathcal{O}^n$ is denoted by $\mathrm{disc}_K(M)$, and that of an $\mathcal{O}'$-module M' by $\mathrm{disc}_{K'}(M')$, so as to mark the difference of whether it "lives upstairs or downstairs." Similarly for localized modules.

Some auxiliary lemmas. A fundamental lemma is key to simplifications: [21]

Lemma 5.4. *Let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers of a number field K. Let M, N be $\mathcal{O}$-modules. Then $M \subset N$ if $M_P \subset N_P$ for all primes P of $\mathcal{O}$. Thus, $M = N$ if M, N are locally everywhere identical.*

Proof. Let $x \in M$. Since $M \subset M_P$, there are $y = y(P) \in N$, $s = s(P) \in \mathcal{O} - P$ such that $x = y/s$. The $\mathcal{O}$-ideal generated by these $s(P)$ is the unit ideal; if

[21] This is Ch. I, Proposition 18 in [11].

not, it would be contained in some prime Q and we have the contradiction that $s(Q)$ is not included in it. Ideals of $\mathcal{O}$ are finitely generated so there are values $\mu = \mu(P) \in \mathcal{O}$, all but finitely many zero, such that $\sum_P \mu(P) \cdot s(P) = 1$. But now $x = \sum_P \mu(P) \cdot s(P) \cdot x = \sum_P \mu(P) \cdot y(P)$. Thus $x \in N$. □

Towards Proposition 4.1, in our relative setting $\mathcal{O}/\mathcal{O}'$, we apply this lemma to $\mathcal{O}$-modules in two ways: just as above, with $S = \mathcal{O} - P$ (P a prime of $\mathcal{O}$) and with $S' = \mathcal{O}' - P'$ (P' a prime of $\mathcal{O}'$). To see that the lemma also applies to the latter is trivial; just verbatim substitution in its proof. In the sequel, a module becomes a free module of the same rank after localization (since the rings become PIDs). We then apply some basic facts of theory of free modules over PID. These can be extracted from Section 2.3.

Lemma 5.5. *Suppose K/K' is Galois. Let $M \subset \mathcal{O}^n$ be an $\mathcal{O}$-submodule of maximal rank n. Suppose M is G-stable. Then $\mathrm{disc}_K(M)$ is G-stable. Let P' be a prime of $\mathcal{O}'$ and let Q the product of the distinct primes of $\mathcal{O}$ lying above it. If $P' \mid \mathrm{disc}_{K'}(M^G)$, then $Q \mid \mathrm{disc}_K(M)$.*

Proof. The G-stability of $\mathrm{disc}_K(M)$ follows easily from the definition of discriminant, taking G-stability of M into account[22]. By Lemma 2.12, $\mathrm{disc}_{K'}(M^G)$ is well-defined. By G-stability, all of P''s conjugates divide $\mathrm{disc}_K(M)$ or none (see Proposition 2.16). Suppose the latter, towards a contradiction. Then $\mathrm{disc}_K(M_{P'})$ is the unit-ideal, and, hence, $M_{P'} = (\mathcal{O}_{P'})^n$. But P' divides $\mathrm{disc}_{K'}(M^G)$ by assumption. Therefore, the free n-dimensional $\mathcal{O}'_{P'}$-module $(M^G)_{P'}$ is a *proper* submodule of $(\mathcal{O}'_{P'})^n$. Since $S'(P')$ is G-stable (because $S'(P') \subset \mathcal{O}'$), we see that $(M^G)_{P'} = (M_{P'})^G$. Thus, there is the contradiction $(M^G)_{P'} = (M_{P'})^G = ((\mathcal{O}_{P'})^n)^G = (\mathcal{O}'_{P'})^n$. □

The following lemma proves that Proposition 4.1 holds in most of the localized rings $\mathcal{O}_{P'}$ (the ones corresponding to unramified primes P'). The proof in these rings is easier than in $\mathcal{O}_K$ since they are principal.

Lemma 5.6. *Suppose K/K' is Galois. Let $P' \subseteq \mathcal{O}'$ be a prime ideal that does not ramify in K/K'. Then $\mathcal{O}_{P'}/\mathcal{O}'_{P'}$ is unramified and $\mathcal{O}'_{P'}$ is a PID. Let $M \subseteq (\mathcal{O}_{P'})^n$ be a module of rank n. If M is G-stable then $M^G \cdot \mathcal{O}_{P'} = M$.*

Proof. The fact that $\mathcal{O}'_{P'}$ is a PID follows from preliminaries and the fact that $\mathcal{O}_{P'}/\mathcal{O}'_{P'}$ is unramified follows from the fact that the only nonzero prime ideal in $\mathcal{O}'_{P'}$ is P', which does not ramify by assumption. Since $\mathcal{O}'_{P'}$ is a PID, $\mathcal{O}_{P'}$ is d-dimensional free over $\mathcal{O}'_{P'}$. Let $\{\alpha_1, \ldots, \alpha_d\}$ be a basis. Since $\mathcal{O}_{P'}/\mathcal{O}'_{P'}$ is unramified, the determinant $\det(\phi_j(\alpha_i))_{i,j}$ of this basis is a unit of $\mathcal{O}'_{P'}$ and,

[22] A given decomposition of M as an internal direct sum of rank-1 submodules is turned into another such one of M by application of $\phi \in G$. The claim follows since the discriminant does not depend on the choice of decomposition.

therefore, also a unit of $\mathcal{O}_{P'}$.[23] Hence, the matrix $A := (\phi_j(\alpha_i))_{i,j}$, defined over $\mathcal{O}_{P'}$, is invertible over $\mathcal{O}_{P'}$. The claim follows by the argument from the proof of Lemma 2.12, *replacing* K *by* $\mathcal{O}_{P'}$ in the argument involving A: each element of $m \in M$ is a finite $\mathcal{O}_{P'}$-linear combination of elements from M^G. □

It is now easy to "glue" these local results together to get the desired global result.

