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

Ronald Cramer[1,2], Daniël van Gent[2], Andrea Lesavourey[3], and Alice Pellet-Mary[4⋆]

[1] Leiden Univ., Leiden, The Netherlands
[2] CWI, Amsterdam, The Netherlands
cramer@cwi.nl
daniel.van.gent@cwi.nl
[3] Univ. Limoges, CNRS, XLIM, UMR 7252, F-87000 Limoges, France
andrea.lesavourey@unilim.fr
[4] Univ. Bordeaux, CNRS, Inria, Bordeaux INP, IMB, UMR 5251, Talence, France
alice.pellet-mary@math.u-bordeaux.fr

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 nd can in fact be seen as a lattice of rank only $nd/|G|$. 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).

Keywords: module lattices, number fields, subfields and automorphisms

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 with ring of integers $\mathcal{O}_K$. 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 $\mathcal{O}_K^n$ is a subset of $\mathcal{O}_K^n$ 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) $\mathbf{b}_1, \ldots, \mathbf{b}_r \in \mathcal{O}_K^n$ such that $M = \{\sum_{i=1}^r x_i \mathbf{b}_i \,|\, x_i \in \mathcal{O}_K\}$. For

⋆ Corresponding author.

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 $M \subseteq O_K$, the module M is usually called a non-zero 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 [12] or the Ring and Module Learning With Errors (LWE) assumptions [20,15,6,13]. These hardness assumptions have been successfully used to construct efficient post-quantum primitives, including three of the five post-quantum primitives standardized by the NIST so far.[5] 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 [18,20,15], as well as from finding short vectors in module lattices of rank at least 2 to solving NTRU and Module-LWE [9,13] (this is restricted to special rank-2 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 at least 2 in such a way that finding a short vector in these modules 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: the maps sending X to X^i, for i odd in $[1, 2d]$). 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., $g(x) = x$ for all $g \in G$), 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 $M \subseteq O_K^n$ such that for all $\mathbf{m} \in M$ and all $g \in G$, the vector $g(\mathbf{m})$ is in M, where g 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 belong to a subfield K'. Clearly, we cannot ask that M is an $O_{K'}$-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 O_K of an $O_{K'}$-submodule M' in $O_{K'}^n$, i.e., $M = M' \cdot O_K$. If we can prove that a module M belongs to a subfield K' in this sense, then it means that we can solve some algorithmic problems, such as finding short vectors in M, by actually considering the underlying $O_{K'}$-module M', which has a smaller dimension than M when seen as a $\mathbb{Z}$-lattice.

This question was already answered in the case of ideal lattices (i.e., for $n = 1$) in [17,5].[6] In these works, the authors showed that indeed, if some ideal I in O_K is stabilized (as a set) by some group G of automorphisms of K, then under some mild assumption on I one can see it as an ideal in a subfield K' of K of degree $d/|G|$. In

[5] https://csrc.nist.gov/projects/post-quantum-cryptography

[6] [17] proved it for *prime* ideal lattices, and [5] generalized it to any ideal.

the case of module lattices of rank at least 2 there is so far no clear answer to this question. Partial results exist [19], but they are significantly more restrictive than the simple condition "M is stabilized by a group G of automorphisms".

Contributions. In this article, we answer the question for modules of any rank, by generalizing the ideas of [17,5]. We prove that if a module M is stabilized as a set by a group G of automorphisms of K (we say that M is G-*stable*), then M can be seen as a module of a smaller field K', whose dimension is $|G|$ times smaller than that of K. This results holds under some mild condition on the discriminant ideal of M,[7] which is the same condition that [5] already had for their result on ideals. More precisely, we prove the following result.

Main result 1 (Informal formulation, see Theorem 3). *Let K/K' be a Galois extension of number fields with Galois group G, let $M \subseteq \mathcal{O}_K^n$ be a module of rank n whose discriminant is non-ramified. Then M is G-stable if and only if $\mathcal{O}_K \cdot (M \cap \mathcal{O}_{K'}^n) = M$.*

We provide two proofs of this result, targeted at different audiences. The first proof is mathematically more natural, but it requires knowledge about projective modules and localization, which are not recalled in the article. As a matter of fact, we achieve this through proving another result which is of independent interest: Theorem 2 states that a G-stable module M whose discriminant is coprime to wildly ramified primes can be decomposed as a direct sum of G-stable modules of rank 1, i.e. $M = M_1 \oplus \cdots \oplus M_n$.

For the readers who are not familiar with these notions, we provide a second proof in Appendix A. This proof is less mathematically enlightening but it has the advantage of being quite elementary and self-contained, using only pseudo-bases and the Hermite Normal Form.

Main results 1 can be used algorithmically to compute short vectors in a G-stable module M. The idea is to compute short vectors in the $\mathcal{O}_{K'}$-module $M' = M \cap \mathcal{O}_{K'}^n$, which has a smaller dimension. Unfortunately, we are not able to use this strategy to solve the (approximate) Shortest Vector Problem in M, because we do not have sufficiently good bounds relating the first minimum of M to the first minimum of M'. But we do have tight bounds relating the root determinant of M with the root determinant of M', hence we can use the strategy hinted at above to solve the (approximate) Hermite Shortest Vector Problem (γ-HSVP). This problem asks, given as input a lattice L of rank r, to output a non-zero vector of L whose Euclidean norm is at most $\gamma \cdot \det(L)^{1/r}$. Overall, we prove the following result.

Main result 2 (Informal formulation, see Theorem 4). *There is an algorithm that takes as input a module $M \subseteq \mathcal{O}_K^n$ of rank n (for some $n > 0$) whose discriminant is non-ramified, and a parameter $\gamma \geq 1$, and solves γ-HSVP in M by running a γ-HSVP solver on a $\mathbb{Z}$-lattice of rank nd/d_M, where d_M is the number of automorphisms of K fixing M as a set.*

[7] 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.

Remark that the algorithm from Main result 2 is more efficient when the number of automorphisms d_M fixing the module M is large. This quantity is at most as large as d, the degree of the field K. Hence, while our result remains valid for number fields of any degree and modules of any rank, it would be more useful for modules of small ranks (e.g., constant rank) over a large degree number field. In the case of modules of constant rank and fields whose degree d tends to infinity, our algorithm may have a runtime as small as polynomial if the module is stabilized by a group of automorphisms whose size is a constant fraction of d. On the other hand, if the degree d of K is fixed and the rank n of M tends to infinity, then our algorithm will always have an exponential runtime for polynomial approximation factors γ (but the constant in the exponent may be decreased in cases where M is stabilized by some automorphisms).

Main results 1 and 2 are the central contributions of this article. In addition to these results, we also make the following observation: when a module M is G-stable, then there is a simple (non-tight) relation between the Euclidean norm of a shortest non-zero vector of M and the one of $M \cap \mathcal{O}_{K'}^n$. The proof of this relation is quite elementary, requiring only the trace form, and does not require any assumption on the discriminant of the module M. Using this, we are able to describe an algorithm that solves approximate-SVP in M, by solving approximate-SVP in $M \cap \mathcal{O}_{K'}^n$, which has a smaller dimension. Unlike the previous results for HSVP, we now have a loss in the approximation factor. More precisely, we prove the following result.

Main result 3 (Informal and specialized formulation, see Theorem 1 and Lemma 6). *Let K be a power-of-two cyclotomic number field of degree d. There is an algorithm that takes as input a module $M \subseteq \mathcal{O}_K^n$ of rank n and a parameter $\gamma \geq 1$, and solves $(d \cdot \gamma)$-SVP in M by running a γ-SVP solver on a $\mathbb{Z}$-lattice of rank at most nd/d_M, where d_M is the number of automorphisms of K fixing M as a set.* [8]

This result applies even if the discriminant of M is ramified, and has a simpler proof than Main result 2. On the negative side, the reduction induces a loss of a factor d (or even $d\Delta_K^{1/d}$ for arbitrary number fields) on the approximation factor, whereas Main result 2 had no loss. We also believe that the proof of Main result 2 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 might be useful to solve other algorithmic problems, such as the closest vector problem or the bounded distance decoding problem.

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 consists in forgetting about the module structure of the lattice and running plain lattice reduction algorithm (such as the BKZ algorithm) on it. In particular, the modules that are obtained from random instances of NTRU, Ring

[8] 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 can be as large as $d\Delta_K^{1/d}$.

or Module-LWE are very unlikely to be fixed by any automorphism of K other than 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 warning sign e.g., for future designers who may wish to introduce such symmetries for the sake of performance. For example, a variant of Ring-LWE where the elements a_i are chosen with certain symmetry properties (e.g., $\overline{a_i} = a_i$) would be a bad idea, even if the secret s and the error terms e_i do not have any symmetries. This is because the lattice associated to the Ring-LWE problem only depends on the elements a_i and the modulus $q \in \mathbb{Z}$. So if the a_i's were to be chosen in a subfield of K, then the associated lattice would become G-stable for a non-trivial group G and one could use our algorithm to find a short vector of this lattice (or rather its dual), which would enable to solve the (decision) Ring-LWE problem.