Proof (Proof of Proposition 4.1). Let us write $\mathcal{O} = \mathcal{O}_K$ and $\mathcal{O}' = \mathcal{O}_{K'}$ the respective ring of integers of K and K'. By Lemma 5.4, proving Proposition 4.1 is equivalent to showing that, for each prime P' of $\mathcal{O}'$, we have $M_{P'} = (M^G)_{P'} \cdot \mathcal{O}_{P'}$. Let P' be a prime of $\mathcal{O}'$ that ramifies (if there is any). Lemma 5.5 implies that P' does not divide $\mathrm{disc}_{K'}(M^G)$, as otherwise $\mathrm{disc}_K(M)$ would be ramified. So $M_{P'} = (\mathcal{O}_{P'})^n$ and thus $(M^G)_{P'} = (M_{P'})^G = (\mathcal{O}_{P'})^n$. So the result is true for such P'. Now suppose P' does not ramify. Then Lemma 5.6 implies $M_{P'} = (M_{P'})^G \cdot \mathcal{O}_{P'}$. Since $(M_{P'})^G = (M^G)_{P'}$, the result is also true for these P'. □

6 Generalizations

6.1 Other Galois-Action

In this section we characterise more general Galois-actions, that one could consider as well. Namely we are interested in any G-action on K^n that is compatible with the G-action on K. This means that we have an injective morphism, denoted $\phi \mapsto \phi\cdot$, sending G into the group of K'-linear automorphisms of K^n (viewed as K'-space) with the property that $\phi \cdot (\lambda x) = \phi(\lambda) \cdot (\phi \cdot x)$ for all $\lambda \in K$ and $x \in K^n$. Given such a morphism, we write again $\phi(x)$ for $\phi \cdot x$. The action described earlier is consistent with this definition. We will say that such action is K*-compatible*. We now classify all such actions.

Lemma 6.1. *Consider K/K' a Galois extension of number fields with Galois group G. Then the K-compatible Galois-actions of G onto K^n are the ones that can be written as $\alpha_{\mathbf{B}} : \phi \in G \mapsto \mathbf{B} \circ (\phi\cdot) \circ \mathbf{B}^{-1}$, where $\mathbf{B}$ is a matrix in $GL_n(K)$. The column-vectors of $\mathbf{B}$ then form a basis of G-invariant vectors of K^n under $\alpha_{\mathbf{B}}$.*

Proof. First consider that we have a K-invariant Galois action. First note that there is K-basis that consists of G-invariant vectors (see the text preceding Lemma 2.12). The G-invariant space is exactly the K'-span of this basis. Let us note $\mathbf{B}$ its matrix expressed in the canonical basis of K^n. Then, it is also clear

[23] Indeed, the ideal generated by the determinant of a basis is divisible only by ramified primes. Since there are no ramified primes here, then this ideal must be $\mathcal{O}'_{P'}$, and so the determinant of the basis is a unit.

that the G-action on $x \in K^n$ is the same as writing x as a coordinate-vector in that basis, applying $\phi \in G$ coordinate-wise, and writing the result back in the standard basis. Meaning that the action at hand is in fact $\alpha_{\mathbf{B}}$. Conversely, consider K-linear automorphism K^n given by a matrix $\mathbf{B} \in GL_n(K)$. It is then easy to verify that $\alpha_{\mathbf{B}}$ is indeed K-compatible and that each column-vector of $\mathbf{B}$ is invariant under the action of $\alpha_{\mathbf{B}}$. This completes the classification. □

Equivalently, we may view this as follows. Suppose that M is G-stable in the generalized sense. Then $\mathbf{B}^{-1}M$ is G-stable in the coordinate-wise sense, vice versa. Moreover, $\phi \mapsto \mathbf{B} \circ (\phi \cdot) \circ \mathbf{B}^{-1}(m) = m$ if and only if $\phi(B^{-1}m) = m$, so the same relation between the respective invariant spaces holds.

There is little hope into generalising our results to such actions. First, note that any free module M defined as $\mathbf{B} \cdot (\mathcal{O}_K)^n$ with $\mathbf{B} \in GL_n(K)$ is stable under $\alpha_{\mathbf{B}}$. So if we could use this to efficiently find short vectors in the module, then we would have an algorithm to solve SVP in all free modules. Second, remark that if $\mathbf{v}$ is a solution to SVP in $\mathbf{B}^{-1} \cdot M$ with the coordinate-wise action, then there is no guarantee that $\mathbf{B} \cdot \mathbf{v}$ is also a short vector in M. As a matter of fact, both approaches tend to show that this amounts to reducing the basis $\mathbf{B}$.

6.2 Modules in K^n

Let $M \subset K^n$ be a finitely generated $\mathcal{O}$-submodule of maximal rank n. Let P be a prime of $\mathcal{O}$. We say M is *P-integral* if $M \subset (\mathcal{O}_P)^n$ [24]. It is *maximally* P-integral if $M_P\ (= M \cdot \mathcal{O}_P) = (\mathcal{O}_P)^n$. Let V be a *finite* subset of the primes of $\mathcal{O}$. We say that M is *V-integral* if it is P-integral for each $P \in V$. It is *maximally* so if it is maximally P-integral for each $P \in V$. Consider the ideal $\mathcal{I}$ of $\mathcal{O}$ consisting of all $\mu \in \mathcal{O}$ with $\mu \cdot M \subset \mathcal{O}^n$. If M is P-integral for some prime P, then it is clear, by looking at a finite set of generators of M, that there is $\mu \in \mathcal{I}$ with $\mu \notin P$. So if M is P-integral for all $P \in V$, then $\mathcal{I}$ is not divisible by any $P \in V$. Using CRT, we now select some $\mu \in \mathcal{I} \cap \mathcal{O}'$ such that $\mu \notin P$ for all $P \in V$.

If M is maximally V-integral, then, in addition, the discriminant $\mu^{2n} \cdot \mathrm{disc}_K(M)$ of $\mu \cdot M \subset \mathcal{O}^n$ (now an ideal of $\mathcal{O}$) is not divisible by any $P \in V$. Indeed, let $P \in V$. Then $(\mu \cdot M)_P = M_P$, since $\mu \notin P$. By assumption, $M_P = (\mathcal{O}_P)^n$, so the discriminant of $(\mu \cdot M)_P$ is the unit-ideal. Therefore, P does not divide the discriminant of $\mu \cdot M$. We now say that M is *unramified* if it is maximally V-integral where V is the set of ramified primes (w.r.t $\mathcal{O}/\mathcal{O}'$). We say that M is *not wildly ramified* if the same holds but with V replaced by the set of wildly ramified primes. Note that those two sets are finite in our setting. Since $(\mu \cdot M)^G = \mu \cdot M^G$, we have:

Corollary 6.2. *Let $M \subset K^n$ be a finitely generated $\mathcal{O}$-submodule of maximal rank n. Suppose M is unramified (w.r.t. $\mathcal{O}/\mathcal{O}'$). Then M is G-stable if, and only if, $M = M^G \cdot \mathcal{O}$.*