We also note that G-stable modules appeared in recent cryptographic constructions, albeit not in the context of the (Hermite) shortest vector problem. Indeed, the signature scheme Hawk [8], which was selected for the second round of NIST's additional call for digital signatures,[9] relies on the hardness of the module Lattice Isomorphism Problem (module-LIP) in the module lattice $M = \mathcal{O}_K^2$. This is typically a G-stable module for the group G consisting of all automorphisms of K (i.e., a very large group G). The module-LIP problem for a rank-n module M asks, given a Gram matrix $\mathbf{Q} \in \mathcal{O}_K^{n\times n}$, to recover a basis $\mathbf{B}$ of M such that $\mathbf{Q} = \overline{\mathbf{B}}^T\mathbf{B}$, with the guarantee that such a $\mathbf{B}$ exists (i.e., it asks to factor the Gram matrix $\mathbf{Q}$ into a basis of M). In Hawk's case, $M = \mathcal{O}_K^2$ has rank 2 and $K' = \mathbb{Q}$. If we were able to extend our Main result 2 to the lattice isomorphism problem and reduce the LIP problem in $M = \mathcal{O}_K^2$ to the LIP problem in $M \cap \mathbb{Z}^2$, this would be devastating for the signature scheme Hawk, since we would end up in a lattice of dimension only 2 (over $\mathbb{Z}$). However, we emphasize that extending our Main result 2 to the LIP problem seems far from trivial. One of the reasons of this difficulty seems to be the fact that the Gram matrix $\mathbf{Q}$ only represents the module M up to (K-)isometries, but the G-stability property is not preserved by (K-)isometries. Hence, it seems hard to exploit the G-stability of M given only the Gram matrix $\mathbf{Q}$. As another hint that this generalization is probably hard, we note that a recent article by van Gent and Pulles [10] suggests that recovering even a single non-trivial automorphism of M when given as input the Gram matrix $\mathbf{Q}$ seems to be a hard problem (for some definition of "non-trivial" defined in [10]).

Open problems. A natural question left open by this work is whether Main result 1 can be used to solve other algorithmic problems than the Hermite shortest vector problem, via a reduction to the subfield. In other words, once we know that a module M is an inflated module from a subfield K', can we use it to reduce some algorithmic problem $\mathcal{P}$ in M to $\mathcal{P}$ in $M' := M \cap \mathcal{O}_{K'}^n$. We partially solve this question for the shortest vector problem, but our reduction induces some loss on the approximation factor γ, which is not fully satisfactory.

[9] https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures

We mentioned earlier this question for the closest vector problem (CVP) and the bounded distance decoding problem (BDD). Let us emphasize that this generalization is far from immediate, since the target vector of CVP and BDD may not belong to the subfield K'. In [5, Se. 4.2], the authors solved (a variant of) BDD in G-stable ideals, by reducing it to SVP in another G-stable ideal, but this induces a loss on the approximation factor (due to the BDD to SVP reduction). We let open the question of reducing CVP/BDD in M directly to CVP/BDD in $M' = M \cap O_{K'}^n$.

Another important algorithmic problem to consider would be the lattice isomorphism problem, as described above (i.e., in its formulation "factoring a Gram matrix"). As we discussed above, this would have a strong impact on the signature scheme Hawk, but it seems far from easy to obtain.

Organization of the paper. In Section 3, we start by proving Main result 3, which is the simplest of our results, and requires little mathematical background, in addition to being independent from the other results of this article. We then prove Main result 1 in Section 4 (recall that we also provide a more elementary proof of this result in Appendix A, for readers who are not familiar with the mathematical objects used in Section 4). Finally, we use Main result 1 to prove Main result 2 in Subsection 4.1.

2 Preliminaries

In this article, we suppose that the reader is familiar with the notion of lattices and number fields (including Galois theory and localization). More detailed preliminaries can be found in [5], and more details about localization can be found in [2].

We encode a (finitely generated) free abelian group as its rank r and its elements as a vector in $\mathbb{Z}^r$. We encode a $\mathbb{Z}$-linear map between free abelian groups (seen as $\mathbb{Z}$-modules) as an integer matrix in the natural way. A subgroup is encoded as the image of an injective map. A ring structure on a free abelian group is encoded as a multiplication map for each basis element. If R is such a ring, we similarly encode an R-module structure on a free abelian group M as a linear map $R \to \mathrm{Hom}_{\mathbb{Z}}(M, M)$. We will use the same conventions, mutatis mutandis, for $\mathbb{Q}$-vector spaces.

2.1 Lattices

For a lattice $L \subset \mathbb{R}^m$ of rank n, we write $\lambda_1(L) := \min\{\|\mathbf{v}\| \mid \mathbf{v} \in L \setminus \{0\}\}$ its *first minimum*, and let $\det(L) = \sqrt{\det(\mathbf{B}^T\mathbf{B})}$ be its *determinant*, where $\mathbf{B}$ is any basis of L.

Definition 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 $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(L)$. 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 $\|\mathbf{v}\| \leq \gamma \cdot \sqrt{n} \cdot \det(L)^{1/n}$.*

Minkowski's first theorem states that $\lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$ for any rank-n lattice L. Consequently, for all $\gamma \geq 1$ a solution to γ-HSVP always exists, and γ-HSVP reduces to γ-SVP in the same lattice.

When we want to find short vectors in a lattice, we can use the BKZ algorithm, which gives us different trade-offs between runtime and approximation factor. Below, we recall the provable complexity of variants of the BKZ algorithm. Note that the provable complexity statement only applies when the lattice L has rational coefficients, which will not be our case here. Still, this statement provides some intuition about the runtime needed to solve γ-SVP in lattices of rank n.

Lemma 1 ([11, Theorem 1] and [1, Theorem D.1]). *There is a probabilistic algorithm that takes as input a basis $\mathbf{B}_L \subset \mathbb{Q}^{n\times n}$ 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 [11, 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 [11, Theorem 1]). □

The following lemma states that the intersection of a lattice with a subspace can be computed efficiently. A proof can be found in, e.g., [5, Lemma A.1].

Lemma 2. *There exists a polynomial-time algorithm that, given basis of a lattice $L \subset \mathbb{Q}^m$ and a subspace $V \subseteq \mathbb{Q}^m$, computes a basis of the intersection lattice $L \cap V$.*

2.2 Number fields

For a number field K, write O_K for its *maximal order* and Δ_K for the absolute value of its discriminant. For an extension of number fields K/K', write $\mathrm{Tr}_{K/K'}$ and $N_{K/K'}$ for the relative *trace* and *norm* respectively. Some of our proofs rely on *localization*. We have made sure to confine its occurrence to proofs only, with the singular exception of Lemma 14, so that a reader that is inexperienced with this technique should still be able to understand all theorem statements.

The following lemma will help us relate the discriminants of a field K and of one of its subfields K'.

Lemma 3 (e.g., Exercice 23 in [16]). *Let K/K' be an extension of number fields of degrees d and d' respectively. Then $\Delta_K^{1/d} \geq \Delta_{K'}^{1/d'}$.*

In this article, we see O_K-modules (included in K^n) as lattices. This is done thanks to the following inner product.

Definition 2. *Let K be a number field of degree d. We equip K with the inner product*

$$\langle x, y\rangle_K = \frac{1}{d}\sum_{\sigma:K\to\mathbb{C}} \sigma(x)\overline{\sigma(y)},$$

where the σ ranges over all d embeddings of K into $\mathbb{C}$. We extend the inner product to K^m in the natural way and write $\|x\|_K = \sqrt{\langle x, x\rangle_K}$.

We note that the above inner product equips O_K (and by extension any finitely generated O_K-module in K^m) with a lattice structure. We will hence use lattice related quantities, such as $\det(M)$ or $\lambda_1(M)$ for modules $M \subseteq K^m$, which correspond to the determinant or first minimum of M when seen as a Euclidean lattice via the above inner product.

It is important to note however that the geometry induced by the inner product above does not correspond exactly to the usual geometry used in module lattice-based cryptography (one usually uses the geometry induced by the canonical embedding). The two geometries differ by a scaling factor $\sqrt{d}$ (where d is the degree of K), hence there are immediate reductions for solving SVP/HSVP between the two different geometries. In other words, an algorithm solving γ-(H)SVP for our choice of inner product immediately gives an algorithm solving γ-(H)SVP (with the same complexity) for the usual choice of inner product (and vice versa).

The following lemma justifies our choice of this slightly non standard inner product. It will also allow us to drop the subscript K from the notation of the inner product.

Lemma 4. *Let K/K' be an extension of number fields and let $x, y \in K'$. Then $\langle x, y\rangle_K = \langle x, y\rangle_{K'}$.*

Proof. The restriction map $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \to \mathrm{Hom}_{\mathbb{Q}}(K', \mathbb{C})$ is surjective, and each map $K' \to \mathbb{C}$ has exactly $[K : K']$ preimages. Hence for $x, y \in K'$ we obtain

$$\frac{1}{[K' : \mathbb{Q}]}\sum_{\sigma:K'\to\mathbb{C}} \sigma(x)\overline{\sigma(y)} = \frac{1}{[K' : \mathbb{Q}]}\sum_{\tau:K\to\mathbb{C}} \frac{\tau(x)\overline{\tau(y)}}{[K : K']} = \frac{1}{[K : \mathbb{Q}]}\sum_{\tau:K\to\mathbb{C}} \tau(x)\overline{\tau(y)},$$

as was to be shown. □

The determinant of O_K when seen as a lattice with our inner product $\langle\cdot,\cdot\rangle_K$ is given in the following lemma. Note the unusual factor $d^{-d/2}$ in the right-hand-side, which comes from the fact that our inner product is scaled by a factor d^{-1}, compared to the more standard one.

Lemma 5. *Let K be a number field. Then* $\det(O_K) = \sqrt{\Delta_K} \cdot d^{-d/2}$.