[24] Equivalently, generating sets are always over $(\mathcal{O}_P)^n$

Corollary 6.3. *Let $M \subset K^n$ be a finitely generated $\mathcal{O}$-submodule of maximal rank n. Suppose M is not wildly ramified. Then Theorem B.1 also holds in K^n.*

6.3 The Non-Galois Case

In the same setting, consider an *intermediate extension* F of a Galois extension K/K'. Note that K/F is Galois but F/K' need not be. Consider an $\mathcal{O}_F$-submodule $M \subset \mathcal{O}_F^n$, with discriminant $\mathrm{disc}_F(M)$. We can handle this scenario too. We extend M over $\mathcal{O}$ and apply our theory there. Lemma 6.5 below makes the desired connection. Primes unramified in $\mathcal{O}_F/\mathcal{O}'$ may ramified in $\mathcal{O}$. So the conditions will be on $\mathrm{disc}_F(M) \cdot \mathcal{O}$ rather than $\mathrm{disc}_F(M)$. All in all, if our field extension is not Galois, we may pass to its normal closure (in some given algebraically closed field containing both).

Lemma 6.4 (Extend-then-Contract for Modules). *Let E/F be a finite separable extension of fields. Suppose $\mathcal{O}_E/\mathcal{O}_F$ is an extension of Dedekind domains such that E (F) is the quotient field of $\mathcal{O}_E$ ($\mathcal{O}_F$) and such that $\mathcal{O}_E$ is the integral closure of $\mathcal{O}_F$ in E. Let $M \subset \mathcal{O}_F^n$ be an $\mathcal{O}_F$-submodule of maximal rank n. Then $(M \cdot \mathcal{O}_E) \cap F^n = M$. In other words, extend-then-contract is the identity operation here.*

Proof. First note that $(M \cdot \mathcal{O}_E) \cap F^n = (M \cdot \mathcal{O}_E) \cap (\mathcal{O}_F)^n$. Clearly, $M \subset (M \cdot \mathcal{O}_E) \cap F^n$ and write D, D^* for their resp. discriminants. By direct inspection, $M \cdot \mathcal{O}_E = ((M \cdot \mathcal{O}_E) \cap F^n) \cdot \mathcal{O}_E$. Therefore, $D \cdot \mathcal{O} = D^* \cdot \mathcal{O}$. By Lemma A.1, it follows that $D = D^*$. So, by Lemma 2.9, the claim follows. [25] □

Lemma 6.5. *Let $M \subset (\mathcal{O}_F)^n$ be an $\mathcal{O}_F$-submodule. Suppose it is of maximal rank n and suppose $M \cdot \mathcal{O}$ is G-stable. Then $M = (M \cap (K')^n) \cdot \mathcal{O}_F$ if, and only if, $(M \cdot \mathcal{O}) = (M \cdot \mathcal{O})^G \cdot \mathcal{O}$.*

Proof. Before proving the claim, note that we have

$$(M \cdot \mathcal{O})^G = (M \cdot \mathcal{O}) \cap (K')^n = ((M \cdot \mathcal{O}) \cap F^n) \cap (K')^n = M \cap (K')^n,$$

where the first and second equalities are trivial, and the third follows from Lemma 6.4. Thus, the "K'-rational part" of M equals that of $M \cdot \mathcal{O}$, with maximal rank n; indeed, apply Lemma 2.12 to $M \cdot \mathcal{O}$, which is G-stable (by assumption) and of maximal rank n (since M is). Write $M' := M \cap (K')^n$. From the above, the forward direction is by subsitution since

$$M \cdot \mathcal{O} = (M' \cdot \mathcal{O}_F) \cdot \mathcal{O} = M' \cdot \mathcal{O} = (M \cdot \mathcal{O})^G \cdot \mathcal{O}.$$

In the other, let $H \subset G$ be the subgroup that fixes F. Then:

$$M = (M \cdot \mathcal{O})^H = ((M \cdot \mathcal{O})^G \cdot \mathcal{O})^H = (M' \cdot \mathcal{O})^H = ((M' \cdot \mathcal{O}_F) \cdot \mathcal{O})^H = M' \cdot \mathcal{O}_F.$$

[25] Remark that this can also be recovered from lemma 2.13 and corollary 2.14 together with the observation that the result is true for ideals.

Indeed, the first equality is by Lemma 6.4, the second by applying H-invariance to the hypothesis, the third is from the above, the fourth is trivial, and the fifth is, again, by Lemma 6.4; use that $M' \cdot \mathcal{O}_F$ is of maximal rank n (since M' is). □

References

1. Aggarwal, D., Stephens-Davidowitz, N.: Just take the average! an embarrassingly simple 2^n-time algorithm for svp (and cvp). In: SOSA (2018), http://arxiv.org/abs/1709.01535
2. Atiyah, M., MacDonald, I.: Introduction To Commutative Algebra. Addison-Wesley series in mathematics, Avalon Publishing (1994)
3. Boudgoust, K., Gachon, E., Pellet-Mary, A.: Some easy instances of ideal-svp and implications on the partial vandermonde knapsack problem. In: Advances in Cryptology–CRYPTO 2022. pp. 480–509. Springer (2022)
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. p. 309–325. ITCS '12, Association for Computing Machinery, New York, NY, USA (2012). https://doi.org/10.1145/2090236.2090262, https://doi.org/10.1145/2090236.2090262
5. Cohen, H.: Advanced Topics in Computational Number Theory. Graduate Texts in Mathematics, Springer New York (2012), https://books.google.cz/books?id=OFjdBwAAQBAJ
6. Felderhoff, J., Pellet-Mary, A., Stehlé, D.: On module unique-svp and ntru. In: Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part III. pp. 709–740. Springer (2022)
7. Fröhlich, A., Taylor, M.J.: Algebraic Number Theory. Cambridge Studies in Advanced Mathematics, Cambridge University Press (1991). https://doi.org/10.1017/CBO9781139172165
8. Hanrot, G., Pujol, X., Stehlé, D.: Analyzing blockwise lattice algorithms using dynamical systems. In: Advances in Cryptology–CRYPTO 2011. pp. 447–464. Springer (2011)
9. Hoffstein, J., Pipher, J., Silverman, J.H.: Ntru: A ring-based public key cryptosystem. In: Algorithmic number theory, pp. 267–288. Springer (1998)
10. Johnston, H.: Notes on galois modules. Notes accompanying the course 'Galois Modules' given in Cambridge (2011)
11. Lang, S.: Algebraic Number Theory. Springer New York (1994). https://doi.org/10.1007/978-1-4612-0853-2, https://doi.org/10.1007%2F978-1-4612-0853-2
12. Lang, S.: Algebra. Springer New York (2002). https://doi.org/10.1007/978-1-4613-0041-0, https://doi.org/10.1007%2F978-1-4613-0041-0
13. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography **75** (06 2014). https://doi.org/10.1007/s10623-014-9938-4
14. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010. pp. 1–23. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
15. Marcus, D.A.: Number fields, vol. 1995. Springer (1977)

16. Milne, J.: Algebraic number theory
17. Pan, Y., Xu, J., Wadleigh, N., Cheng, Q.: On the ideal shortest vector problem over random rational primes. In: Advances in Cryptology–EUROCRYPT 2021. pp. 559–583. Springer (2021)
18. Pellet-Mary, A., Stehlé, D.: On the Hardness of NTRU Problem. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021. vol. 13090. Springer (2021)
19. Porter, C., Mendelsohn, A., Ling, C.: Subfield Algorithms for Ideal- and Module-SVP Based on the Decomposition Group (2021). https://doi.org/10.48550/ARXIV.2105.03219, https://arxiv.org/abs/2105.03219
20. Silverman, J.H.: The Arithmetic of Elliptic Curves. Springer New York (2009). https://doi.org/10.1007/978-0-387-09494-6, https://doi.org/10.10072F978-0-387-09494-6
21. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Matsui, M. (ed.) Advances in Cryptology – ASIACRYPT 2009. pp. 617–635. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)

A Proof of Lemma 2.17

In this section, we prove Lemma 2.17, which we recall below ($K, K', \mathcal{O}$ and $\mathcal{O}'$ are as defined in Section 2.3, subsection "setting").

Lemma (Lemma 2.17). *Suppose K/K' is Galois. Let I be an ideal of $\mathcal{O}$. Suppose that I is not divisible by any ramified prime of $\mathcal{O}$. Then I is G-stable if and only if $I = I^G \cdot \mathcal{O}$. In other words, I is G-stable if and only if it equals the extension of its contraction.*

We will use the following two straightforward lemmas. Note that these lemmas do not suppose that K/K' is Galois.

Lemma A.1. *Let I', J' be ideals of $\mathcal{O}'$. Then $\mathcal{O} \cdot I' = \mathcal{O} \cdot J'$ if and only if $I' = J'$. In other words, the resp. extensions of two ideals coincide if and only if these ideals are identical.*

Proof. Only the forward direction needs commenting. *Extension by* $\mathcal{O}$ of an $\mathcal{O}'$-ideal means taking alle finite $\mathcal{O}$-linear combination over that ideal, resulting in an $\mathcal{O}$-ideal (containing the original one as a subset). Suppose $I' \neq J'$, and wlog, that both are nonzero. Then their respective Dedekind-factorizations in $\mathcal{O}'$ differ. Dedekind-factorization "after extension" of an ideal is determined precisely by substituting, for each prime dividing the ideal in question, the splitting of that prime after extension. Therefore, the Dedekind-factorizations (in $\mathcal{O}$) of $\mathcal{O} \cdot I', \mathcal{O} \cdot J'$ differ and the latter are distinct. The other direction is trivial. □

Lemma A.2. *Let I' be an ideal of $\mathcal{O}'$. Then $(\mathcal{O} \cdot I') \cap K' = I'$. In other words, extend-then-contract is the identity operation.*

Proof. The $\mathcal{O}$-extensions of the $\mathcal{O}'$-ideals I' and $(\mathcal{O} \cdot I') \cap K'$ coincide. So these $\mathcal{O}'$-ideals must be equal by Lemma A.1. □

We can now prove Lemma 2.17.

Proof. We start with the forward direction. The claim is trivial if $I = (0)$ or if $I = \mathcal{O}$. So assume $(0) \subsetneq I \subsetneq \mathcal{O}$. Let P be a prime ideal of $\mathcal{O}$ dividing I. Since I is G-stable, all of the conjugates of P divide I as well, to the same power. Thus, the corresponding powers in the Dedekind-factorization of I are the same. But since P is not ramified, the product over its complete set of conjugates is an extension of a prime ideal of $\mathcal{O}'$. After dividing out the appropriate power of the latter extension from the Dedekind-factorization of I (so as to get rid of P and all of its conjugates), induction can be applied. Thus, I is the extension of some ideal I' of $\mathcal{O}'$, i.e., $I = I' \cdot \mathcal{O}$. By Lemma A.2, it follows that $I \cap K' = I'$. Extending both sides over $\mathcal{O}$ yields $(I \cap K') \cdot \mathcal{O} = I$. Or, equivalently, $I = I^G \cdot \mathcal{O}$. In the reverse direction, an extension of some ideal I' of $\mathcal{O}'$ is always G-stable: it consists of the finite $\mathcal{O}$-sums of I'-elements and the latter elements are all fixed by G. □

Remark A.3. The lemma can fail if I is divisible by some ramified prime. Suppose P' ramifies in $\mathcal{O}$. Then $I := \prod_{i=1}^{r} P_i$ is G-stable, but the extension of its contraction equals I^e with $e > 1$.

That said, we have the following strengthening.

Corollary A.4. *Suppose K/K' is Galois. Let I be a ideal of $\mathcal{O}$. Suppose that $I = I_U \cdot I_R$, where I_U is an unramified ideal of $\mathcal{O}$ and where I_R is an ideal of $\mathcal{O}$ comaximal [26] with I_U and where $I_R = J' \cdot \mathcal{O}$ for some ideal J' of $\mathcal{O}'$. (So I_R is possibly divisible by a ramified prime, but, if it is, in not too bad way). Then I is G-stable if and only if $I = \mathcal{O} \cdot I^G$.*

Proof. Only the forward direction requires commenting. Coprimeness now implies that both I_U and I_R are G-stable (since the G-action stays within each). So I_U is also an extension of an $\mathcal{O}'$-ideal, and therefore I as well. Lemma A.2 settles the claim. □

B A third proof of Proposition 4.1

Theorem B.1. *Suppose K/K' is Galois. Let $M \subset \mathcal{O}^n$ be an $\mathcal{O}$-submodule of maximal rank n. Suppose M is G-stable and $\mathrm{disc}_K(M)$ is not divisible by any prime of $\mathcal{O}$ that is wildly ramified in $\mathcal{O}/\mathcal{O}'$. Then there are rank-1, G-stable $\mathcal{O}$-submodules $M_1, \ldots, M_n \subset M$ yielding the internal direct sum decomposition $M = M_1 \oplus \cdots \oplus M_n$.*