We also consider an infinity norm on K, defined by $\|x\|_\infty = \max_{\sigma:K\to\mathbb{C}} |\sigma(x)|$, where σ ranges over all embeddings from K to $\mathbb{C}$. For a subfield $K' \subseteq K$ we define $\delta_{K/K'}$ to be the minimal $r \in \mathbb{R}_{\geq 0}$ such that the $\mathcal{O}_{K'}$-module generated by $\{x \in \mathcal{O}_K \mid \|x\|_\infty \leq r\}$ has full rank in $\mathcal{O}_K$. The following lemma relates this quantity with some more standard field-related objects.

Lemma 6. *For any extension of number fields K/K', we have $1 \leq \delta_{K/K'} \leq \delta_{K/\mathbb{Q}} \leq \Delta_K^{1/d}$. 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 $\|\alpha\|_\infty \geq 1$, since $|N_{K/\mathbb{Q}}(\alpha)| \geq 1$ is the product of the complex embeddings of α. In particular, we obtain the first inequality. For the second, note that any set that generates $\mathcal{O}_K$ over $\mathbb{Z}$ also generates $\mathcal{O}_K$ over $\mathcal{O}_{K'}$. The third we know from [3] and [4, Theorem A.4] ([3] gave an asymptotic result and [4, Theorem A.4] made the constant explicit).

In the case of a cyclotomic number field $K = \mathbb{Q}(\zeta)$, the set $\{\zeta^i \mid i \geq 0\}$ generates $\mathcal{O}_K$ as a $\mathbb{Z}$-module, and $\|\zeta^i\|_\infty = 1$ for all i. □

Lemma 7 (Trace pairing). *Let K/K' be an extension of number fields. Then the trace $\mathrm{Tr}_{K/K'} : K \to K'$ is surjective and the K'-bilinear form $K \times K \to K'$ given by $(x, y) \mapsto \mathrm{Tr}_{K/K'}(xy)$, the* trace pairing*, is non-degenerate.*

Definition 3 (Discriminant). *Let K be a number field and $M \subset K^m$ be a rank-n module. Let $\varphi : K \times K \to K$ be the K-valued bilinear form defined by $\varphi(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^m x_i y_i$ where $\mathbf{x} = (x_1, \ldots, x_m)$ and $\mathbf{y} = (y_1, \ldots, y_m) \in K^m$. The* (ideal) discriminant *of M is the fractional $\mathcal{O}_K$-ideal*

$$\mathrm{disc}_K(M) = \sum_{(\mathbf{b}_1,\ldots,\mathbf{b}_n)} \mathcal{O}_K \cdot \det(\varphi(\mathbf{b}_i, \mathbf{b}_j))_{1\leq i,j\leq n}$$

where the sum ranges over all K-linearly independent tuples in M^n.

Lemma 8. *Let K be a number field of degree d and let $M \subset K^n$ be an $\mathcal{O}_K$-module of rank n (i.e., M has full rank). Then*

$$\det(M)^2 = N_{K/\mathbb{Q}}(\mathrm{disc}_K(M)) \cdot \Delta_K^n \cdot d^{-dn}.$$

Proof. Note that $\det(aM) = a^{dn} \det(M)$ for all $a \in \mathbb{Z}$ and $\mathrm{disc}_K(aM) = a^{2n}\mathrm{disc}_K(M)$ for all integers $a \in \mathbb{Z}$. Hence by scaling with integers we may assume without loss of generality that $M \subseteq \mathcal{O}_K^n$. Additionally, we may prove this equality locally, hence we may assume without loss of generality that M is free with basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Let $T : \mathcal{O}_K^n \to M$ be the corresponding basis transformation. Note that $\det(M)^2 = \det(\mathcal{O}_K^n)^2 \cdot \#(\mathcal{O}_K^n/M)^2 = \Delta_K^n \cdot d^{-dn} \cdot \det_{\mathbb{Q}}(T)^2$ by Lemma 5. Then $\mathrm{disc}_K(M) = \mathrm{disc}_K(\mathcal{O}_K^n) \cdot \det_K(T)^2 = \det_K(T)^2$ and $N_{K/\mathbb{Q}}(\mathrm{disc}_K(M)) = N_{K/\mathbb{Q}}(\det_K(T)^2) = \det_{\mathbb{Q}}(T)^2 = \Delta_K^{-n} \cdot d^{dn} \cdot \det(M)^2$, as was to be shown. □

Note that Lemma 8 only holds for full rank modules. It can fail when the module is not of full rank because the bilinear form φ in the definition of $\mathrm{disc}_K(M)$ need not be 'definite', i.e., there can be non-zero vectors x such that $\varphi(x,x) = 0$. For an explicit example, take $K = \mathbb{Q}[i]$ and $M = \mathcal{O}_K \cdot \mathbf{v} \subset K^2$ with $\mathbf{v} = (1\ i)^T$. Then $\mathrm{disc}_K(M) = \det(\mathbf{v}^T\mathbf{v})\mathcal{O}_K = \{0\}$ is the zero ideal. But M is not the zero lattice, so $\det(M) \neq 0$ and the formula from Lemma 8 cannot hold.

Definition 4 (Ramification). *Let K/K' be an extension of number fields and let $\mathfrak{p}$ be a prime of K, i.e. a maximal ideal of $\mathcal{O}_K$, and $\mathfrak{p}' = \mathfrak{p} \cap K'$. The* ramification index *$e_{K/K'}(\mathfrak{p})$ of $\mathfrak{p}$ over K' is the exponent of $\mathfrak{p}$ in the factorization of $\mathcal{O}_K \cdot \mathfrak{p}'$. We say $\mathfrak{p}$ is* ramified (over K') *if $e_{K/K'}(\mathfrak{p}) > 1$. We say $\mathfrak{p}$ is* tamely ramified *if $\mathfrak{p}$ is ramified and $e_{K/K'}(\mathfrak{p})$ is coprime to $\#(\mathcal{O}_K/\mathfrak{p})$. A ramified prime that is not tamely ramified is said to be* wildly ramified.

Lemma 9. *Let K/K' be an extension of number fields and let $\mathfrak{p}'$ be a prime of K'. Then every prime of K above $\mathfrak{p}'$ is wildly ramified over K' if and only if $\mathrm{Tr}_{K/K'}(\mathcal{O}_K) \subseteq \mathfrak{p}'$.*

Note that if K/K' is Galois, then if a prime of K above $\mathfrak{p}'$ is wildly ramified, then all primes above $\mathfrak{p}'$ are, since the Galois group acts transitively on the primes above $\mathfrak{p}'$.

Proof. Let $p \in \mathbb{Z}$ be the prime dividing $\#(\mathcal{O}_{K'}/\mathfrak{p}')$.

($\Rightarrow$) By assumption there is some ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K\mathfrak{p}' = \mathfrak{a}^p$. Let $a \in \mathcal{O}_K$ be a generator for $\mathfrak{a}/\mathcal{O}_K\mathfrak{p}'$, which exists since $\mathfrak{a}$ is invertible and $\mathcal{O}_K/\mathfrak{p}'\mathcal{O}_K$ is semi-local. Then $\mathcal{O}_K/\mathfrak{p}'\mathcal{O}_K \cong \bigoplus_{i=0}^{p-1} \mathfrak{a}^i/\mathfrak{a}^{i+1} \cong \bigoplus_{i=0}^{p-1} a^i\mathcal{O}_K/a^i\mathfrak{a} \cong (\mathcal{O}_K/\mathfrak{a})^p$ as $(\mathcal{O}_{K'}/\mathfrak{p}')$-vector spaces. The multiplication action of $x \in \mathcal{O}_K/\mathfrak{p}'\mathcal{O}_K$ on the latter representation is given by an upper triangular matrix with each diagonal entry equal to $x \pmod{\mathfrak{a}}$. Hence $\mathrm{Tr}_{K/K'}(x)$ is a multiple of p modulo $\mathfrak{a}$.

($\Leftarrow$) Factor $\mathcal{O}_K\mathfrak{p}' = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$. Let $x_i \in \mathcal{O}_K$ satisfying $\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}_i)/(\mathcal{O}_{K'}/\mathfrak{p}')}(x_i) \equiv 1 \pmod{\mathfrak{p}'}$ and $x_i \equiv 0 \pmod{\mathfrak{p}_j^{e_j}}$ for all $j \neq i$. Then $0 \equiv \mathrm{Tr}_{K/K'}(x_i) \equiv e_i \pmod{\mathfrak{p}'}$, so $\mathfrak{p}_i$ is wildly ramified over K'. □

2.3 Contracting and extending modules

For a group G acting on a set X we write $X^G = \{x \in X \mid (\forall\, g \in G)\ g(x) = x\}$. We say a subset $Y \subseteq X$ is G-stable if $g(Y) := \{g(y) \mid y \in Y\} \subseteq Y$ for all $g \in G$. In this article, we will only consider the case where G is a subgroup of the automorphisms group $\mathrm{Aut}_{\mathbb{Q}}(K)$, and $X = M \subseteq K^m$ is an $\mathcal{O}_K$-module. In this case, we consider the natural action of $g \in \mathrm{Aut}_{\mathbb{Q}}(K)$ on vectors of K^m by applying g coordinate-wise. Let K/K' be a Galois extension with Galois group G, and let $M \subseteq K^m$ be a rank-n $\mathcal{O}_K$-module. The set $M^G = M \cap (K')^m$ is what we call the contraction of the module M inside the subfield K'. Reciprocally, for a module $M' \subset (K')^m$, the extension of M' to K is the module $\mathcal{O}_K \cdot M' := \left\{\sum_{i=1}^r x_i\mathbf{v}_i \mid r > 0, \mathbf{v}_i \in M', x_i \in \mathcal{O}_K\right\} \subset K^m$.

In the case when $M = I$ is an ideal of $\mathcal{O}_K$ (i.e., $m = n = 1$), it was proven in [5] that (under some ramification condition), contracting and then extending a G-stable ideal recovers the ideal we started from. We recall this result below.

Lemma 10 ([5, Le. 3.3]). *Suppose K/K' is Galois with Galois group G, and let $\mathcal{O}_K$ be the maximal order of K. Let I be an ideal of $\mathcal{O}_K$, not divisible by any ramified prime of K/K'. If I is G-stable, then $I = I^G \cdot \mathcal{O}_K$.*

We remark that this lemma holds even when we localize $\mathcal{O}_K$ at any multiplicative set of non-zero elements of $\mathcal{O}_{K'}$, which will be of particular interest for the proof of Theorem 3.

The discriminant of a module behaves nicely when we extend the module to a larger field, as stated in the following lemma.

Lemma 11. *Let K/K' be an extension of number fields and suppose $M' \subseteq (K')^m$ is an $\mathcal{O}_{K'}$-module. Let $M = \mathcal{O}_K \cdot M' \subseteq K^m$ be the extension of M' to K. Then* $\mathrm{disc}_K(M) = \mathcal{O}_K \cdot \mathrm{disc}_{K'}(M')$.

Proof. We may prove equality of the two ideals locally at the primes $\mathfrak{p}'$ of $\mathcal{O}_{K'}$. Let $\mathfrak{p}'$ be such a prime. We write $X_{\mathfrak{p}'}$ for the localization of X at $\mathfrak{p}'$. Then $\mathcal{O}_{K',\mathfrak{p}'}$ is local and hence $M'_{\mathfrak{p}'}$ has an $\mathcal{O}_{K',\mathfrak{p}'}$-basis $\mathbf{b} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Then $\mathrm{disc}_K(M')_{\mathfrak{p}'} = \mathcal{O}_{K',\mathfrak{p}'} \cdot \det(\varphi(\mathbf{b}_i, \mathbf{b}_j))_{1 \le i,j \le n}$ (where φ is as in Definition 3), since for any other linearly independent set the determinant is an $\mathcal{O}_{K',\mathfrak{p}'}$-multiple. However, $\mathbf{b}$ is an $\mathcal{O}_{K,\mathfrak{p}'}$-basis for M, so here we obtain the same expression with K and M instead of K' and M', from which the lemma follows. □

The next lemma states that, given as input a module M, one can efficiently compute all K-automorphisms stabilizing M as a set, as well as the subfield fixed by these automorphisms.

Lemma 12. *There exists a polynomial-time algorithm that, given a number field K and an $\mathcal{O}_K$-module $M \subseteq K^m$ for some $m \ge 0$, computes*

$$G = \{g \in \mathrm{Aut}_{\mathbb{Q}}(K) \mid g(M) = M\},$$

as well as K^G and M^G. This group G is the largest subgroup of $\mathrm{Aut}_{\mathbb{Q}}(K)$ such that M is G-stable.

Proof. We may compute some $\alpha \in K$ such that $\mathbb{Q}(\alpha) = K$ and in turn, using [14], all roots $\beta_1, \ldots, \beta_r \in K$ of the minimal polynomial of α, each of which corresponds to an automorphism $\alpha \mapsto \beta_i$ of K. Hence we may compute $\mathrm{Aut}_{\mathbb{Q}}(K)$. In turn, we may compute G. By Lemma 7 we may compute K^G as the image of $x \mapsto \sum_{g \in G} g(x)$. Finally, $M^G = M \cap (K^G)^m$ is obtained by intersecting a lattice with a subspace, using Lemma 2. □

3 Solving approximate-SVP via the trace map

Lemma 13. *Let K/K' be a Galois extension of number fields with Galois group G and suppose $M \subseteq K^m$ is a G-stable $\mathcal{O}_K$-submodule of rank $n > 0$. Then*

1. *for every non-zero* $\mathbf{x} \in M$ *there exists an* $\alpha \in \mathcal{O}_K$ *such that* $\|\alpha\|_\infty \leq \delta_{K/K'}$ *and* $\mathrm{Tr}_{K/K'}(\alpha\mathbf{x}) \neq 0$,
2. *the* $\mathcal{O}_{K'}$*-module* M^G *is non-zero of rank at most* n.

Proof. (1) Let $\alpha_1, \ldots, \alpha_{[K:K']} \in \mathcal{O}_K$ be K'-linearly independent such that $\|\alpha_i\|_\infty \leq \delta_{K/K'}$, which exist by definition of $\delta_{K/K'}$. Let j be such that $\mathbf{x}_j \neq 0$, which exists because $\mathbf{x} \neq 0$. By Lemma 7 there exists some i such that $\mathrm{Tr}_{K/K'}(\alpha_i \mathbf{x}_j) \neq 0$ and consequently $\mathrm{Tr}_{K/K'}(\alpha_i \mathbf{x}) \neq 0$, as was to be shown.

(2) We have $0 \subsetneq \mathrm{Tr}_{K/K'}(M) \subseteq M^G$ by (1) (for the first inclusion) and by the G-stability of M (for the second inclusion). Note that the rank r of M^G as $\mathcal{O}_{K'}$-module equals the dimension of $K' \cdot M^G$ as K'-vector space. Choose some K'-basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ of $K' \cdot M^G$ and suppose that $\sum_i \alpha_i \mathbf{b}_i = 0$ for some $\alpha_1, \ldots, \alpha_r \in K$. Then

$$0 = \mathrm{Tr}_{K/K'}(\beta \sum_i \alpha_i \mathbf{b}_i) = \sum_i \mathrm{Tr}_{K/K'}(\alpha_i \beta)\mathbf{b}_i$$

for all $\beta \in K$. It follows that $\mathrm{Tr}_{K/K'}(\alpha_i \beta) = 0$ for all $\beta \in K$ and i. By Lemma 7 we have $\alpha_i = 0$ for all i. Hence $\mathbf{b}_1, \ldots, \mathbf{b}_r$ is a K-basis of $K \cdot M^G \subseteq K \cdot M$, and $r \leq n$. □

Theorem 1. *There is an algorithm that takes as input the ring of integers* $\mathcal{O}_K$ *of a number field* K *of degree* d*, an* $\mathcal{O}_K$*-submodule* $M \subseteq K^m$ *of rank* n *for some integers* $m \geq n > 0$*, and a parameter* $\gamma' \geq 1$*, and solves* γ*-SVP in* M *by making one call to an oracle solving* γ'*-SVP in* $\mathbb{Z}$*-lattices of rank* $\leq nd/d_M$*, where* $d_M = \#\{g \in \mathrm{Aut}_{\mathbb{Q}}(K) \mid g(M) = M\}$ *and* $\gamma = d_M \cdot \delta_{K/\mathbb{Q}} \cdot \gamma'$*. Except for the oracle call, the algorithm runs in polynomial time in its input size.*

The call to the oracle solving γ-SVP in lattices of rank nd/d_M can be implemented using the BKZ algorithm. In our case however, the lattice we want to run BKZ on has real coefficients, so the complexity analysis of the BKZ algorithm from Lemma 1 does not apply directly. By carefully rounding the coordinates of the lattice, it should be possible to achieve a runtime similar to that in Lemma 1, but this is beyond the scope of this article. We also note that in the case where K is a CM field (including the totally real case), then all the inner products between vectors of the lattice are rational, i.e., the Gram matrix of any basis of the lattice has rational coefficients, even though the basis itself does not have rational coefficients. This should be sufficient to have provable complexities for (variants of) the BKZ algorithm.

Proof. Let $G = \{g \in \mathrm{Aut}_{\mathbb{Q}}(K) \mid g(M) = M\}$. We will show that $\lambda_1(M^G) \leq d_M \cdot \delta_{K/\mathbb{Q}} \cdot \lambda_1(M)$, from which it will follow that any solution to γ'-SVP in M^G is a solution to γ-SVP in M. The algorithm from the theorem will simply compute M^G (in polynomial time thanks to Lemma 12), then run the γ'-SVP oracle on M^G, and output the vector returned by the oracle.

Note that M is G-stable by definition of G, and the extension K/K^G is Galois with Galois group G, hence, we can use Lemma 13. Let $\mathbf{x} \in M$ be a shortest non-zero vector and let $\alpha \in \mathcal{O}_K$ be as in Lemma 13 (1). Then $\mathbf{y} := \mathrm{Tr}_{K/K^G}(\alpha \mathbf{x}) \in M^G$ by G-stability of

M, and is non-zero by Lemma 13 (1). Moreover, it satisfies

$$\|\mathbf{y}\| \leq \sum_{g \in G} \|g(\alpha \mathbf{x})\| = d_M \cdot \|\alpha \mathbf{x}\| \leq d_M \cdot \|\alpha\|_\infty \cdot \|\mathbf{x}\| \leq d_M \cdot \delta_{K/K^G} \cdot \lambda_1(M),$$

where we used the fact that for any $\mathbf{x} \in K^m$, and any $g \in \mathrm{Aut}_{\mathbb{Q}}(K)$, $\|g(\mathbf{x})\| = \|\mathbf{x}\|$. Using the fact that $\delta_{K/K^G} \leq \delta_{K/\mathbb{Q}}$ (see Lemma 6) proves that $\lambda_1(M^G) \leq d_M \cdot \delta_{K/\mathbb{Q}} \cdot \lambda_1(M)$ as desired.