[26] Their sum is the whole ring

Proof. The proof is from scratch. It uses a local-global approach but none of our previous results. Let π be the projection on one fixed choice of the n coordinates in K^n (w.r.t. standard basis of unit vectors). Consider $N := \pi(M)$. This is a nonzero $\mathcal{O}$-ideal (since M has maximal rank), and it is thus projective. Let g be a split, i.e., an $\mathcal{O}$-morphism with $\pi \circ g$ equal to the identity on N. This gives (internally) $M = (\ker \pi) \oplus g(N)$, as $\mathcal{O}$-modules. One sees at once that both N and $\ker \pi$ are G-stable since M is[27]. However, there is no guarantee that $g(N)$ is G-stable as well. We remedy this by tailoring g into a new g^* that *doubles* as π-split both as $\mathcal{O}$-morphism *and* as $\mathcal{O}'[G]$-morphism. This is by a local-global approach [28] in combination with an "averaging" manoeuvre from basic representation theory that can render maps linear over a group ring [29] and that is tailored to our scenario by exploiting a fact about the $\mathcal{O}'$-ideal $\mathrm{Tr}_{K/K'}(\mathcal{O})$. Inductive application then establishes the theorem. Indeed, define the $\mathcal{O}$-submodule $M' := \ker \pi \subset \mathcal{O}^{n-1}$. This has rank $n-1$ since N has rank 1. Besides, its discriminant is not divisible by any wildly ramified prime P. Indeed, since $P \not| \mathrm{disc}_K(M)$, we have $M_P = (\mathcal{O}_P)^n$. From $M = \ker \pi \oplus N$, we see that $(\ker \pi)_P = (\mathcal{O}_P)^{n-1}$ (since N is rank-1). Thus $P \not| \mathrm{disc}_K(\ker \pi)$. So, with M' in hand, now choose a new π (projecting on one of the remaining $n-1$ coordinates), get the new g^*, and so on. After n steps we obtain the full claimed decomposition of M. It is left to show how to obtain g^*.

Consider the $\mathcal{O}'$-ideal $\mathrm{Tr}_{K/K'}(\mathcal{O})$. It is known (see e.g. [10]) that, in our setting (and assuming K/K' is Galois as we do), a prime P' of $\mathcal{O}'$ divides this ideal if and only if it ramifies wildly in $\mathcal{O}$. As a stepping stone, we first show how to get g^* in case $\mathcal{O}/\mathcal{O}'$ is *tame*, i.e., there may be ramifying primes but no prime that ramifies wildly. Afterwards, we show how to adapt the proof for the general case, using the local-global approach. So assume, for the moment, that $\mathcal{O}/\mathcal{O}'$ is tame. Hence, there is no condition on $\mathrm{disc}_K(M)$ and $\mathrm{Tr}_{K/K'}(\mathcal{O}) = \mathcal{O}'$. Choose $\alpha \in \mathcal{O}$ with $\mathrm{Tr}_{K/K'}(\alpha) = 1$ and *redefine* g by "averaging over G" as follows:

$$g^* : N \longrightarrow M, \quad z \mapsto \sum_{\phi \in G} \phi(\alpha) \cdot (\phi \circ g \circ \phi^{-1})(z).$$

By direct inspection, this is a split of π both as $\mathcal{O}$-morphism and as $\mathcal{O}'[G]$-morphism. Our specific choice of α plays out when verifying the latter. [30]

Now assume there is wild ramification. Thus, we no longer have such α. But since we have it *locally* where needed, there is a suitable local-global rendition, as we now explain. Let P' be any prime of $\mathcal{O}'$. Consider the localized extension $\mathcal{O}_{P'}/\mathcal{O}'_{P'}$, together with the surjective $\mathcal{O}_{P'}$-linear map $\pi_{P'} : M_{P'} \to N_{P'}$, and

[27] This conclusion also holds if π were to be replaced with some other linear form *defined over* $\mathcal{O}'$.

[28] Inspired by Ch. I, Proposition 26 in [11]

[29] See e.g. [12], Ch. XVIII, & 1.

[30] More usually, there is the scalar factor $1/n$ in the averaging to ensure the right outcome. But this is not affordable here; hence our specific choice of α. Its functionality is the same as in that $1/n$-case.

the $\mathcal{O}_{P'}$-linear map $g_{P'} : N_{P'} \to M_{P'}$, the extension of g by $\mathcal{O}_{P'}$ (just take $\mathcal{O}_{P'}$-linear combinations). Then observe that $g_{P'}$ is a split of $\pi_{P'}$ and that $\pi_{P'}$ is an $\mathcal{O}'_{P'}[G]$-morphism (since $M_{P'}$-is G-stable). For each P' we will modify $g_{P'}$, call the modification $g^*_{P'}$, and glue those $g^*_{P'}$'s together in order to obtain the claimed tailored global split g^* of π. We divide the primes P' into two categories: (I) the (finitely many) ones that ramify wildly in $\mathcal{O}$ and (II) the rest.

Let P' be a prime in Category I. Since $\mathrm{disc}_K(M)$ is not divisible by any wildly ramified prime, it is not divisible by any prime above P'. Therefore, $M_{P'} = (\mathcal{O}_{P'})^n$ and $N_{P'} = \pi_{P'}(M_{P'}) = \mathcal{O}_{P'}$. Now *replace* $g_{P'}$ by $g^*_{P'}$ as follows. The new version $g^*_{P'}$ sends 1 to a vector in $(\mathcal{O}'_{P'})^n$ (which is G-invariant by definition) whose π-image equals 1. This is then $\mathcal{O}_{P'}$-linearly extended. This way, it is indeed a $\mathcal{O}'_{P'}[G]$-morphism, in addition to being a $\mathcal{O}_{P'}$-morphism. Also, it is a split since $\pi_{P'}$ sends that vector back to 1. A concrete choice is to map 1 to the unit vector $e_\pi \in (\mathcal{O}'_{P'})^n$ whose $\pi_{P'}$-image equals 1. Towards gluing, we choose $\lambda(P') \in S'(P') := \mathcal{O}' - P'$ such that $\lambda(P') \cdot g^*_{P'}$ sends $N \subset \mathcal{O}_{P'}$ into M. It is sufficient to choose $\lambda(P') \in S'(P')$ with $\lambda(P') \cdot e_\pi \in M$. Such $\lambda(P')$ exists since $(\mathcal{O}_{P'})^n = M_{P'}$ (established above), and thus $e_\pi = m/s$ for some $m \in M, s \in S'(P')$. So we can set $\lambda(P') = s$.