Finally, by Lemma 13 (2), M^G in an $\mathcal{O}_{K^G}$-module of rank at most n, hence a $\mathbb{Z}$-lattice of rank at most nd/d_M (since K^G is a field of degree d/d_M), which proves that the oracle is indeed called on a $\mathbb{Z}$-lattice of rank $\leq nd/d_M$. □

4 Contracting and extending a module

In this section we first give a proof of Theorem 3, which states that contracting and then extending a G-stable module recovers the original module (under some condition on the discriminant of the module). We then use this result in Theorem 4, to describe an algorithm solving γ-HSVP in a G-stable module. The proof provided here is quite natural from a mathematical point of view, but requires some background on projective modules and localization. An alternative proof to Theorem 3 is available in Appendix A, using more elementary notions (which are recalled in the appendix).

Lemma 14. *Let R be a commutative ring, S an R-algebra, and $f : M \to N$ an S-module homomorphism with N finitely presented. Then f has a right inverse if and only if the localization $f_{\mathfrak{m}}$ has a right inverse for every maximal ideal $\mathfrak{m}$ of R.*

Note that S need not be commutative. If S is a Noetherian ring and N is finitely generated, then N is finitely presented.

Proof. Note that f has a right inverse if and only if the map $\mathrm{Hom}_S(N, M) \to \mathrm{Hom}_S(N, N)$ given by $g \mapsto f \circ g$ is surjective. Moreover, surjectivity holds if and only if it holds locally at the maximal ideals $\mathfrak{m} \subset R$. Thus it suffices to show that the natural map $\mathrm{Hom}_S(A, B)_{\mathfrak{m}} \to \mathrm{Hom}_{S_{\mathfrak{m}}}(A_{\mathfrak{m}}, B_{\mathfrak{m}})$ for S-modules A and B is an isomorphism when A is finitely presented. By the assumption on A there exists an exact sequence $S^s \to S^t \to A \to 0$. We obtain the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_S(A, B)_{\mathfrak{m}} & \longrightarrow & B_{\mathfrak{m}}^t & \longrightarrow & B_{\mathfrak{m}}^s \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}_{S_{\mathfrak{m}}}(A_{\mathfrak{m}}, B_{\mathfrak{m}}) & \longrightarrow & B_{\mathfrak{m}}^t & \longrightarrow & B_{\mathfrak{m}}^s
\end{array}$$

where the exact rows are given by applying the hom and localization functors to the original sequence in different orders, and using the natural isomorphism $\mathrm{Hom}_S(S^n, B) \cong B^n$. The claim now follows from the five-lemma. □

Theorem 2. *Let K/K' be a Galois extension of number fields with Galois group G, let $\mathcal{O} \subseteq K$ be a Dedekind domain containing $\mathcal{O}_K$, and let $M \subseteq \mathcal{O}^n$ be a $\mathcal{O}$-submodule of rank n whose discriminant $\operatorname{disc}_K(M)$ is coprime to any prime of K' that is wildly ramified in $\mathcal{O}$. If M is G-stable, then there are rank-1, G-stable $\mathcal{O}$-submodules $M_1, \dots, M_n \subseteq M$ yielding the internal direct sum decomposition $M = M_1 \oplus \cdots \oplus M_n$.*

Proof. Let $\mathcal{O}' = K' \cap \mathcal{O}$. Consider the twisted group $\mathcal{O}'$-algebra $R = \mathcal{O}\langle G \rangle$, whose additive group is a free left-$\mathcal{O}$-module with basis G and where multiplication is given by $xg \cdot yh = (xg(y))(gh)$ for $x, y \in \mathcal{O}$ and $g, h \in G$. Note that $\mathcal{O}$ and hence $\mathcal{O}^n$ are R-modules in a natural way. Moreover, an $\mathcal{O}$-submodule of $\mathcal{O}^n$ is G-stable if and only if it is an R-submodule.

Consider any coordinate projection $\mathcal{O}^n \to \mathcal{O}$ and let $\pi : M \to N$ be its surjective restriction. Note that π is an R-module homomorphism since M is G-stable. It suffices to show that π has a right-inverse as R-module homomorphism, because then N is a rank-1, G-stable direct summand of M by the splitting lemma and we are done by induction. By Lemma 14, we may assume $\mathcal{O}'$ is local with maximal ideal $\mathfrak{p}$.

Suppose that $\mathfrak{p}$ ramifies wildly in $\mathcal{O}$. Then by assumption $\mathfrak{p}$ is coprime to $\operatorname{disc}_K(M)$. Hence $\operatorname{disc}_K(M) = \mathcal{O}$, so $M = \mathcal{O}^n$. In this case π clearly has a right-inverse.

Suppose now that $\mathfrak{p}$ is tame in $\mathcal{O}$. Then the trace map $\operatorname{Tr} : \mathcal{O} \to \mathcal{O}'$ is surjective by Lemma 9, so let $\alpha \in \mathcal{O}$ be such that $\operatorname{Tr}(\alpha) = 1$. Note that N is an ideal of $\mathcal{O}$ and hence a projective $\mathcal{O}$-module, so π considered as an $\mathcal{O}$-module homomorphism has a right-inverse r. Consider the map $\rho : N \to M$ given by

$$n \mapsto \sum_{g \in G} g(\alpha) \cdot (g \circ r \circ g^{-1})(n).$$

One easily verifies that ρ is an R-module homomorphism. Since π commutes with G, we obtain $(\pi \circ \rho)(n) = \sum_{g \in G} g(\alpha) \cdot n = n$ for all $n \in N$, so ρ is a right-inverse of π, which finishes the proof. □

The assumption that the discriminant is not wildly ramified cannot be omitted in Theorem 2, as the following proposition shows.

Proposition 1. *Let K/K' be a Galois extension of number fields with Galois group G and suppose there is a prime of K that ramifies wildly and completely over K'. Then there exists some G-stable $\mathcal{O}_K$-submodule of $\mathcal{O}_K^n$ that is not a direct sum of rank-1 G-stable submodules.*

Proof. Let $\alpha \in \mathcal{O}_K$ be such that $\{g(\alpha) \mid g \in G\}$ is a K'-basis of K. Note that $g(\alpha)/\alpha \in \mathcal{O}_{K,\mathfrak{p}}^*$ for all $g \in G$ since $\mathfrak{p}$ is the unique prime of $\mathcal{O}_K$ above $\mathfrak{p}'$. We may then choose $\beta \in \mathcal{O}_K \setminus \mathfrak{p}$ such that $\beta g(\alpha)/\alpha \in \mathcal{O}_K$ for all $g \in G$. Consider the $\mathcal{O}_K$-submodule $M \subseteq F = \prod_{g \in G} \mathcal{O}_K$ generated by $\mathbf{v} = (\beta/\alpha) \cdot (g(\alpha))_{g \in G}$ and its G-conjugates. Note that $\mathbf{v}$ and its conjugates are K-linearly independent and that M is G-stable by construction.

Suppose $N \subseteq M$ is a rank-1 G-stable direct summand of M. Then $N/\mathfrak{p}N$ is a G-stable direct summand of $M/\mathfrak{p}M$. Since N is of rank 1 there exists some $\mathbf{w} \in N$ such that $N/\mathfrak{p}N = \mathbf{w} \cdot (O_K/\mathfrak{p})$. Write $\overline{\mathbf{w}} = \sum_{g\in G} a_g \cdot g(\overline{\mathbf{v}})$ with $a_g \in O_K/\mathfrak{p}$. Because N is G-stable, there exists for each $h \in G$ some $b_h \in (O_K/\mathfrak{p})^*$ such that $h(\overline{\mathbf{w}}) = b_h\overline{\mathbf{w}}$. Since $\mathfrak{p}$ is totally ramified, the elements of $O_K/\mathfrak{p}$ are fixed by G. Hence

$$\sum_{g\in G} b_h a_g \cdot g(\overline{\mathbf{v}}) = b_h\overline{\mathbf{w}} = h(\overline{\mathbf{w}}) = \sum_{g\in G} a_g \cdot h(g(\overline{\mathbf{v}})) = \sum_{g\in G} a_{h^{-1}g} \cdot g(\overline{\mathbf{v}}),$$

and $b_h a_g = a_{h^{-1}g}$ for all $g, h \in G$. Since $\mathfrak{p}$ is wildly and completely ramified, we have that $\#G \in \mathfrak{p}'$. In particular, each $x \in O_{K'}/\mathfrak{p}'$ such that $x^{\#G} = 1$ satisfies $x = 1$. Let $g \in G$ be such that $a_g \neq 0$. Then

$$b_h^{\#G} = \prod_{i=0}^{\#G-1} \frac{a_{h^{i+1}g}}{a_{h^i g}} = \frac{a_{h^{\#G}g}}{a_g} = 1,$$

hence $b_h = 1$ for all h. It follows that $a_g = a_h$ for all $g, h \in G$. Hence $\overline{\mathbf{w}} \in \mathrm{Tr}_{K/K'}(M/\mathfrak{p}M)$ and $N \subseteq \mathfrak{p}M + \mathrm{Tr}_{K/K'}(M)$. Since $\mathfrak{p}$ is wildly ramified, we have $\mathrm{Tr}_{K/K'}(M) \subseteq \mathrm{Tr}_{K/K'}(O_K)F \subseteq \mathfrak{p}F$ by Lemma 9, so $N \subseteq \mathfrak{p}F$ but $M \nsubseteq \mathfrak{p}F$. As this holds for all N, we conclude that M cannot be a direct sum of rank-1 G-stable submodules. □

Example 1. Taking $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$ with $\alpha = 1+\mathrm{i}, \beta = 1$ and $\mathfrak{p} = (\alpha)$ in Proposition 1 gives the explicit $\mathbb{Z}[\mathrm{i}]$-module generated by $(1, \mathrm{i})$ and $(1, -\mathrm{i})$. It can be verified by hand that this module is G-stable (where $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\mathrm{i}))$), but that it cannot be written as a direct sum of two rank-1 G-stable submodules.