Now let P' be a prime in Category II. Choose a finite set of $\mathcal{O}'$-generators for the $\mathcal{O}'$-ideal $\mathrm{Tr}_{K/K'}(\mathcal{O})$. By the aforementioned fact, at least one of the latter is not contained in P', say $\gamma = \gamma(P') \in \mathcal{O}'$. (Indeed, otherwise P' would divide the ideal). Choose $\beta = \beta(P') \in \mathcal{O}$ such that $\mathrm{Tr}_{K/K'}(\beta) = \gamma$. Then $\alpha = \alpha(P') := \beta/\gamma \in \mathcal{O}_{P'}$ (and so are its G-conjugates) and $\mathrm{Tr}_{K/K'}(\alpha) = 1$. (This is no contradiction with the fact about $\mathrm{Tr}_{K/K'}(\mathcal{O})$ since $\alpha \in \mathcal{O}_{P'}$). Now *redefine* $g_{P'}$ as follows

$$g^*_{P'} : N_{P'} \longrightarrow M_{P'}, \quad z \mapsto \sum_{\phi \in G} \phi(\alpha(P')) \cdot (\phi \circ g_{P'} \circ \phi^{-1})(z).$$

Again, by direct inspection, this is a split of $\pi_{P'}$ both as $\mathcal{O}_{P'}$-morphism and as $\mathcal{O}'_{P'}[G]$-morphism. Now define $\lambda(P') := \gamma(P')$ (which sits in $S'(P')$) and note that $\lambda_{P'} \cdot g^*_{P'}(N) \subset M$.

We glue all the data together. For each prime P' of $\mathcal{O}_{P'}$ we have chosen $\lambda(P') \in S'(P')$ such that $\lambda(P') \cdot g^*_{P'}(N) \subset M$. So the $\mathcal{O}'$-ideal generated by these $\lambda(P')$ is the unit-ideal; indeed, if not, there is some P' without a $\lambda(P')$; absurd. Therefore, there is a *finite* set V of primes P' and, for each $P' \in V$, there is $\kappa(P') \in \mathcal{O}'$ with $\sum_{P' \in V} \kappa(P') \cdot \lambda(P') = 1$. (Note that V necessarily contains a wildly ramifying prime since the λ's from Category II are contained in the ideal $\mathrm{Tr}_{K/K'}(\mathcal{O})$, which is proper by assumption. Also, by factorizing the corresponding ideals $(\lambda) \cdot \mathcal{O}'$, it is easy to make V explicit.) One verifies directly that g^* can be taken as

$$g^* : N \longrightarrow M, \quad z \mapsto \sum_{P' \in V} \kappa(P') \cdot \lambda(P') \cdot g^*_{P'}(z).$$

□

Corollary B.2. *Proposition 4.1 can be recovered as corollary.*

Proof. The proof is straightforward. The theorem implies M has a pseudo-basis of $b_1, \dots, b_n \in (K')^n$, with nonzero G-stable ideals $J_1, \dots, J_n$ of $\mathcal{O}$. Namely, fix index i. By Lemma 2.12, there is a nonzero element $b_i' \in (M_i)^G \subset (\mathcal{O}')^n$. Let J_i be the fractional $\mathcal{O}$-ideal of K with $M_i = J_i \cdot b_i'$. By multiplication with some suitable nonzero $\mu \in \mathcal{O}'$, we may assume it is an $\mathcal{O}$-ideal. [31] So set $b_i := b_i'/\mu \in (K')^n$. The claim holds if and only if, for each J_i, we have $J_i = J_i' \cdot \mathcal{O}$ with $J_i' = J_i \cap \mathcal{O}'$. If all J_i are unramified, then Lemma 2.17 settles it. Write $N := M^G \cdot \mathcal{O}$. Now suppose some J_i is divisible by a ramified prime P. Note that the pseudo-basis vectors may not be in $\mathcal{O}^n$, so this does not contradict the assumption that $\mathrm{disc}_K(M)$ is unramified. Applying Lemma 5.5, $\mathrm{disc}_K(N)$ is unramified. Since M and N share the same pseudo-basis vectors (in $(K')^n$) here, $\mathrm{disc}_K(N)/\mathrm{disc}_K(M)$ is the square of the product over all $(J_i' \cdot \mathcal{O})/J_i$, which is unramified. Thus P and its conjugates divide J_i to the same power as it divides $J_i' \cdot \mathcal{O}$. Hence, this power is a multiple of the ramification exponent of P. Thus, the contribution of P and its conjugates is an the extension of some power of the prime below P. Clearly, this also holds for possible other ramified primes that divide J_i and that are not conjugate to P and for other J_i of the same type; Lemma A.4 settles the claim. □

C Looser approximation factors for HSVP in ideals

In this section we are mainly interested into describing more precisely the approximation factor one can get if restrict-then-extend is not the identity, in the case of ideals. We will fully describe such approximation factor for any ideal depending on its prime factorisation, and by doing so we generalise results of [17,19,3]. We consider ideals of general extensions K/K', i.e. without assuming there is a non trivial automorphism.

To study general ideals we will need the following lemmas.

Lemma C.1. *Consider K/K' an extension of number fields, and I, J such that $I \cap K'$ and $J \cap K'$ are two coprime ideals of K'. Then $IJ \cap K' = (I \cap K') \cdot (J \cap K')$.*

Lemma C.2 ([5]). *Consider K/K' an extension of number fields, P a prime ideal of K and $e \in \mathbb{Z}_{\geq 0}$. Moreover fix $a = \lceil \frac{e}{e(P|P \cap K')} \rceil$ Then $P \cap K' = (P \cap K')^a$.*

Lemma C.3. *Consider K/K' an extension of number fields, P' a prime ideal of K', P_1, P_2 two prime ideals of K above P' and $(\alpha_1, \alpha_2) \in \mathbb{Z}^2_{\geq 0}$. Denote $e(P_1|P')$ and $e(P_2|P')$ by e_1 and e_2 respectively, and write $i_0 := \mathrm{argmax}\{\lceil \alpha_1/e_1 \rceil, \lceil \alpha_2/e_2 \rceil\}$. Then $P_1^{\alpha_1} P_2^{\alpha_2} \cap K' = P'^{\lceil \alpha_{i_0}/e_{i_0} \rceil} \cap K'$.*

[31] An element of K may be written as fraction of an $\mathcal{O}$-element and an $\mathcal{O}'$-element.

We will express the increased approximation factor found through this intersection strategy depending on the prime factorisation of I, when $(I \cap K') \cdot \mathcal{O}_K \subsetneq I$. Such formulas have been identified in [19] but the ones we give are more general, both because we consider extensions which are not necessarily Galois and ideals which can be divided by ramified primes.

First let us express how much one can loose using the volumes of the corresponding lattices (via σ_K).

Lemma C.4. *Consider an extension K/K' of number fields with respective degrees d and d', together with I an ideal of K. Then any solution to γ-HSVP in $\sigma_{K'}(I \cap K')$ is also a solution to γ'-HSVP in $\sigma_K(I)$, such that*

$$\frac{\gamma'}{\gamma} = \frac{\mathcal{N}_{K'}(I \cap K')^{1/d'}}{\mathcal{N}_K(I)^{1/d}}. \tag{2}$$

Proof. The proof is very similar to what has been done in the one of Theorem 4.2. Let us write I' for $I \cap K'$. Consider $x \in I'$ a solution to γ-HSVP in I', i.e. satisfying $\|\sigma_{K'}(x)\| \leqslant \gamma \cdot \sqrt{d'} \cdot \left(\mathcal{N}_{K'}(I')\sqrt{\Delta_{K'}}\right)^{1/d'}$. Then remark that $\|\sigma_K(x)\| = \sqrt{d/d'} \cdot \|\sigma_{K'}(x)\|_{K'}$, so we have $\|\sigma_K(x)\| \leqslant \gamma \cdot \sqrt{d} \cdot \left(\mathcal{N}_{K'}(I') \cdot \sqrt{\Delta_{K'}}\right)^{1/d'}$. Moreover we know that $\Delta_K = \Delta_{K'}^{d/d'} \cdot \mathcal{N}_{K'}(\mathfrak{d}(K/K'))$ (where $\mathfrak{d}(K/K')$ is the relative discriminant) therefore

$$\|\sigma_K(x)\| \leqslant \frac{\gamma \cdot \sqrt{d} \cdot \left(\sqrt{\Delta_K} \cdot \mathrm{N}_{K/\mathbb{Q}}(I)\right)^{1/d}}{\mathcal{N}_{K/K'}(\mathfrak{d}(K/K'))^{1/2d}} \cdot \frac{\mathcal{N}_{K'}(I')^{1/d'}}{\mathcal{N}_K(I)^{1/d}},$$

which gives the claimed result. □

Notation 1. *Given K/K' an extension of number fields with degrees d and d' and I an ideal of $\mathcal{O}_K$, we will denote by $q(I, K')$ the quotient $\frac{\mathcal{N}_{K'}(I \cap K')^{1/d'}}{\mathcal{N}_K(I)^{1/d}}$.*

Clearly $q(I, K')$ encompasses the quality of the vector obtained by solving γ-HSVP in $I \cap K'$. We will express which $q(I, K')$ can be reached in function of the prime factorisation of I. We starts with ideals above a unique prime ideal P' of $\mathcal{O}_{K'}$, then the general case follows easily.

Notation 2. *Consider K/K' an extension of number fields, P' a prime ideal of K', and $I = \prod_{P|P'} P^{v_P}$ with $v_P \geqslant 0$. We will write $\beta_I := \max_{P|P'} \left\lceil \frac{v_P}{e(P|P')} \right\rceil$ and $f_I := \sum_{P|P'} \frac{v_P}{\beta_I} f(P|P')$.*

Proposition C.5. *Consider K/K' an extension of number fields with respective degrees d and d', P' a prime ideal of $\mathcal{O}_{K'}$, and $I = \prod_{P|P'} P^{v_P}$ with $v_P \geqslant 0$. Then we have that*

$$q(I, K') = \mathcal{N}_{K'}(I \cap K')^{\frac{d/d' - f_I}{d}}. \tag{3}$$

Proof. From Lemmas C.2 and C.3 we have $I \cap K' = P'^{\beta_I}$. Then one has $\mathcal{N}_{K'}(I \cap K')^{\frac{1}{d'}} = \mathcal{N}_{K'}(P')^{\frac{\beta_I}{d'}}$. Additionally one has

$$\mathcal{N}_K(I) = \prod_{P|P'} \mathcal{N}_{K'}(P')^{v_P f(P|P')} = \mathcal{N}_{K'}(P')^{\sum_{P|P'} v_P f(P|P')},$$

which gives $\mathcal{N}_K(I)^{\frac{1}{d}} = \mathcal{N}_{K'}(P')^{\frac{\beta_I f_I}{d}}$. Thus we have that the quotient $q(I, K')$ is $\mathcal{N}_{K'}(P')^{\beta_I \cdot \frac{(d/d' - f_I)}{d}} = \mathcal{N}_{K'}(I \cap K')^{\frac{d/d' - f_I}{d}}$. □

Now let us show that Proposition C.5 can be extended to general ideals I.

Notation 3. *Consider K/K' an extension of number fields, $S = \{P'_1, \dots, P'_t\}$ a set of primes ideals of K'. Let $I = \prod_{P' \in S} \prod_{P|P'} P^{v_P}$ an ideal of K. We will denote by $I(P')$ the ideal $\prod_{P|P'} P^{v_P}$.*

Theorem C.6. *Consider K/K' an extension of number fields with respective degrees d and d', $S = \{P'_1, \dots, P'_t\}$ a set of primes ideals of K'. Let $I = \prod_{P' \in S} \prod_{P|P'} P^{v_P}$ an ideal of K. Then we have*

$$q(I, K') = \mathcal{N}_{K'}\left(I(P') \cap K'\right)^{\frac{d/d' - f_{I(P')}}{d}}. \tag{4}$$

Proof. By Lemma C.1 and Lemma C.2, we can see that we have

$$I \cap \mathcal{O}_{K'} = \prod_{P' \in S} \left(I(P') \cap K'\right) = \prod_{i=1}^{r} P'^{\beta_{I(P')}}.$$

Now, using the proof of Proposition C.5, we remark that

$$\forall P' \in S, \mathcal{N}_{K'}(P')^{\frac{\beta_{I(P')}}{d'}} = \mathcal{N}_K(I(P'))^{\frac{1}{d}} \cdot \mathcal{N}_{K'}\left(I(P') \cap K'\right)^{\frac{d/d' - f_{I(P')}}{d}},$$

so it follows that

$$q(I, K') = \prod_{P'} q(I(P'), K') = \prod_{P' \in S} \mathcal{N}_{K'}\left(I(P') \cap K'\right)^{\frac{d/d' - f_{I(P')}}{d}}.$$

□

Consequently [17, Theorem 4], [19, Theorem 3] and [3, Theorem 3.2.] can be extended to general extensions K/K' and general ideals I, see Corollary C.7.