We can now use Theorem 2 to prove that for a G-stable module M (with some restriction on its discriminant), contracting and then extending M does not change the module. This is formally stated in the following theorem.

Theorem 3. *Let K/K' be a Galois extension of number fields with Galois group G, let $O \subseteq K$ be a Dedekind domain containing O_K, and let $M \subseteq O^n$ be a O-submodule of full rank n whose discriminant $\mathrm{disc}_K(M)$ is coprime to any prime of K' that is ramified in O. Then M is G-stable if and only if $O \cdot M^G = M$.*

Proof. If $O \cdot M^G = M$, then for all $g \in G$ we have $g(M) = O \cdot g(M^G) = O \cdot M^G = M$, which proves the backward implication. To prove the forward implication, it suffices to prove it locally at the primes of $O' = O \cap K'$, and thus we assume O' is local with prime $\mathfrak{p}'$. If $\mathfrak{p}'$ is ramified in O, then by assumption $\mathrm{disc}_K(M) = O$ and consequently $M = O^n$. In particular, $O \cdot M^G = M$ holds in this case. If $\mathfrak{p}'$ is unramified in O, then M is isomorphic as $O\langle G\rangle$-module to a direct sum of rank-1 modules of O by Theorem 2. These $O\langle G\rangle$-modules are each isomorphic to a fractional ideal of O, which no ramified prime divides by assumption. The result then follows from Lemma 10. □

Note that in Theorem 2, we only asked $\mathrm{disc}_K(M)$ to be coprime with any wildly ramified prime ideal, whereas in Theorem 3 we need to exclude all ramified prime ideals.

This is not an artifact of the proof: there exist counter-examples to Theorem 3 if we allow $\mathrm{disc}_K(M)$ to be divisible by tamely ramified primes. To see this, take $\mathfrak{p}$ to be any prime ideal of $\mathcal{O}_K$ which is fully ramified in K/K', but not wildly ramified. In other words, if $\mathfrak{p}' = \mathfrak{p} \cap \mathcal{O}_{K'}$ is the prime below $\mathfrak{p}$, then $\mathfrak{p}'\mathcal{O}_K = \mathfrak{p}^e$, where $e = [K : K']$. Then, take $n = 1$ and M to be the rank-1 module equal to $\mathfrak{p}$. Its discriminant is precisely $\mathrm{disc}_K(M) = \mathfrak{p}$, which is coprime to any wildly ramified prime by assumption. But $M^G = \mathfrak{p}^G = \mathfrak{p}'$, and so $\mathcal{O}_K M^G = \mathcal{O}_K \mathfrak{p}' = \mathfrak{p}^e \neq M$ (as soon as $e = [K : K'] > 1$).

Example 2 (Continuation of Example 1). The module M generated by $(1, \mathrm{i})$ and $(1, -\mathrm{i})$ in $K = \mathbb{Q}(i)$ has discriminant $2\mathcal{O}_K$, which is wildly ramified in $K/\mathbb{Q}$. One can check that $M^G = 2\mathbb{Z}^2$ and so $\mathcal{O}_K M^G = 2\mathcal{O}_K^2$ is included in M, but not equal to M.

4.1 Application: Solving Hermite SVP without loss in the approximation factor

We will now prove our main algorithmic result.

Theorem 4. *There is an algorithm that takes as input the ring of integers $\mathcal{O}_K$ of a number field K of degree d, an $\mathcal{O}_K$-submodule $M \subseteq K^n$ of rank $n > 0$ such that $\mathrm{disc}(M)$ is not divisible by any ramified prime, and a parameter $\gamma \geq 1$, and solves γ-HSVP in M, by making one call to an oracle solving γ-HSVP in $\mathbb{Z}$-lattices of rank nd/d_M, where $d_M = \#\{g \in \mathrm{Aut}_{\mathbb{Q}}(K) \mid g(M) = M\}$. Except for this call to the oracle, the algorithm runs in polynomial time in its input size.*

Proof. Let $G = \{g \in \mathrm{Aut}_{\mathbb{Q}}(K) \mid g(M) = M\}$. We will show that a solution to γ-HSVP in M^G is a solution to γ-HSVP in M. The algorithm from the theorem will then simply compute M^G (in polynomial time thanks to Lemma 12), then run the γ-HSVP oracle on M^G, and output the vector returned by the oracle. Note that M is G-stable by definition of G, that the extension K/K^G is Galois with Galois group G, and that the discriminant of M is unramified by assumption, hence, we can apply Theorem 3 to obtain that $M = \mathcal{O}_K \cdot M^G$. This implies in particular that M^G has rank exactly n, so we call our oracle on a $\mathbb{Z}$-lattice of rank nd/d_M as desired.

Let us then prove that a solution to γ-HSVP in M^G is a solution to γ-HSVP in M. First observe that

$$\mathcal{O}_K \cdot \mathrm{disc}_{K^G}(M^G) = \mathrm{disc}_K(\mathcal{O}_K \cdot M^G) = \mathrm{disc}_K(M),$$

where the first equality is Lemma 11 and the second is Theorem 3. Then by applying Lemma 8 twice we obtain

$$\begin{aligned}
\det(M^G)^{2d_M} &= N_{K^G/\mathbb{Q}}(\mathrm{disc}_{K^G}(M^G))^{d_M} \cdot \Delta_{K^G}^{nd_M} \cdot \left(\frac{d}{d_M}\right)^{-dn} \\
&= N_{K/\mathbb{Q}}(\mathcal{O}_K \cdot \mathrm{disc}_{K^G}(M^G)) \cdot \Delta_{K^G}^{nd_M} \cdot d^{-dn} \cdot d_M^{dn} \\
&= N_{K/\mathbb{Q}}(\mathrm{disc}_K(M)) \cdot \Delta_{K^G}^{nd_M} \cdot d^{-dn} \cdot d_M^{dn} \\
&= \det(M)^2 \cdot \left(\frac{\Delta_{K^G}^{d_M}}{\Delta_K}\right)^n \cdot d_M^{dn}.
\end{aligned}$$

It follows from Lemma 3 that $\Delta_{K^G}^{d_M}/\Delta_K \leq 1$. Hence if $\mathbf{x} \in M^G$ is a solution to γ-HSVP in M^G, then

$$0 < \|\mathbf{x}\| \leq \gamma \cdot \sqrt{nd/d_M} \cdot \det(M^G)^{d_M/(nd)} \leq \gamma \cdot \sqrt{nd} \cdot \det(M)^{1/(nd)},$$

so indeed $\mathbf{x}$ is a solution to γ-HSVP in M. □

Acknowledgment. We thank the reviewers of Crypto 2023 and Nutmic 2026 for their constructive comments. Alice Pellet-Mary is supported by the TOTORO ANR grant (ANR-23-CE48-0002) and by the France 2030 program, managed by the French National Research Agency (ANR-22-PETQ-0008 PQ-TLS). Daniël van Gent is supported by the Quantum Software Consortium project (file number 024.003.037) of the Zwaartekracht research programme which is (partly) financed by the Dutch Research Council (NWO).

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. Bhargava, M., Shankar, A., Taniguchi, T., Thorne, F., Tsimerman, J., Zhao, Y.: Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. Journal of the American Mathematical Society **33**(4), 1087–1099 (2020), https://doi.org/10.1090/jams/945
4. de Boer, K.: Random walks on Arakelov class groups. Ph.D. thesis, Leiden University (2022), https://hdl.handle.net/1887/3463719
5. 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), https://doi.org/10.1007/978-3-031-15979-4_17
6. 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
7. Cohen, H.: Advanced Topics in Computational Number Theory. Graduate Texts in Mathematics, Springer New York (2012), https://doi.org/10.1007/978-1-4419-8489-0
8. Ducas, L., Postlethwaite, E.W., Pulles, L.N., van Woerden, W.P.J.: Hawk: Module LIP makes lattice signatures fast, compact and simple. In: Agrawal, S., Lin, D. (eds.) 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 IV. Lecture Notes in Computer Science, vol. 13794, pp. 65–94. Springer (2022), https://doi.org/10.1007/978-3-031-22972-5_3
9. 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), https://doi.org/10.1007/978-3-031-22969-5_24
10. van Gent, D.M.H., Pulles, L.N.: HAWK: Having automorphisms weakens key. IACR Communications in Cryptology **2**(2) (2025), https://doi.org/10.62056/a3qjp2w9p

11. Hanrot, G., Pujol, X., Stehlé, D.: Analyzing blockwise lattice algorithms using dynamical systems. In: Advances in Cryptology–CRYPTO 2011. pp. 447–464. Springer (2011), https://doi.org/10.1007/978-3-642-22792-9_25
12. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Algorithmic number theory, pp. 267–288. Springer (1998), https://doi.org/10.1007/BFb0054868
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. Lenstra, A.K.: Factoring polynomials over algebraic number fields. Lecture Notes in Computer Science **162** (1983), https://doi.org/10.1007/3-540-12868-9_108
15. 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), https://doi.org/10.1007/978-3-642-13190-5_1
16. Marcus, D.A.: Number fields, vol. 1995. Springer (1977), https://doi.org/10.1007/978-3-319-90233-3
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), https://doi.org/10.1007/978-3-030-77870-5_20
18. Pellet-Mary, A., Stehlé, D.: On the Hardness of the NTRU Problem. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021. vol. 13090. Springer (2021), https://doi.org/10.1007/978-3-030-92062-3_1
19. Porter, C., Mendelsohn, A., Ling, C.: Subfield Algorithms for Ideal- and Module-SVP Based on the Decomposition Group (2021), https://arxiv.org/abs/2105.03219
20. 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), https://doi.org/10.1007/978-3-642-10366-7_36

A A proof using pseudo-bases

In this section we give an alternative proof to Theorem 3 (in the special case where $\mathcal{O} = \mathcal{O}_K$ is the ring of integer of K) using the theory of pseudo bases. We first recall some preliminaries about pseudo-bases and Hermite normal form.