Corollary C.7. *Consider K/K' an extension of number fields, $S = \{P'_1, \dots, P'_t\}$ and $I = \prod_{i=1}^{t} I(P'_i)$ an ideal of K such as in Theorem C.6. Then the following assertions are equivalent :*

(*i*) $q(I, K') = 1$;

(*ii*) $\forall i \in [\![1,t]\!], \forall P \mid P'_i, v_P \equiv 0 \bmod e(P|P'_i)$ *and* $\frac{v_P}{e(P|P'_i)} = \beta_{I(P'_i)}$.
(*iii*) $I = (I \cap K') \cdot \mathcal{O}_K$;

If they are satisfied then γ-HSVP in $\sigma_K(I)$ reduces to γ-HSVP in $\sigma_{K'}(I \cap K')$.

Proof. Using Theorem C.6 together with the definition of β_I and f_I we have

$$\begin{aligned}(i) &\iff \forall P' \in S,\ q(I(P'), K') = 1 \iff \forall P' \in S,\ f_{I(P')} = [K : K'] \\ &\iff \forall P' \in S,\ \forall P \mid P', v_P = \max_{P|P'} \left\lceil \frac{v_P}{e(P|P')} \right\rceil \cdot e(P|P') \\ &\iff (ii).\end{aligned}$$

Now let us show that (*ii*) and (*iii*) are equivalent. Since for any $P' \in S$ we have that $I(P') \cap K' = P'^{\beta_{I(P')}}$, we get that

$$(I \cap K') \cdot \mathcal{O}_K = \prod_{P' \in S} \prod_{P|P'} P^{e(P|P')\beta_{I(P')}}$$

which leads to

$$(iii) \iff \forall P' \in S, \forall P \mid P', v_P = e(P|P')\beta_I \iff (ii).$$

The part on the HSVP is clear by Lemma C.4. □

Remark C.8. We could not find a way of expressing the precise loss in approximation factor for modules in all generality. If M admits a pseudo-basis with basis vectors in $(K')^n$ such as in Lemma 2.15 then one can look ideal-by-ideal, similarly to what was done in [19]. However a module does not admit such decomposition in general.

D Direct sum in a free extension

In this section we will extend some observations made by Pan et al. [17] regarding how an ideal I can be decomposed as a direct sum of multiple copies of $I \cap K'$ as soon as it is stable under $G = \mathrm{Aut}_{K'}(K)$ and that $\mathcal{O}_K$ is free as an $\mathcal{O}_{K'}$-module. We show that this is also true for modules. More precisely we have:

Proposition D.1. *Let K/K' be an extension such that $\mathcal{O}_K$ is free as a $\mathcal{O}_{K'}$-module with basis $\mathcal{B}_{K/K'} = (c_1, \ldots, c_d)$. Let $M \subseteq (\mathcal{O}_K)^n$ be a full-rank module such that $M = (M \cap (K')^n) \cdot \mathcal{O}_K$. Then one has the following set equality $M = \bigoplus_{i=1}^{d} (M \cap (K')^n) \cdot c_i$.*

First let us prove the following lemma.

Lemma D.2. *Consider K/K' an extension of number fields together with $\mathcal{O}_K/\mathcal{O}_{K'}$ their respective ring of integers. Let $M \subseteq (\mathcal{O}_K)^n$ be a $\mathcal{O}_K$-submodule. Then the following assertions are equivalent:*

(i) there exist $\mathbf{m}_1, \dots, \mathbf{m}_r$ elements of $(K')^n$ such that $M = \sum_{i=1}^r \mathcal{O}_K \cdot \mathbf{m}_i$;
(ii) $M = (M \cap (K')^n) \cdot \mathcal{O}_K$.

Proof. We will denote by M' the $\mathcal{O}_{K'}$-module $M \cap (K')^n$. Assume (i) and let N be the $\mathcal{O}_{K'}$-module $\sum_{i=1}^r \mathcal{O}_{K'} \cdot \mathbf{m}_i$. Then $N \subseteq M'$ and $N \cdot \mathcal{O}_K = M$ which gives (ii). The module M' is finitely generated over $\mathcal{O}_{K'}$ so there are $\mathbf{m}_1, \dots, \mathbf{m}_r$ elements of K'^n such that $M' = \sum_{i=1}^r \mathcal{O}_{K'} \cdot \mathbf{m}_i$. Then clearly (ii) implies (i). □

Proof (Proposition D.1). Clearly $\sum_{j=1}^d M' c_i$ is included in M and the sum is in fact direct (because $(c_i)_{1 \leqslant i \leqslant d}$ is a $\mathcal{O}_{K'}$-basis of $\mathcal{O}_K$). Let us show the reverse inclusion. From Lemma D.2 and its proof we know that there are $\mathbf{m}_1, \dots, \mathbf{m}_r \in (K')^n$ such that $M = \sum_{j=1}^r \mathcal{O}_K \mathbf{m}_j$ and $M' = M \cap (K')^n = \sum_{j=1}^d \mathcal{O}_{K'} \mathbf{m}_j$. Consider $m \in M$ and write it as $\sum_{j=1}^r \lambda_j \mathbf{m}_j$ with $\lambda_j \in \mathcal{O}_K$ for all $j \in [\![1, r]\!]$. Then we have $\lambda_j = \sum_{i=1}^d \lambda_{i,j} c_i$ with $\lambda_{i,j} \in \mathcal{O}_{K'}$ for any i, j. Thus we obtain

$$m = \sum_{j=1}^r (\sum_{i=1}^d \lambda_{i,j} c_i) \mathbf{m}_j = \sum_{i=1}^d (\sum_{j=1}^r \lambda_{i,j} \mathbf{m}_j) c_i \in \sum_{i=1}^d M' c_i.$$

This is true for any $m \in M$ so $M \subseteq \bigoplus_{i=1}^d M' c_i$. □