A.1 Additional preliminaries

Let us first recall the definition of pseudo-bases, see [7] for more details. For any rank-n $\mathcal{O}_K$-module $M \subset K^m$, there exists K-linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in K^n$ and fractional ideals $I_i \subset K$ such that

$$M = \mathbf{b}_1 I_1 + \cdots + \mathbf{b}_n I_n := \{\sum_{i=1}^{n} x_i \mathbf{b}_i \,|\, x_i \in I_i\}.$$

We say that $((\mathbf{b}_i, I_i))_{1 \le i \le n}$ is a *pseudo-basis* of the module M.

Any rank-n module $M \subset K^n$ admits a special pseudo-basis $((\mathbf{b}_i, I_i))_{1 \le i \le n}$, called the *Hermite Normal Form* of M (or HNF for short). This pseudo-basis is such that the

matrix $\mathbf{B} \in K^{n\times n}$ formed by concatenating the column vectors $\mathbf{b}_i$ is upper triangular with 1's on the diagonal (see [7, Thm. 1.4.6]).

The following two lemmas describe pseudo-bases for the extension and contraction of a module. More precisely, Lemma 15 describes some pseudo-bases of the extension $O_K \cdot M'$, and Lemma 16 describes some pseudo-bases of the contraction $M \cap K'$ (provided we have a pseudo-basis of M with special properties).

Lemma 15. *Let K/K' be number fields. Let $M' \subset (K')^m$ be an $O_{K'}$-module of rank n. Let $((\mathbf{b}'_i, I'_i))_{1\le i\le n}$ be a pseudo-basis of M' (with $\mathbf{b}'_i \in (K')^m$ and I'_i fractional $O_{K'}$-ideals). Then $O_K \cdot M'$ is an O_K-module of rank n in K^m and $((\mathbf{b}'_i, I'_i O_K))_{1\le i\le n}$ is a pseudo-basis of it.*

Proof. This follows from the definition of $O_K \cdot M'$ and $I'_i \cdot O_K$. □

Lemma 16. *Let K/K' be number fields. Let $M \subset K^m$ be a rank-n O_K-module (for some $m \ge n > 0$). Assume that M admits a pseudo-basis $((\mathbf{b}'_i, I_i))_{1\le i\le n}$ with the vectors $\mathbf{b}'_i \in (K')^m$ (instead of in K^m), and the $I_i \subset K$ fractional O_K-ideals (as usual). Then, $M \cap (K')^m$ is an $O_{K'}$-module of rank n and $((\mathbf{b}'_i, I'_i))_{1\le i\le n}$ is a pseudo-basis of it, where $I'_i = I_i \cap K'$.*

Proof. Let M' be the rank-n $O_{K'}$-module generated by the pseudo-basis $((\mathbf{b}'_i, I'_i))_{1\le i\le n}$. 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 $1 \le i \le n$ 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, $x_i \in I_i \cap K' = I'_i$, which implies that $\mathbf{v} \in M'$ as desired. □

The following lemma provides an alternative definition for the discriminant of a module, which will be useful in our pseudo-basis-based proof. In particular, the lemma shows that the ideal discriminant of a module $M \subseteq K^m$ can be efficiently computed, when given a pseudo-basis of M.

Lemma 17. *Let $M \subset K^m$ be a rank-n O_K-module with pseudo-basis $((\mathbf{b}_i, I_i))_{1\le i\le n}$. Let $\mathbf{B} \in K^{m\times n}$ be the matrix whose columns are the $\mathbf{b}_i$'s. Then*

$$\mathrm{disc}_K(M) = \left(\prod_{i=1}^{n} I_i\right)^2 \cdot \det(\mathbf{B}^T\mathbf{B}), \tag{1}$$

where $\det : M_n(K) \to K$ is the determinant over K. In particular, the ideal on the right hand side of Equation (1) does not depend on the choice of the pseudo-basis.

Proof. Let us first remark that $\det(\mathbf{B}^T\mathbf{B}) = \det((\varphi(\mathbf{b}_i, \mathbf{b}_j))_{i,j})$, for φ as in Definition 3 (i.e., $\varphi(\mathbf{x}, \mathbf{y}) = \sum_i x_i y_i$). We prove first the inclusion $\mathrm{disc}_K(M) \subseteq \left(\prod_{i=1}^n I_i\right)^2 \cdot \det(\mathbf{B}^T\mathbf{B})$.

Since the right-hand side is an ideal, it suffices to show that for any linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in M, $\det((\varphi(\mathbf{v}_i, \mathbf{v}_j))_{i,j}) \in \left(\prod_{i=1}^n I_i\right)^2 \cdot \det(\mathbf{B}^T\mathbf{B})$. Since the $\mathbf{v}_j$'s are in M, then for each j, there exists $\alpha_{i,j} \in I_i$ such that $\mathbf{v}_j = \sum_i \alpha_{i,j}\mathbf{b}_i$. Writing $\mathbf{V}$ the matrix whose columns are the $\mathbf{v}_j$'s and $\mathbf{A} = (\alpha_{i,j})_{i,j}$, we have that $\mathbf{V} = \mathbf{BA}$. Then $\det(\mathbf{V}^T\mathbf{V}) = \det(\mathbf{A})^2 \det(\mathbf{B}^T\mathbf{B})$, and the desired inclusion follows from the fact that $\det(\mathbf{A}) \in \prod_i I_i$, since $\alpha_{i,j} \in I_i$ for all (i, j)'s.

For the reverse inclusion, let us first observe that, for any fractional ideal I of K, then I^2 is the ideal generated by the squares of I (i.e., $I^2 = \langle \alpha^2 | \alpha \in I \rangle$).[10] Hence, to prove the inclusion it suffices to prove that for any $\alpha_i \in I_i$, we have $\prod_i \alpha_i^2 \det(\mathbf{B}^T\mathbf{B}) \in \mathrm{disc}_K(M)$. Taking $\mathbf{v}_i = \alpha_i \mathbf{b}_i$, we have that each $\mathbf{v}_i$ belongs to M, and that they are linearly independent. Hence, by definition of $\mathrm{disc}_K(M)$, we have $\prod_i \alpha_i^2 \det(\mathbf{B}^T\mathbf{B}) = \det((\varphi(\mathbf{v}_i, \mathbf{v}_j))_{i,j}) \in \mathrm{disc}_K(M)$ as desired. □

A.2 Alternative proof of Theorem 3

We now proceed to give an alternative proof to Theorem 3, in the special case where the ring $\mathcal{O}$ is the ring of integers $\mathcal{O}_K$ of K. Since the theory of pseudo-bases also exists for any Dedekind domain $\mathcal{O}$, it is possible that the proof presented in this section can be generalized to the Dedekind domain setting (as in Theorem 3). However, our objective is to make this proof as elementary as possible, so we decided to focus only on the case where $\mathcal{O} = \mathcal{O}_K$. We also note that this special case is the most relevant for cryptographic applications, and is the only one needed to prove our algorithmic result in Theorem 4. We start by proving an auxiliary lemma, which contains most of the technical content.

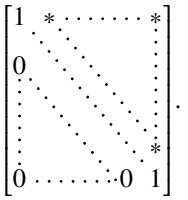
Lemma 18. *Let K/K' be a Galois extension of number fields with Galois group G, together with $M \subseteq \mathcal{O}_K^n$ an $\mathcal{O}_K$-module of rank n. If M is G-stable and $\mathrm{disc}_K(M)$ is not divisible by any prime ideal that is wildly ramified in K/K', then there exists a pseudo-basis $((\mathbf{b}_k, I_k))_{1 \le k \le n}$ of M such that $\mathbf{b}_k \in (K')^n$, $\det_K(\mathbf{b}_1, \ldots, \mathbf{b}_n) = 1$, and $I_k \subseteq \mathcal{O}_K$ is G-stable.*

Note that this lemma implies that the module M can be decomposed as a direct sum of rank-1 G-stable submodules (the submodules $I_k\mathbf{b}_k$, for $k = 1$ to n). This is similar to what was proven in Theorem 2, in the special case where $\mathcal{O} = \mathcal{O}_K$.

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

[10] A proof of this fact is as follows. Without loss of generality, we can assume that $I \subseteq \mathcal{O}_K$ is an integral ideal (we can scale it by an integer if this is not the case). Write $I = a\mathcal{O}_K + b\mathcal{O}_K$ for some $a, b \in \mathcal{O}_K$ (there is a two-elements representation of the ideal since $\mathcal{O}_K$ is a Dedekind domain). Then, thanks to the unique factorization of I into prime ideals, we have that $I = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{\min(v_\mathfrak{p}(a), v_\mathfrak{p}(b))}$, where $v_\mathfrak{p}(\cdot)$ is the valuation at $\mathfrak{p}$. Taking the square, we obtain $I^2 = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{2\min(v_\mathfrak{p}(a), v_\mathfrak{p}(b))} = a^2\mathcal{O}_K + b^2\mathcal{O}_K$. Hence, I^2 is generated by a^2 and b^2, for some $a, b \in I$.

form



Since $M \subseteq (\mathcal{O}_K)^n$ and because $\mathbf{B}$ has 1's on its diagonal, this implies that for each $k \in [\![1, n]\!]$ the ideal I_k is integral. Let us show that these ideals are also G-stable.

Fix $k \in [\![1, n]\!]$, $g \in G$ and $x \in I_k$. Then $g(x\mathbf{b}_k) \in M$ since M is G-stable, thus we get $g(x\mathbf{b}_k) = \sum_{i=1}^{n} x_i b_i$ with $x_i \in I_i$ for any $i \in [\![1, n]\!]$. Recall that g is applied to $x\mathbf{b}_k$ coordinate-wise, hence the i-th coordinate of $g(x\mathbf{b}_k)$ is 0 for $i > k$, and for $i = k$ it is equal to $g(x \cdot 1) = g(x)$. Considering the triangular shape of the matrix $\mathbf{B}$, one can conclude that $\forall i > k, x_i = 0$. Moreover if one focuses on the k-th coefficient of $g(x\mathbf{b}_k)$, one has $g(x) = x_k \in I_k$. This is true for any $g \in G$ 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 $\mathbf{B}$ is triangular with 1's on the diagonal, then, by Lemma 17, it holds that $\mathrm{disc}_K(M) = \prod_{k=1}^{n} I_k^2$. Recall that we required that $\mathrm{disc}_K(M)$ be coprime with all wildly ramified ideals of $\mathcal{O}_K$. Using Lemma 9, this implies that $\mathrm{disc}_K(M) \cap K'$ is coprime with $\mathrm{Tr}_{K/K'}(\mathcal{O}_K)$. Indeed, Lemma 9 tells us that when K/K' is Galois (which is our case here), then the only prime ideals $\mathfrak{p}'$ of K' that divide $\mathrm{Tr}_{K/K'}(\mathcal{O}_K)$ are precisely the ones that are wildly ramified in K/K'. Since the prime ideals dividing $\mathrm{disc}_K(M) \cap K'$ are below the prime ideals dividing $\mathrm{disc}_K(M)$, then none of them is wildly ramified, and so $\mathrm{disc}_K(M) \cap K'$ is coprime with $\mathrm{Tr}_{K/K'}(\mathcal{O}_K)$.

Overall, we obtain that $I_k \cap K'$ is coprime with $\mathrm{Tr}_{K/K'}(\mathcal{O}_K)$ for all k's (here, we use the fact that the I_k's are integral ideals, which implies that I_k divides $\mathrm{disc}_K(M)$ and so $I_k \cap K'$ divides $\mathrm{disc}_K(M) \cap K'$). This implies that for each k, there exist some elements $\alpha_k \in \mathcal{O}_K$ and $\beta_k \in I_k \cap K'$ such that $\mathrm{Tr}_{K/K'}(\alpha_k) = 1 + \beta_k$. 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 $i \leqslant k$. We start by the case $i = k$. For a given $x \in I_{k+1}$ and $g \in G$, the vector $g(x\mathbf{b}_{k+1})$ belongs to M, so, as above, one can write:

$$g(x\mathbf{b}_{k+1}) = \sum_{i=1}^{k} x_i \mathbf{b}_i + g(x)\mathbf{b}_{k+1}, \tag{2}$$

for some $x_i \in I_i$. Looking at the k-th coordinate gives $g(xz_k) = x_k + g(x)z_k$, which leads to $g(x)(z_k - g(z_k)) = -x_k \in I_k$. This is true for any $x \in I_{k+1}$ hence we have $g(I_{k+1}) \cdot (z_k - g(z_k)) \subseteq I_k$. Since I_{k+1} is G-stable, this is equivalent to $I_{k+1} \cdot (z_k - g(z_k)) \subseteq$

I_k, i.e.,

$$(z_k - g(z_k)) \in I_k \cdot I_{k+1}^{-1}.$$

Let $\alpha_k \in O_K$ 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 $g(\alpha_k) \in O_K$, it holds that $g(\alpha_k) \cdot (z_k - g(z_k)) \in I_k \cdot I_{k+1}^{-1}$. Summing over all $g \in G$ 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 $\mathbf{b}_{k+1} \cdot I_{k+1} \subset (O_K)^n$ (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 $\mathbf{b}'_{k+1} := \mathbf{b}_{k+1} + (\mathrm{Tr}_{K/K'}(\alpha_k z_k) - z_k) \cdot \mathbf{b}_k$. This is still a pseudo-basis of M thanks to the fact that $z_k - \mathrm{Tr}_{K/K'}(\alpha_k \cdot z_k) \in I_k \cdot I_{k+1}^{-1}$. And it ensures that the k-th coefficient of $\mathbf{b}'_k$ is equal to $\mathrm{Tr}_{K/K'}(\alpha_k z_k) \in K'$.

This proves the initialization step of our (inner) induction. Let us now write $y_{k,k+1}$ this element. We 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 $g \in G$. We will use Equation (2) 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 (2) which gives $g(x)g(z_{i-1}) = x_{i-1} + g(x)z_{i-1}$, using ($*$). We see that we are in the same situation as before, replacing k by $i-1$. Thus, the same steps lead to $z_{i-1} - \mathrm{Tr}_{K/K'}(\alpha_{i-1}z_{i-1}) \in I_{i-1}I_{k+1}^{-1}$, and we can replace $\mathbf{b}_{k+1}$ by $\mathbf{b}'_{k+1} := \mathbf{b}_{k+1} + (\mathrm{Tr}_{K/K'}(\alpha_{i-1}z_{i-1}) - z_{i-1}) \cdot \mathbf{b}_{i-1}$, whose $(i-1)$-th coefficient is $y_{i-1,k+1} := \mathrm{Tr}_{K/K'}(\alpha_{i-1}z_{i-1}) \in K'$. This does not modify the coefficients of $\mathbf{b}_{k+1}$ whose index is at least i, so they remain in K' as desired. This ends our proof by induction.

We are left with proving ($*$). We will again show this by induction. The k-th coordinate of Equation (2) gives $g(xy_{k,k+1}) = g(x)y_{k,k+1} = x_k + g(x)y_{k,k+1}$, using the fact that $g(y_{k,k+1}) = y_{k,k+1}$, since $y_{k,k+1} \in K'$. Thus, we have $x_k = 0$. Now assume that $x_k = x_{k-1} = \cdots = x_j = 0$ for some fixed $j \in [\![i+1, k]\!]$. The $(j-1)$-th coordinate in Equation (2) gives $g(x)g(y_{j-1,k+1}) = g(x)y_{j-1,k+1} = \sum_{l=j-1}^{k} x_l y_{j-1,l} + g(x)y_{k+1,l}$. By induction hypothesis we have $g(x)y_{j-1,k+1} = x_{j-1} + g(x)y_{k+1,l}$, 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 $\det(\mathbf{b}_1, \ldots, \mathbf{b}_n) = 1$. This follows from the fact that the matrix $\mathbf{B}$ is triangular with 1's on the diagonal. □

We can now use these two lemmas to prove Theorem 3, in the special case when $O = O_K$.

Theorem 5 (Theorem 3 specialized with $O = O_K$). *Let K/K' be a Galois extension of number fields, with Galois group G, and let O_K be the ring of integers of K. Let $M \subseteq O_K^n$ be an O_K-module of full rank n 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 $O_K \cdot M^G = M$.*

Proof. The assumption that the discriminant of M is coprime with all ramified primes implies in particular that it is coprime with all wildly ramified primes. We can then apply Lemma 18, which tells us that there exists a pseudo-basis $((\mathbf{b}_k, I_k))_{1\leq k\leq n}$ 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 $\det(\mathbf{b}_1, \ldots, \mathbf{b}_n) = 1$. We first remark that since $\det(\mathbf{b}_1, \ldots, \mathbf{b}_n) = 1$ and the ideals I_k are integral, then each ideal I_k divides the discriminant of M (by Lemma 17), and so is unramified by assumption.

Using Lemmas 16 and 15, we then see that $((\mathbf{b}_k, (I_k \cap K') \cdot \mathcal{O}_K))_{1\leq k\leq n}$ is a pseudo-basis of $\mathcal{O}_K \cdot (M \cap K') = \mathcal{O}_K \cdot M^G$. Here, we use the fact that the $\mathbf{b}_i$'s are in K', so we can indeed apply Lemma 16. Since the ideals I_k are G-stable, integral and unramified, we know from Lemma 10 that $(I_k \cap K') \cdot \mathcal{O}_K = I_k$ for all k. This implies that $\mathcal{O}_K \cdot M^G = M$ as desired. □